ISSN: 2473-4901
v10 n6202

# An Analysis of Methodologies for the Prevention and Mitigation of Cheating in Online Gaming Using Artificial Intelligence and its Ethical Impact

Alexander J. Flynn
Flynna6@southernct.edu

Brandon D. Tischer
Tischerb1@southernct.edu

Jose D. Mandujano
Mandujanoj3@southernct.edu

Mark A. Pisano
Pisanom1@southernct.edu

Business Information Systems
Southern Connecticut State University
New Haven, CT 06515, USA

## Abstract

Artificial intelligence (AI) encompasses diverse technologies that utilize data to perform complex tasks traditionally requiring human intelligence. Over the past decade, AI has become integral to various sectors, such as e-commerce, healthcare, manufacturing, and entertainment. AI's impact on the gaming industry is particularly noteworthy, revolutionizing gameplay through advancements like machine learning. This technology enhances gaming experiences by creating more realistic and autonomous non-player characters. AI also plays a critical role in combating cheating in online gaming through sophisticated anti-cheat measures. This discussion explores AI's significant contributions to gaming, highlighting its evolution in shaping immersive environments and addressing industry-specific challenges. By leveraging AI, the gaming sector enhances gameplay dynamics and ensures fairness and integrity, thus influencing the future of interactive entertainment.

**Keywords:** Artificial Intelligence, Gaming, Machine Learning, Anti-cheat

### 1. INTRODUCTION

What is artificial intelligence? Artificial intelligence (AI) "is beyond a specific technology, but is rather, a combination of different technologies, systems, and devices that use data to perform some complex, complicated tasks (Gbadegeshin, et al., 2021)." Artificial intelligence is a broad term that describes systems capable of performing tasks typically requiring human intelligence, such as problem-solving, learning, reasoning, perception, learning comprehension, and decision-making, and can range from basic rule-based algorithms to highly complex neural networks. Over the last decade, AI has witnessed widespread adoption across many domains, including e-commerce, healthcare, financial services, logistics, manufacturing, software

development, and much more. AI has the potential to revolutionize many of these industries further, even becoming its own industry, with many companies and organizations now existing to research, create, and distribute AI algorithms and software to support these sectors. According to the McKinsey Global Institute, AI could potentially contribute an additional $13 trillion to global economic activity, an increase of 16% (Bughin et al., 2018). This demonstrates AI's massive potential impact across the global economy due to its vast applications and use cases. Due to the broad appeal of artificial intelligence, questions may arise regarding its effects on particular industries. AI has made an impact, especially in the entertainment industry, with generative applications. Its ability to generate text, imagery, sound, and video has popularized the concept among the general public. However, many forms of AI can work to assist in or automate countless tasks. Its effect on the video gaming industry is especially apparent as it has worked for years in the background, typically under the name 'machine learning,' contributing to revolutionary gameplay and creating immersive experiences. It has been used in the development and gameplay of video games, with just one example being the behavior of non-player characters and how they interact with the player to create enhanced depth and realism for the player. Using AI, these non-player characters can become far more autonomous, reactive, and believable than those designed using traditional methodologies (Buede ey al., 2013). Here, we will discuss its impact on the gaming industry, specifically how it has revolutionized processes and techniques for mitigating the act of cheating in online gaming, known as anti-cheat, while also addressing ethical considerations and recommendations for fair implementation.

## 2. GAMING INDUSTRY

AI has already had an impact on the gaming industry. The gaming industry is another behemoth, worth $300 billion as of 2021 (Accenture, 2021), and it is considered one of the most tech-forward industries in entertainment.

Video games have grown from simple simulations to significant entertainment experiences. As such, the industry has grown and matured over the past few decades. It is a multibillion-dollar industry that drives hardware and software innovations and other digital transformations. Unsurprisingly, in 2023, the video game industry outperformed the music and film industries by around $249.6 billion dollars. (Jyothiraditya, 2024). This growth and performance have a significant economic impact, supporting all of the jobs required to further create and innovate, from game development and publishing to all miscellaneous needs. (Oguguo, 2024). This has indeed become an industry that influences daily life.

This extensive industry comprises a large number of companies that produce a wide range of games. This variety allows for the production of games that are enjoyed by all generations, including Baby Boomers (1946-1964), Generation X (1965-1980), Millennials (1981-1996), GenZ (1996-2012), and the current generation of children. (Ball, 2024). This is truly an industry that can significantly impact both financially and socially.

As mentioned before, the gaming industry is made up of a large number of companies of varying sizes. Additionally, it is common for larger gaming companies to buy smaller ones to gain a specific user segment or to gain their intellectual property. For this paper, the authors will focus on several companies that stand out based on revenue. This includes Sony Interactive Entertainment, Tencent Games, Microsoft (Xbox Game Studios, Bethesda Softworks, and Activision Blizzard), Nintendo, and NetEase Games. These companies had revenues ranging from roughly $11 billion to $30 billion dollars. (Oguguo, 2024).

Due to the industry's large size, it is helpful to narrow the scope of evaluation to the larger companies. The idea is that they will have the most influence on the overall industry and its usage of AI technologies, such as anti-cheats.

## 3. CHEATING

Playing online video games is a very common pastime and an enjoyable thing to do as a teen or young adult. As you play these online games such as Fortnite, Call of Duty, Counter Strike 2, and League of Legends you can encounter an abundance of cheaters. A cheater refers to a player who uses various methods to gain an advantage over the gameplay that the developers do not intend. The number of cheaters and type of cheaters can vary per game. These cheating methods usually make the game easier / achieve an unfair advantage to other players, which harms the game. Some of these cheats in gaming can be categorized based on various methods, intents, and tools used. Some of the standard classifications are Software cheats, where you install an application such as aim bots/ Trigger

Bot in first-person shooter video games. According to Irdeto (Omdia, 2022), a global digital platform security company specializing in cybersecurity services in various industries, several cheats disrupt gameplay.

- Aim-bot/Trigger Bot: These automate aiming, guaranteeing near-perfect accuracy or automatically firing when the crosshairs are over an enemy. This eliminates the skill required for good aim, making combat a one-sided affair and ruining the satisfaction of landing a difficult shot.
- Wallhack: This cheat allows players to see enemies through walls and obstacles, granting them complete situational awareness. This destroys the balance of hidden movement and surprise attacks that are core mechanics in many games.
- Esp/Extrasensory Perception: This broad category encompasses cheats that reveal hidden information like player health, location, and equipment. This removes the challenge of gathering intel and outmaneuvering opponents, making winning much easier for the cheater but incredibly frustrating for those targeted.
- Speed Hacks/No Clip: These manipulate movement speed or allow players to walk through walls, completely breaking the game's intended pace and level design. It can make it impossible for others to react or compete.
- Bots: Automated programs play the game for the user, farming resources, grinding levels, or even competing in online matches without human input. This removes the entire point of playing the game and the sense of accomplishment from achieving goals.

Network cheats are also a unique way to get ahead of other players, usually in networked games that manipulate the communication between the client and the server, which affects gameplay data integrity and the user experience. Examples of network cheats are lag switching, a device that temporarily interrupts a player's network connection, creating a lag spike, and packet injections, where the user can alter gameplay mechanics such as revealing player positions, increasing player speed, and making yourself invulnerable to damage.

The last type of cheat the cheater can use is Scripts. Scripts can be created by players or third parties and have various purposes. One of them is macro scripting, which automates a series of inputs or actions that would make the task in the game easier for the player.

To counteract these practices, game developers create anti-cheats for their games or invest in a third-party solution. These anti-cheats try to counteract and neutralize cheating attempts to ensure a fair and enjoyable gaming experience for all players.

## 4. MOTIVATIONS AND IMPACTS OF CHEATING

As someone who plays games, participates in sports, or navigates daily life, consider the motivations behind why someone might cheat. Many players frequently encounter this thought, especially when faced with a hacker in their game lobby, as they feel all emotions. There are several reasons why cheaters might want to hack into these games. Players with a solid competitive drive may cheat to gain the benefits of winning, such as cash prizes, in-game rewards like experience points or unlockable items, and the satisfaction of defeating better players. High levels of aggression can make these individuals cheat to release their frustration or hostility towards these players. Additionally, peer influence and social norms play a role; if cheating is widely accepted or common among peers, individuals are more inclined to conform. The low risk of getting banned in some games encourages this behavior, increasing cheater engagement. (Sung Je et al., 2021)

Cheating in video games disrupts fair play and destroys the players' trust. When another person you are facing cheats in the game, the player often feels frustrated due to the cheater's unreachable abilities. These acts also make the player feel a diminished sense of accomplishment due to the fair play that is originally intended, and it destroys the satisfaction of overcoming everyday challenges in the game, such as leveling up or improving. Even the players who cheat are impacted in some way; they miss out on the challenge and excitement of the intended game.

Cheating eliminates the opportunity to strategize, practice, and improve, as cheaters rely on unfair advantages to achieve results they could not attain otherwise. This deprives them of learning opportunities and mastering game mechanics, eventually leading to boredom. Moreover, cheating ruins the experience for other players. It disrupts the community by fostering a hostile environment. Trust among players dissolves, toxic behavior escalates, and a cycle of cheating

is perpetuated. Honest players often feel discouraged or abandon the game altogether due to rampant cheating.

## 5. AI ANTI-CHEAT

There is high demand across the gaming industry to use cutting-edge technology to enhance customer experiences and build value for game companies. However, technology like AI has also been used to help solve problems that have haunted this industry for years, such as cheating. Cheating in online gameplay is a significant problem that many developers are determined to solve, as it creates unfair advantages and may discourage honest players from using these platforms. Many companies believe that highly advanced technologies such as artificial intelligence and machine learning are the best way to mitigate this to get ahead of cheaters, who can also be highly adept at using technology to their advantage.

Anti-cheat software incorporates various methodologies to maximize efficacy in detecting cheating software. Machine learning is applied across many areas to detect cheats, including detecting third-party software, image and video analysis, communication monitoring, assigning risk scores and preemptive actions, and more. This is because of the flexibility and effectiveness of pattern recognition common in machine learning algorithms. Given there are many use cases for machine learning algorithms in cheating detection, we will focus on a few examples.

Machine learning is used for pattern recognition, and in the context of cheat detection, this is used to analyze player behavior to detect anomalies. The software can analyze player movements, aiming precision, or reaction times and compare them against rules or standards that define typical human behaviors. If they do not match within a given margin of error, this will be flagged as potential cheating behaviors. Convolutional neural networks (CNNs) are effective in this pattern recognition due to their ability to recognize patterns across various contexts in gaming behavior. (José Pedro Pinto, 2021)

Machine learning enhances anti-cheating by providing an automated and efficient approach to combat cheating. Many companies have integrated AI with their anti-cheat systems with applications ranging from simple tasks to complex cheat detection. The most current and best way to stop cheating is AI. Cheating is an ever-changing aspect of gaming, driven by the constant demand for unfair advantages. To keep up, anti-cheat developers must continuously evolve and improve their systems. AI offers a more dynamic and efficient solution by detecting abnormal gameplay with real-time monitoring and adapting to new cheating techniques. AI can analyze vast amounts of gameplay data to find unusual behavior such as reaction time and weird movements that cannot be possible which indicate cheating. This differs from traditional methods that rely on more static algorithms and predefined rules, which can be bypassed by sophisticated cheat developers or anyone searching for cheats to install or purchase.

For many developers of online games, the goal is to eliminate multiple forms of cheating within their games to ensure a level playing field for all players. As trends have indicated, the increasingly complex methods of mitigating cheating have given way to more sophisticated ways to subvert and evade them. Artificial intelligence enhances anti-cheat techniques by providing an automated and efficient approach to combat cheating. Many companies have integrated AI with their anti-cheat systems with applications ranging from simple tasks to complex cheat detection.

There are multitudes of examples of anti-cheat tools that use AI technologies such as machine learning, chiefly of which being BattlEye, the system in use in PlayerUnknown's Battlegrounds (PUBG), DayZ, and other popular games. According to their website, BattlEye, or BE, was founded by Bastian Suter in October 2004. It was initially used as a third-party tool that online game administrators could implement into their servers. Still, eventually, as it gained popularity, game developers began to build it into the game at a deeper level, providing further ability for cheating detection and prevention. Their system constantly evolves, using an intelligent and dynamic on-the-fly detection system that works autonomously from the developer. (BattlEye, n.d.). Scanning and detection enable developers to take action against offending users, usually through bans.

Most creators of anti-cheat systems do not disclose in detail the methods in which they accomplish the goal of preventing and catching these exploits, as cheaters can and will take advantage of this sensitive information. However, in the case of BattlEye's high-level overview of how the system works is given. Their system is advertised as a "fully fledged proactive protection system" that includes "fast, dynamic, and permanent scanning of the player's system in user- and kernel-mode using innovative,

sophisticated specific and heuristic/generic detection and cheat analysis routines for maximum effectiveness. (BattlEye, n.d.)."

A second popular anti-cheat system, Easy Anti-Cheat (EAC), was created by Epic Games and is used in popular titles such as Apex Legends, Fortnite, and Rust. Epic Games refers to itself as an industry leader in the anti-cheat space. They counter the root cause of cheating with industry-leading prevention techniques that are constantly evolving and believe advanced prevention is more effective than older mass-penalization approaches. (Epic Games, Inc, 2024).

EAC is on the client side and uses vigilant memory scanning during gameplay. This real-time monitoring actively monitors the client's memory for any suspicious activity that attempts to alter the game's memory. This system helps maintain a fair environment for the game by addressing these cheats now as they occur.

Additionally, it can detect what is output gameplay-wise by the game through behavior analysis. It can be used to find unusual behavior, such as reaction time and weird movements that cannot be possible by an actual human, which indicates cheating. By vast amounts of data, it learns what constitutes normal and analyzes the outliers to identify if they are cheating. This area is beneficial as it is a different way of detection; instead of seeing if the person has cheated on the computer, it looks at the abnormal gameplay deviations through many datasets. This is effective against cheats that can bypass detection in any anti-cheat system. Along with behavioral analysis, AI will create personalized risk profiles, focusing efforts on players who are most likely to cheat based on past behavior or in-game actions (Team Modl.ai, 2024). This enhances the efficiency of anti-cheat measures by prioritizing high-risk players and placing them in different game lobbies with other cheaters. This can be found in Valve's Game Counter Strike 2. This differs from traditional methods that rely on more static algorithms and predefined rules, which can be bypassed by sophisticated cheat developers or anyone searching for cheats to install or purchase.

A third key player is Valve and its Valve Anti-Cheat (VAC), an "automated system designed to detect cheats installed on users' computers. (Steam Support, n.d.)." This is a more traditional system where a player will be permanently banned from a game server if any cheats are identified on their computer. It typically requires analysis of computer files and processes at the kernel level. In the past few years, however, Valve has been developing more advanced methodologies for detecting and stopping the use of cheat software in online game environments. In a patent filing, they outline the use of deep learning techniques to train models to "classify particular types of gameplay actions as being unauthorized if cheat software use is detected. (International Patent Patent No. WO 2019/182868 A1, 2019)." This newer system has come to be known as VACnet. All these key players have in common that they are all used extensively across different online games played by millions, and they all incorporate some form of artificial intelligence in their techniques, showing that it is a highly useful and essential tool for stopping cheating in online gaming.

While artificial intelligence can be beneficial and effective in the fight against cheating in online games, there are still disadvantages and limitations to the technologies that should be noted, especially when exploring its implementation into games that have the potential to reach millions of people. The first is that AI uses large amounts of data and will use either machine learning algorithms, large-language models (LLMs), or a combination of these to achieve a desired output. As these become more complex, it becomes increasingly difficult to trace the decision-making process and calculations used to reach a given conclusion. In turn, predicting precisely how an AI-powered application will react to given inputs becomes more difficult. In online gaming, users could potentially experience false positives where their behavior is flagged as suspicious or consistent with the use of cheating software when it is not the case, leading to player dissatisfaction or, in a worst-case scenario, an automatic ban from the game. This can be limited through extensive testing of the models, with many actions that could trigger the system. It is also worth noting that false positive rates can be the same or higher in more traditional, primitive techniques such as basic rules-based detection.

A second consideration regarding AI-powered anti-cheat methodologies and potential concerns regards privacy. Without proper ethical safeguards, implementation processes, and security protocols in place, players' computer files and data can be exposed to the system. Existing anti-cheat software using more traditional kernel-based approaches access computer resources, processes, and files at a far deeper level than other types of software to detect unauthorized cheating software. Riot Games, creators of the Vanguard anti-cheat software, assure users that

ISSN: 2473-4901
v10 n6202

they do not collect or process any personal information beyond what is required to maintain the integrity and the game's operation. The driver used for the software suite, which is the component that would have kernel-level access to a user's computer, is said not to collect or send any information to Riot Games, and Microsoft has signed this driver as part of their certification process. (The Riot Security Team, 2020). While this is a reasonable assurance by Riot Games, there is no guarantee that the system cannot send personally identifiable information to their servers despite statements that this does not occur. It is reasonable to assume any computer connected to the internet could send out any data stored on the computer if it is not adequately secured. Adding artificial intelligence, with its unclear methods for reaching specific conclusions, could exacerbate this concern as it may be tasked with determining which data it receives from a user's computer is relevant for the system to detect cheat software. It could be automatically sent to a remote server if it misidentifies personal data. This can be prevented through extensive ethical testing of these advanced models to ensure data is correctly identified and any sent data is encrypted and immediately removed using a second detection system at the server level.

## 6. ETHICAL COMPLICATIONS AND FUTURE RECOMMENDATIONS

Going back on the challenges in the previous section, there are Ethical Complications in having an Anti-cheat having full access to your computer. Below is an image called the ring kernel diagram, which illustrates the different privilege levels in computer architecture.

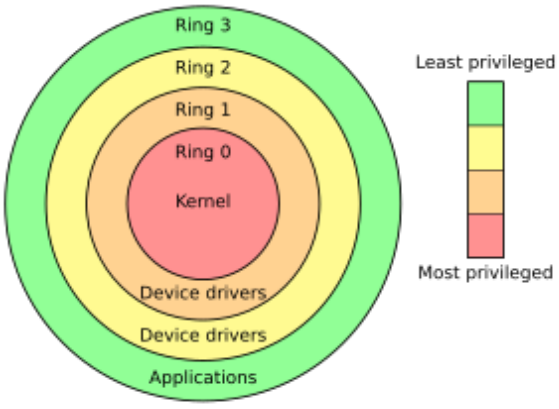


**Figure 1: Ring Kernel Diagram(Szefer, 2019)**

The innermost ring, Ring 0, represents the highest privilege level, typically where most operating system kernels operate. Ring 3, the outermost ring, has the lowest privilege and is where user applications run. Rings 1 and 2 are intermediate levels, often used for device drivers and services requiring more privileges than user applications but less than the kernel.

Going back to Ethical Complications, Anti-cheats ring 0 and ring 1 are some of the most debated topics currently in the anti-cheat realm. Examples of Kernal anti-cheat are Riot Games's Vanguard, Easy Anti-Cheat, and BattlEye. These anti-cheats have been criticized for their unrestricted access to all hardware and memory, making them a target for malware. In addition, this ring has access to sensitive information such as passwords, personal documents, and other private data. Any compromised part within the anti-cheat can be exploited to gain unauthorized access to the entire system. Anti-cheat developers must protect themselves from data breaches. Storing and collecting data at this kernel level must be done securely to prevent data breaches that could expose sensitive information. Ring 3 is also securitized in many aspects. It generally poses fewer risks than Ring 0, but the detection methods can be more resource-intensive and less invasive than kernel-level anti-cheats. However, this tradeoff often lowers the detection rate of sophisticated cheats, which causes many problems against cheaters for players. Developers face the challenges of balancing effective cheat prevention while maintaining users' trust and data security, which is critical for maintaining users' trust and integrity in these gaming environments.

Creators of anti-cheat software can take several steps to ensure it complies with high ethical, privacy, and security standards. Knowing the depth and level of access anti-cheat software can have in a user's computer, there is a much higher expectation for protecting sensitive information. To start, if the installation of anti-cheat software is a condition of installing the paired video game onto one's computer, there should be clearly explained information on where data will be monitored, how much of it is necessary for the software to ensure integrity within the game, and why this data collection is necessary. The software may not need highly privileged access to a user's computer, in which case the user can be given the option to opt out of this more intrusive form of access. After access is granted, users should continue to be aware of how the software interacts with data stored on their computers with regular transparency reports, providing detailed

information on the access and usage of data and if suspicious activity was found. These reports can also be used for auditing, assessing compliance with privacy standards, and identifying any vulnerabilities in security and privacy.

Ideally, this software should incorporate the principles of least privilege and only request the specific permissions required to detect cheating and nothing more. Root access and full administrative privileges should only be given if necessary. A modular approach can also be implemented where, depending on their specific functions, certain software components can be given access only to the data relevant to that particular component. Segmenting data based on sensitivity and necessity will complement this by reinforcing principles of least privilege and keeping personal data separate from game-specific data. Any processes undertaken by the software using higher privileges should be executed in isolated environments to reduce risk to the broader system, and aiming to ensure processes can execute properly without higher-level access should be the priority.

The anti-cheat software can serve as its attack surface and may be highly valuable to hackers due to its ability to gain deeper access to an operating system than other software, so ensuring strong authentication and encryption for secure access and transport of sensitive data is paramount. Incorporating an intrusion detection system (IDS) to monitor for unauthorized access attempts to the software or collected data can complement a complete security strategy.

As methods for cheating in online games advance over time and users become increasingly concerned with data privacy and security, strategies for implementing emerging technologies in anti-cheat software should be considered as a proactive way to combat cheating while maintaining data integrity, privacy, and security. Taking decentralized approaches to handling data removes the need to send data to remote servers for processing and reduces the resources required to secure it. First, as machine learning algorithms continue to be used in a modern anti-cheat software suite to train and reduce errors in cheat detection, concerns may arise regarding the methods for which this is accomplished. Instead of sending data to a centralized server to train a model, a federated learning approach can be incorporated. (Mammen, 2021). First introduced by Google in 2016, federated learning uses multiple devices to collaboratively train a machine learning model without sharing private data under the supervision of a central server. Each device trains the model locally and only communicates outward to send local updates to the server and keep raw data on the device, ensuring sensitive information remains private. The aggregated model updates from multiple devices are then sent back to the user device, with this process being repeated iteratively to improve the model continuously and, therefore, the accuracy and efficiency of the anti-cheat software.

Another technology known as blockchain can significantly enhance anti-cheat software's security, privacy, and functionality. Essentially, blockchain provides for the decentralization and immutability of data, meaning data is stored across a distributed network of notes. Once it is recorded, the data cannot be altered or deleted. All data transactions are recorded on a public blockchain that all participants can verify, and advanced encryption is used to protect data. This powerful technology can be used for storing logs of detected cheating incidents, reducing the risk of the logs being altered or deleted by a malicious party, and the distributed nature of blockchain allows secure storage of game actions and states. Player reports and audit trails provide transparency to the actions taken by the software, which is empowered by the blockchain, and zero-knowledge proofs can verify cheating without revealing sensitive information. The blockchain can also incentivize cheating detection with a bounty system that rewards players for reporting new cheating methods, rewarding cryptocurrency tokens to those who participate. It also allows the game’s online community to vote on suspected cheating incidents, the records of which can be stored securely on the blockchain and would increase the engagement of players in combating cheats rather than completely relying on the effectiveness of the software. Both emerging technologies discuss decentralization as a central tenet of their functionality, revealing a trend across the broader technology space.

## 7. CONCLUSIONS

The future of cheating detection in online gaming, particularly with the rise of AI, emphasizes the need for robust anti-cheat software to ensure fair

play. Especially in esports, identifying cheaters is increasingly vital as prize pools and online tournaments grow. It has been established that artificial intelligence and related technologies, such as machine learning, have revolutionized the world of combating cheating in online gaming, and innovation continues to blossom in this space. However, ensuring thorough testing and compliance with ethical and privacy standards remains top of mind for those wishing to create a fair and enriching gaming experience. Understanding why players may cheat can be an insightful method of informing new methods of cheating prevention that can be empowered by artificial intelligence and may warrant additional research. While much progress has been made by key industry players working to innovate in anti-cheat, there is still plenty of work to achieve these goals. Incorporating highly stringent standards for increasing the security and privacy of data used and transported by anti-cheat software, such as principles of least privilege, data segmentation, encryption, and regular auditing, are essential for an effective, reliable, and trustworthy AI-powered anti-cheat system. Emerging technologies like federated learning (FL) and blockchain can empower these systems to reinforce these principles and create the best and most reliable system possible. Additionally, for the future, our recommendations for companies in the direction of AI are to focus on Real-time monitoring and adaptive algorithms and implement AI technologies that monitor gameplay and adapt. Enhance gameplay data collection and analysis to train AI on these vast datasets. Finally, Ensure Strong security measures, incorporating encryption and authentication. By focusing on these areas, companies leverage AI to create a more secure and enjoyable gaming environment, enhance the player experience, and maintain the integrity of online gaming.

## 8. REFERENCES

Accenture. (2021). Global Gaming Industry Value Now Exceeds $300 Billion, *New Accenture Report Finds*. Retrieved June 5, 2024 from https://newsroom.accenture.com/news/2021/global-gaming-industry-value-now-exceeds-300-billion-new-accenture-report-finds

Ball, B. (2024). Marketing Video Games to Aging Demographics: A Generational Profile Analysis. *Digital Commons Lindenwood University* 893. Retrieved June 6, 2024 from https://digitalcommons.lindenwood.edu/theses/893

BattlEye. (n.d.). About: How We Came Here. *The Anti-Cheat Gold Standard.* Retrieved June 5, 2024 from https://www.battleye.com/about/

Buede, D., DeBlosis, B., Maxwell, D., McCarter, B., & Vienna, V. (2013). Filling The Need For Intelligent, Adaptive, Non-Player Characters. *Interservice/Industry Training, Simulation, and Education Conference*, (p. 10).

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes From The AI Frontier Modeling The Impact Of AI On The World Economy. *McKinsey Global Institute.* Retrieved June 5, 2024 from https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-AI-frontier-modeling-the-impact-of-ai-on-the-world-economy#/

Cox, A. J., McDonald, J., Engel, V. G., & Rhoten, M. (2019). International Patent Patent No. WO 2019/182868 A1.

Epic Games, Inc. (2024). About: Don't Bear With The Cheaters. *Epic Games Easy Anti-Cheat* Retrieved June 5, 2024 from https://www.easy.ac/en-US

Gbadegeshin, S. A., Natsheh, A. A., Ghafel, K., Tikkanen, J., Gray, A., Rimpiläinen, A., & Hirvonen, N. (2021). What Is An Artificial Intelligence (AI): A Simple Buzzword Or A Worthwhile Inevitability? *14th annual International Conference of Education, Research and Innovation*, (pp. 468-479). doi:10.21125/iceri.2021.0171

José Pedro Pinto, A. P. (2021). Deep learning and multivariate time series for cheat detection in video games. *Machine Learning*, 110(12), 3037-3057.

Jyothiraditya, P. (2024). Video Game Industry in the *US. International Journal of Science and Research Archive*, 11(1), 1257-1265. doi:10.30574/ijsra.2024.11.1.0194

Mammen, P. M. (2021). Federated Learning: Opportunities and Challenges. *ACM Conference (Conference'17)*. New York. doi:https://doi.org/10.48550/arXiv.2101.05428

Oguguo, P. C. (2024). Innovation and Intellectual Property Use in the Global Video Game Industry. *World Intellectual Property Organization (WIPO) Economic Research Working Paper Series* 85, 30.

Omdia. (2022). Faster internet speeds and more extensive data plans are exponentially increasing the number of players, but also

ISSN: 2473-4901
v10 n6202

broadening the opportunities for pirates and cheaters in the gaming industry. *Irdeto*. Retrieved June 5, 2024 from https://irdeto.com/news/irdeto-survey-reveals-increased-worry-of-cheating-and-tampering

Steam Support (n.d.). Valve Anti-Cheat (VAC) System. *Steam Corporate*. Retrieved June 3, 2024 from https://help.steampowered.com/en/faqs/view/571A-97DA-70E9-FF74

Sung Je, L., Jeong, E. J., Lee, D. Y., & Kim, G. M. (2021). Why Do Some Users Become Enticed to Cheating in Competitive Online Games? An Empirical Study of Cheating Focused on Competitive Motivation, Self-Esteem, and Aggression. *Frontiers in Psychology*, 12, Article 768825.

Szefer, J. (2019). Processor Architecture Security Part 1: Processor Security and Secure Processors. *ACACES Course on Processor Architecture Security*. Retrieved from https://caslab.csl.yale.edu/tutorials/acaces2019/acaces2019_proc_arch_sec_part-1.pdf

Team Modl.ai. (2024). How to Detect Cheaters in Video Games Using Machine Learning. *Modl.ai* Retrieved June 3, 2024, from https://modl.ai/detect-cheaters-using-ml/

The Riot Security Team. (2020). A Message About Vanguard From Our Security & Privacy Teams. *Riot Games*. Retrieved from https://www.riotgames.com/en/news/a-message-about-vanguard-from-our-security-privacy-teams