International Journal of Inventive Engineering and Sciences (IJIES)
ISSN: 2319-9598 (Online), Volume-12 Issue-6, June 2025

Anti-Cheat and Cybersecurity in eSports and Gaming: A Case Study

Sandeep Kulkarni, Minhaj Khan, S. Bulomine Regi, Dipans Verma, Tejas Tagad

Abstract: ***The esports and gaming industry is growing rapidly, which is drawing the attention of cybersecurity threats and cheating that compromise competitive integrity. This case study examines the implementation of anti-cheat technology and cybersecurity in the gaming ecosystem, focusing on its effectiveness and limitations. It highlights various types of cheating methods, such as aimbots, wallhacks, and account hijacking. It examines how game developers and tournament organisers can tackle these threats through technical and policy-based solutions. This case study will analyse the impact of cheating on player trust, game balance and viability of eSports. By studying real-world examples and current industry practices, this research will show the need for continuous innovation in cybersecurity to protect the digital competition.***

Keywords: eSports, Cybersecurity, anti-Cheat, Gaming, Technology, DDoS, VALVE, Kernel

Abbreviations:
ESIC: Esports Integrity Commission
VMICs: Virtual Machine Introspection Cheats
VAC: Valorant. the Anti-Cheat
DDoS: Distributed Denial-of-Service

I. INTRODUCTION

In recent years, esports has rapidly evolved from a casual leisure activity into a globally recognized competitive sport, driven by digital culture and technological innovation (Li, 2024). The esports industry in India began with LAN gaming cafes in the early 2000s and grew rapidly with the rise of mobile gaming and the advent of affordable internet. Esports has evolved into a global phenomenon, featuring multimillion-dollar tournaments, structured professional teams, and massive live audiences. Events like The International in 2021 offered over $40 million in prize money, while top organisations like Cloud9 and FaZe Clan operate with structures rivalling tradītional sports teams.

Manuscript received on 24 April 2025 | First Revised Manuscript received on 30 May 2025 | Second Revised Manuscript received on 05 June 2025 | Manuscript Accepted on 15 June 2025 | Manuscript published on 30 June 2025.
*Correspondence Author(s)
Dr. Sandeep Kulkarni*, Department of Computer Science, Ajeenkya D.Y. Patil University, Pune (Maharashtra), India. Email ID: sandeeppostdoc@gamil.com, ORCID ID: 0009-0009-2667-8374
Dr. Minhaj Khan, Department of Computer Science, Ajeenkya D.Y. Patil University, Pune (Maharashtra), India. Email ID: minhajkhan7786@gmail.com
Dr. S. Bulomine Regi, Department of Computer Science, Ajeenkya D.Y. Patil University, Pune (Maharashtra), India. Email ID: drregi23@gmail.com
Dipans Verma, Department of Computer Science, Ajeenkya D.Y. Patil University, Pune (Maharashtra), India. Email ID: dipans.verma@s.amity.edu.in
Tejas Tagad, Department of Computer Science, Ajeenkya D.Y. Patil University, Pune (Maharashtra), India. Email ID: tejas.tagad@adypu.edu.in

The COVID-19 pandemic accelerated the industry's growth, and with younger fans now entering the workforce, esports is experiencing continued economic expansion.

As online platforms expand, cheating techniques become increasingly sophisticated, and the intersection of cheating and cybersecurity has emerged as a critical concern in the gaming industry. According to [1], gamers may readily exploit flaws in gaming systems as digital environments evolve, often giving them unfair advantages. Due to social dynamics and security flaws, cheating habits can spread rapidly across online gaming communities as players observe and imitate dishonest behaviour. Cybersecurity solutions often fail to prevent cheating, which has severe consequences for game integrity and fairness. Furthermore, the absence of efficient regulatory frameworks to monitor and discourage cyber-cheating exacerbates these problems and remains a continuous challenge for game producers. In online gaming, cheating and cybersecurity have become significant issues, particularly in popular games like Fortnite, Valorant, and Counter-Strike: Global Offensive (CS: GO). The HAWK framework, which utilises machine learning to identify cheating activities, has shown promise in CS2 for detecting and mitigating unfair acts. With its Vanguard anti-cheat technology, which detects and stops unwanted changes at the kernel level, Valorant has achieved significant progress against cheaters. The creation of Virtual Machine Introspection Cheats (VMICs), which may evade conventional detection techniques, indicates that Fortnite still has cheating issues despite these attempts.

Technologies that prevent cheating are crucial for maintaining fair play in online gaming. Using kernel-level technology, Riot's Vanguard prevents cheats before they have an impact on gameplay in Valorant. The Anti-Cheat (VAC) technology from Valve uses behavioural analysis and signature scanning to identify and prohibit cheaters. In competitive settings, these techniques aid in preserving trust and minimising unfair advantages. Anti-cheat technologies must evolve as cheating techniques become increasingly sophisticated. They now play a role in broader cybersecurity issues, as well as game fairness.

The purpose of this study is to investigate the relationship between cybersecurity and anti-cheat technology in the gaming sector. It focuses on comprehending the effects of cheating in online gaming settings. The study examines the instruments and strategies employed to identify and prevent unfair gaming. It examines how cheating methods have evolved, along with their underlying technological

foundations. The aim is to assess how effectively existing security solutions address these attacks. It also considers the difficulties developers encounter in upholding fair play. The study assesses the broader ramifications for user safety and trust. All things considered, it highlights the importance of robust cybersecurity in gaming.

II. LITERATURE REVIEW

A. Types of Cheating in Online Gaming

Online game cheating has become a recurring issue, with individuals employing various tactics to gain unfair advantages. Among the most popular software-based cheats are aimbots, which automatically lock onto opponents' targets, and wallhacks, which let players see through solid obstacles. These exploits are perilous in competitive settings since they can skew player rankings and detract from other players' experiences, claims [2]. Furthermore, boosting—the practice of low-skilled players paying high-ranked ones to inflate their rankings has become an increasingly significant issue [3]. discovered that by rewarding players who depend on outside assistance rather than their abilities, boosting not only compromises the integrity of ranking systems but also hurts the game's fairness.

Using automated software to perform monotonous tasks in a game is known as botting, and it can be especially detrimental in games that rely on resource farming or grinding. The prevalence of botting in multiplayer online role-playing games (MMORPGs), where automated bots provide players an unfair advantage by automating the game's time-consuming tasks, has been brought to light. Similarly, developers continue to face the difficulty of players taking advantage of unexpected game mechanics or glitches, which is known as exploiting game design weaknesses. According to [4], these "glitches" are frequently taken advantage of in high-stakes situations, which makes it challenging to keep the game balanced.

Along with these software-based tricks, Distributed Denial-of-Service (DDoS) attacks are being increasingly utilised to interfere with online gaming by flooding game servers with traffic, which causes latency or crashes. The increasing use of DDoS attacks in competitive gaming, where players attempt to interfere with opponents' games to gain a tactical advantage, was highlighted. In addition to impairing gameplay, this type of cheating puts online platforms' and game creators' security procedures to the test.

B. Motivations and Social Impact of Cheating

There are many different reasons why people cheat, including societal and personal ones. According to online gamers, they are more prone to cheat if they have greater levels of competitive drive, less self-control, and more hostility. This is consistent with earlier studies that hypothesised that in competitive gaming situations, cheating is frequently motivated by a desire for prestige and recognition. Furthermore, a significant contributing factor to cheating behaviour is social influence. Players are more inclined to cheat when they witness others cheating, especially in settings where cheating is accepted or viewed as a way to obtain an advantage over rivals.

Furthermore, research on rationalization by indicates that gamers perpetuate a loop of dishonesty in gaming groups by using the belief that others are just as dishonest as they are to defend their dishonest behavior. Additionally, it is pointed out that the anonymity offered by online gaming platforms lowers accountability by enabling gamers to engage in dishonest behaviour without fear of serious social or legal repercussions. These results demonstrate the intricate interactions that exist between social dynamics, personal motivations, and the broader culture of cheating within gaming groups.

C. Advanced Cheating Techniques

Traditional software hacks are no longer the only way to cheat in online games. The kernel-level anti-cheat system Vanguard, implemented by Riot Games in Valorant, is a noteworthy example. By continuously monitoring system activities, Vanguard detects cheaters, such as aimbots and wallhacks, at the fundamental system level [5]. Such exploits are now much less common thanks to this strategy, and the only cheats left are simple triggerbots. However, players' privacy concerns have been raised by the implementation of kernel-level drivers, underscoring the need to strike a balance between user privacy and efficient detection of cheats.

D. Cybersecurity Threats in Esports

Numerous cybersecurity risks, including DDoS attacks, phishing, account theft, and espionage, pose significant threats to esports firms. DDoS attacks are designed to overload servers, resulting in outages and interfering with broadcasting or gaming services. For example, such attacks resulted in match cancellations for the League of Legends Champions Korea (LCK), causing serious harm to its reputation. Since attackers aim to steal private data or in-game assets, phishing efforts are common, with 55% of esports stakeholders classifying them as a moderate or severe issue. The industry's susceptibility to cyberattacks is further demonstrated by the fact that 81% of esports companies recognise the growing need for robust security measures (Lauver, 2021).

E. Regulatory Efforts and Industry Responses

Organizations like the Esports Integrity Coalition (ESIC) were founded in response to the growing difficulties in encouraging moral conduct and fighting corruption in the esports sector. To maintain the integrity of esports tournaments, the ESIC tackles problems including match-fixing, software cheating, DDoS attacks, and doping. Despite these initiatives, leagues and organisations are not required to participate in ESIC, resulting in inconsistent enforcement and regulation throughout the sector.

F. Technological Innovations in Anti-Cheat Systems

Innovative solutions are being developed to counter sophisticated cheating techniques. For instance, the HAWK framework successfully detects different forms of cheating in first-person shooter games, such as CS2,

by simulating human expert recognition processes using machine learning approaches. Studies have demonstrated that HAWK captures cheaters who could evade conventional detection techniques with promising efficiency and minimal performance overhead. In a similar vein, AI-powered systems utilise face recognition technology to track player activity and ensure that only authorised players participate. The integrity of esports competitions can be improved by these technologies' ability to identify unapproved players, monitor player presence, and prevent the use of dishonest tactics during games. The dynamic nature of internet gaming demands constant improvements in cybersecurity and anti-cheat solutions. To protect the integrity of esports and online gaming communities, game creators, cybersecurity specialists, and regulatory agencies must continue to collaborate despite the notable progress that has been accomplished.

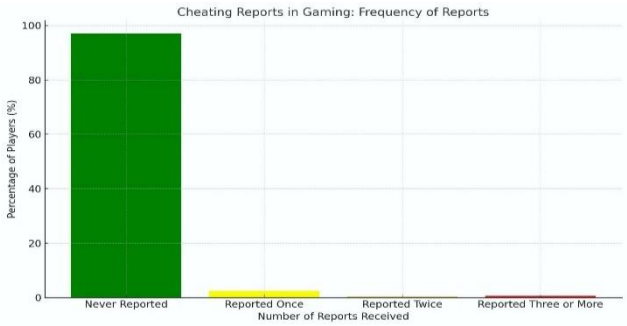
III. METHODOLOGY

The study employs a qualitative case study methodology to investigate cybersecurity and anti-cheat technology in the gaming industry, with a specific focus on the esports sector. The research draws on a range of data sources, including interviews, content analysis, news articles, and developer updates.

A. Case Studies and Data Analysis

i. Case Study 1: Valorant (Riot Games)

Riot Games' implementation of Vanguard, a kernel-level anti-cheat system, has been a subject of much attention. A graph will be plotted using reports published by Riot Games (Chamberlain, P. 2020)



Graph 1 Cheating Reports in Gaming

After the Vanguard (ACS) implementation, 97% of players never received a single report. Approximately 3% of players who have been reported for cheating have been reported by more than 80% of them, with only a single player reporting them. Fewer than three players have reported a score of 90%.

In other words, only 0.6% of gamers have been reported for cheating more than once, and only 0.3% have been reported for cheating three or more times. However, there is not a perfect correlation between reports and cheaters; not all cheaters are reported before they are banned, and many reported players are innocent. As of right present, just 60% of people with 20 reports are banned following review, and only 53% of banned cheats were reported prior to their ban.

ii. Case Study 2: Counter-Strike 2(Valve)

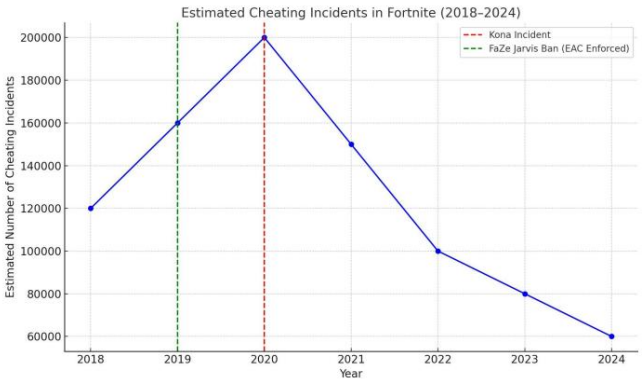
Valve's approach to dealing with cheating through its Steam platform and third-party anti-cheat systems, such as FACEIT and ESEA.

Table 1: Cheat Detection Rates on CS2 Platforms

Platform	Detection Rate (%)	Year Introduced	Key Features
Steam	30%	2012	VAC, regular updates
Faceit	90%	2013	Professional anti-cheat tools
ESEA	85%	2009	Dedicated server-side anti-cheat

iii. Case Study 3: Fortnite (Epic Games)

Fortnite uses Easy Anti-Cheat (EAC) to fight cheating. A graph will be plotted using the available resources and findings on cheaters' detection by EAC.

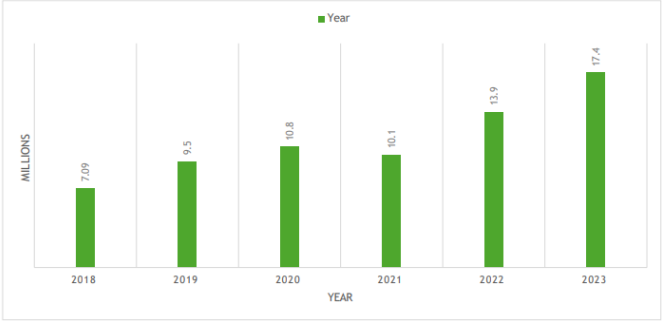


Graph.2 Estimated Cheating Incidents in Fortnite (2018-2024)

This graph shows the number of cheating incidents in Fortnite from 2018 to 2024. 2020 was the peak year, with 200,000 players reported for cheating and subsequently banned from the game. However, advancements in the anti-cheat system have reduced this rate over the years [6].

iv. Case Study 4: Esports Tournament DDoS Attacks

Examining incidents of DDoS attacks in esports tournaments, the data can be illustrated using a bar chart that shows the frequency of DDoS incidents in games.



Graph.3 Esports Tournament DDoS

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Table 2: Comparative Analysis of DDoS Attacks on Gaming Industry (2017–2024)

Year	Source	% of DDoS Attacks Targeting Gaming	Observation
2017	Statista	79%	Extremely high concentration of DDoS attacks aimed at gaming shows gaming as a prime target during this period.
2019	Bitdefender	35.92%	Significant drop compared to 2017, possibly due to improved mitigation strategies or a shift in attacker focus.
2024	Security Magazine	49%	Increase from 2019, indicating a resurgence in targeting gaming platforms, likely due to growing esports events and online infrastructure dependency.

Table 3: Comparison Summary Table

Case Study	Anti-Cheat System	Type	Detection Focus	Data Comparison Metric
Valorant	Vanguard	Kernel-level	Cheating reports	Pre/Post graph (Graph 1)
CS2(Steam)	VAC	Standard	Detection rate	Cross-platform table (Table 1)
CS2 (FACEIT)	FACEIT AC	External	High sensitivity	Cross-platform table (Table 1)
Fortnite	Easy Anti-Cheat	Embedded	Cheating frequency	Trend graph (Graph 2)
Tournaments	N/A	Network-level	DDoS disruptions	Yearly incident comparison(Graph 3)

IV. CASE DESCRIPTION

A. Case study: The "Forsaken" Cheating Scandal in CS: GO (2018)

i. Case:

During an official match at the ESL India Premiership Fall Finals in October 2018, Nikhil "forsaken" Kumawat, a professional CS: GO player for India's OpTic India team, was discovered to be employing an aimbot. The cheat, which gave him automatic targeting skills and was placed in an application called "word.exe" on his computer, was a clear infraction of esports fair-play regulations [7].

ii. Who Was Affected:

- Players & Teams – OpTic India was dissolved after the incident. Forsaken's teammates, who claimed to be unaware of the cheating, were eliminated from the tournament.
- Tournament Organizers (ESL) – ESL faced intense criticism for not detecting the cheat earlier and for failing to disqualify the team immediately during the event [8].
- The Indian CS: GO Scene – The scandal significantly damaged the reputation of Indian esports, casting doubt on the credibility of other local players and organizations.
- OpTic Gaming (Global Organization) – The parent company's image also suffered globally, as the controversy reflected poorly on its internal team management.

iii. Discovery of the Cheating:

The cheat was discovered in real-time during the match, when tournament administrators noticed suspicious aiming behaviour. Upon closer inspection, they accessed his PC and found the cheat software disguised as a text-related executable. Forsaken attempted to delete the file in front of officials, further incriminating himself.

"He tried to alt-tab and delete the file while the admins were checking his PC."

-Dust2 India, 2018 (source)

iv. Action Taken:

- Immediate Ban: Forsaken was banned mid-tournament by ESL and removed from the venue.
- OpTic Disbands Team: OpTic Gaming disbanded its Indian roster entirely after the incident.
- Lifetime Ban: Forsaken was handed a five-year ban from all ESL and ESIC-affiliated events (not technically "lifetime" but effectively career-ending at his level) [9].
- VAC Ban: His Steam account was permanently banned via Valve Anti-Cheat (VAC).

"Following a thorough investigation, ESIC has decided to ban Nikhil's 'forsaken' Kumawat from all esports competitions for five years."

v. Impact on the Game/Esports:

- Loss of Trust: The scandal severely damaged the credibility of India's CS: GO esports community, with major organizations becoming cautious about investing in South Asian rosters.
- Policy Changes: ESL increased its scrutiny of tournament setups, with more rigorous anti-cheat enforcement during LAN events.
- Industry Awareness: The case became a reference point for the need for real-time cheat detection in LAN environments.

"This was not just a player cheating; it was a player compromising the integrity of an entire region's growing esports scene."

V. ANALYSIS & DISCUSSION

A. Effectiveness of the Anti-Cheat Response

The abandoned incident revealed serious flaws in LAN-level cheat detection during professional matches. Although reliable for online gameplay, Valve's VAC system was unable to account for LAN settings where players used their hardware. ESL's initial inability to identify the cheat in pre-match scans pointed to weaknesses in cybersecurity procedures at the tournament level. However, as soon as suspicious activity was noticed, tournament administrators took decisive action. They checked the player's device, verified that unlicensed software was being used, and pulled him from the game in the middle of it. Although they were reactive rather than proactive, the following measures — player ban, team disbandment, and policy updates — demonstrated a good response to the incident. The long-term effect served

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

as a warning for more stringent LAN enforcement measures [10].

B. Was Cybersecurity Handled Well?

In this instance, cybersecurity was only half successful. On the one hand, additional harm was avoided because the cheat was discovered and addressed during the competition. The ease with which the cheat evaded detection technologies, however, emphasizes the necessity of more stringent pre-game equipment inspections and uniform software configurations. Furthermore, a vulnerability was exploited by allowing users to compete on their computers without adequate real-time monitoring.

Following the incident, ESL and OpTic made it plain that they would not tolerate cheating by banning and disbanding the involved team. These actions were essential to restoring credibility to the competition and the area.

C. Impact on User Trust and Game Performance

The controversy among severely damaged trust:
1)Teams and players who questioned the tournament system's fairness and were concerned about unfair play. 2) Following the incident, many fans and audiences had doubts about the Indian esports sector. 3) Organisations and sponsors grew reluctant to invest in fresh or untested local talent pools. 4)The controversy obscured respectable competitors who were playing fairly and compromised the tournament's legitimacy from a performance standpoint. Additionally, it compelled companies to make larger future investments in cybersecurity and player verification.

D. Conclusion of Analysis

The *Forsaken* case highlighted the cybersecurity flaws in professional esports when oversight is incomplete. It was a pivotal moment in Indian esports history, marking the introduction of stricter anti-cheat regulations. Even if more proactive detection is now possible with Riot's Vanguard (Valorant) or FACEIT's proprietary solutions, the abandoned controversy serves as a warning about what occurs when system-level security and real-time cheat detection are not given priority.

VI. FINDINGS

A. Key Observations from the Case:

i. Even in High-Stakes, LAN Environments, Cheating Can Occur: The forsaken case demonstrated that, despite their reputation for security, LAN events are susceptible to cheating if appropriate cybersecurity measures and pre-game checks are not implemented.
ii. Reactive Anti-Cheat Measures Are Inadequate: Although the tournament organisers identified and addressed the cheat during the match, the original inability to prevent the cheat from loading suggests that proactive LAN security tools are lacking.
iii. Serious Repercussions Act as Potent Disincentives: The community was powerfully reminded that cheating has serious repercussions that go beyond personal penalties, including automatic disqualification, team disbandment, and a five-year ESIC ban.
iv. Damage to Regional Growth and Trust: The lawsuit hurt the credibility of reputable players in the area and delayed potential investments in India's nascent esports ecosystem.
v. Absence of LAN Anti-Cheat Standardized Solutions: The lack of uniform security procedures among tournament hosts was highlighted by the use of private setups that lacked safe boot environments or validated software.

B. Effect on Industry:

i. Transition to Proactive and Kernel-Level Anti-Cheat Tools: In response to such instances, firms such as Riot Games have implemented kernel-level anti-cheat systems (Vanguard), which operate continually in the background to stop cheating at the system level even before the game is released.
ii. Increased Attention to LAN-Specific Security Protocols: Tournament organisers are using stricter hardware controls, player machine forensic analysis, and real-time behavioural surveillance during competitive events more frequently.
iii. Professionalization of Esports Compliance: Groups like the Esports Integrity Commission (ESIC) are gaining influence and establishing international standards for cybersecurity, integrity, and discipline in esports competitions.
iv. Growing wants for Accountability and Transparency: When cheating occurs, fans and stakeholders now demand thorough explanations and supporting documentation, prompting more public declarations, inquiries, and in-depth analyses from game developers and tournament organisers.
v. Understanding Regional Fragility: Scandals can have a significant impact on emerging regional scenes. Scandals can result in investor withdrawal, suspicion from international organizations, and slower progress, as was the case in India after the crisis. This emphasizes the necessity of strict compliance from the beginning.

VII. CONCLUSION

A. The Importance of Anti-Cheat and Cybersecurity in the Future of Gaming:

The “Forsaken” cheating scandal highlights how important strong cybersecurity and anti-cheat systems are to preserving the integrity of professional gaming. The stakes are bigger than ever before for players, teams, organisers, and developers as esports continue to gain popularity and income. In addition to interfering with fair play, cheating undermines user confidence, tarnishes brand reputation, and compromises the long-term sustainability of the competitive ecosystem. It is therefore imperative for the credibility and long-term viability of contemporary esports to guarantee safe, cheat-free conditions. Proactive, system-level anti-cheat technologies that can identify and prevent cheating before and during gameplay must be given top priority by game creators and tournament organisers to

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

ensure competitive gaming in the future. To further minimize discrepancies and vulnerabilities, uniform security procedures for LAN events must to be implemented worldwide. Detecting suspicious activity can also be aided by post-match analysis with sophisticated technologies and real-time surveillance. Restoring and preserving player and audience trust also depends on being transparent about how cheating occurrences are handled, primarily through public reports and regular disciplinary measures. Global norms for fair play and enforcement can be further established through cooperation with regulatory organizations like the Esports Integrity Commission (ESIC). This study does have some drawbacks, however. Access to proprietary data was not possible due to internal developer procedures and the sensitive nature of anti-cheat systems. A large portion of the study is based on interviews, public remarks, and third-party reporting, all of which may be biased or superficially technical. Furthermore, although informative, the emphasis on a single instance from the Indian esports community would not adequately represent the variety of cybersecurity techniques found in other games or geographical areas. Notwithstanding these drawbacks, the example provides valuable insights into the challenges and advancements necessary to ensure the survival of esports.

B. Recommendations for Game Developers and Esports Organizers:

i. Use Proactive, System-Level Anti-Cheat Tools: Developers ought to spend money on cutting-edge kernel-level programs (like Riot's Vanguard) that can identify cheats not only when a game is being played but even before it launches.

ii. Standardise Tournament Security Procedures: Esports organizers are required to implement consistent LAN security protocols, such as machine checks, secure boot settings, and limitations on personal devices.

iii. Improve Monitoring in Real Time During Contests: To identify suspect conduct in real time, particularly during high-stakes tournaments, use behavioural analytics and AI-driven cheat detection.

iv. Boost Community Transparency: Open communication regarding security updates, ban waves, and cheat mitigation techniques might help to preserve public trust.

v. Support Integrity Organizations Like ESIC: Independent regulators have the authority to impose sanctions and contribute to the standardisation of international esports integrity standards.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Li, J. (2024). The Rise of E-sports: The Transformation from Leisure Entertainment to a Global Sports Phenomenon. In Proceedings of the 2nd International Conference on Social Psychology and Humanity Studies. DOI: https://doi.org/10.54254/2753-7048/43/20240592
2. Zhang, J., Sun, C., Gu, Y., Zhang, Q., Lin, J., Du, X., & Qian, C. (2024). Identify As A Human Does: A Pathfinder of Next-Generation Anti-Cheat Framework for First-Person Shooter Games, in arXiv preprint arXiv:2409.14830. https://arxiv.org/abs/2409.14830
3. Warren, T. (2024, November 4). Valorant is Winning the War Against PC Gaming Cheaters. In The Verge. https://www.theverge.com/2024/11/4/24283482/valorant-is-winning-the-war-against-pc-gaming-cheaters
4. Aviv, A. J., Byrne, M. D., & Bellovin, S. M. (2009). An Investigation of Cheating in Online Games. In IEEE Security & Privacy, 7(5), 19–25. DOI: https://doi.org/10.1109/MSP.2009.60
5. Breen, E. (2020). The Impact of Cheating and Fraud in Gaming Ecosystems. In Journal of Digital Ethics, 18(2), 205–223. https://quago.io/blog/the-impact-of-cheating-in-online-gaming/
6. Huang, C., & Chen, C. (2019). Boosting in Online Gaming: An Analysis of Cheating and Its Impact. In International Journal of Game Studies, 24(3), 155–171.
7. Parks, R., Lowry, P. B., Wigand, R. T., & Agarwal, N. (2017). Why Students Engage in Cyber-Cheating Through a Collective Movement: A Case of Deviance and Collusion. In Journal of Global Information Management, 25(1), 1–21. DOI: https://doi.org/10.4018/JGIM.2017010101
8. Liao, Y., Zheng, Z., & Wang, C. (2020). Understanding and Mitigating Botting in Online Multiplayer Games. In Computers in Human Behaviour, 103, 188–197. DOI: https://doi.org/10.1016/j.chb.2019.09.027
9. Zengler, T. (2021). What is the Deal with Anti-Cheat Software in Online Games? In Wired. https://www.wired.com/story/kernel-anti-cheat-online-gaming-vulnerabilities
10. Clyde & Co. (2024). The Rise of Cybersecurity Threats in Esports: Legal Implications and Risk Management Approaches. In Clyde & Co Insights. https://www.clydeco.com/en/insights/2024/11/the-rise-of-cybersecurity-threats-in-esports

AUTHOR'S PROFILE

Dr. Sandeep Kulkarni is an accomplished academic and technologist with a Ph.D. and Dsc(Post Doctorate) in Computer Science. He currently serves as an Assistant Professor at Ajeenkya DY Patil University, Seamedu, Pune, where he leverages over five years of industry experience from leading firms such as Capgemini and Oracle. His expertise spans Java technologies, WordPress, front-end development, and data science algorithms. He has co-guided one PHD student under his supervision. Dr. Kulkarni has authored 60 publications and 13 Books, reflecting his significant contributions to fields such as machine learning, cybersecurity, and AI integration in holography. His interdisciplinary approach bridges academia and industry, fostering innovation in emerging technologies.

Dr. Minhaj Khan MSc, MTech, PHD is an Assistant Professor in the Department of Computer Applications at Integral University, Lucknow, with

over seven years of teaching experience. He holds a strong academic and professional background, specialising in cloud computing. Dr. Khan is dedicated to imparting quality education and fostering a deep understanding of emerging technologies among students. His expertise lies in designing and delivering effective course content that bridges theoretical knowledge with practical application. Passionate about academic excellence and technological innovation, he actively contributes to curriculum development, student mentorship, and research in cloud computing. Dr. Khan aims to inspire future professionals and drive impactful advancements in the field of computer science.

Dr. S. Bulomine Regi M.Com., M.Phil., SET., Ph.D. in Commerce., M.B.A (HR)., SET., Ph.D in Management Studies., PGDBA., M.Sc. (Psy)., M.A (Public Administration)., M.A. Tourism & Travel Studies., M.A Women Studies., is a distinguished academician and researcher in commerce and management. Serving as Assistant Professor at St. Mary's College (Autonomous), Thoothukudi, Tamil Nadu, India. She has 10 years of teaching experience. With over 100 research publications and multiple international presentations, her work focuses on behavioural studies on banking, digital payments, and occupational stress. She has received numerous awards, serves on editorial boards, and mentors six Ph.D. scholars and three scholars who have been awarded a Ph.D. in Commerce. She has delivered talks as a resource person for more than 100 events. Her global research contributions and consultancy services reflect her commitment to education, innovation, and social impact, making her a renewed academician.

Dipans Verma is a dedicated scholar currently pursuing a Ph.D. at Amity University, Mumbai. With a strong academic background, he holds an M.Tech in Industrial Mathematics with Computer Applications and a B.Sc. in Mathematics. His academic journey reflects a deep passion for mathematical sciences and technology. Alongside his doctoral studies, Dipans is actively engaged in a data science project that aims to enhance his expertise and contribute to innovative, real-world solutions. His research interests lie at the intersection of mathematics and data-driven technologies, and he is committed to continuous learning and academic excellence. Dipans strives to make meaningful contributions through research, analysis, and application of advanced computational methods.

Tejas Tagad is a third-year BCA student specializing in Artificial Intelligence and Machine Learning. He is skilled in Python programming, machine learning algorithms, and data analysis techniques. With a strong academic foundation and hands-on project experience, Tejas has demonstrated the ability to work effectively in team environments. He has contributed to multiple collaborative projects, showcasing both technical expertise and communication skills. Tejas is a quick learner, always eager to explore emerging technologies and deepen his understanding of the AI and ML domains. Passionate about continuous improvement and innovation, he aims to leverage his knowledge to solve real-world problems and make meaningful contributions in the field of artificial intelligence.