International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

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

Dr. Sandeep Kulkarni[(1)], Tejas Tagad[(2)], Yogesh Choudhary[(3)], Divya Sutar[(4)]
Assistant Professor, Department of Computer
Science, Pune, Maharashtra
BCA, Student1, Department of Bachelors of Computer Applications
BCA, Student2, Department of Bachelors of Computer Applications
BCA, Student3, Department of Bachelors of Computer Applications
Ajeenkya DY Patil University
Lohgaon, Airport Rd, Charholi Budruk, Pune, Maharashtra
Ajeenkya D Y Patil School of Engineering ,Ajeenkya D Y Patil University , Pune
Department of Bachelors of Computer Applications
D Y Patil Knowledge City, Charholi Road Lohegaon Pune, Maharashtra 412105

Abstract - Esports and gaming industry is growing day by day which is grabbing attention of cybersecurity threats and cheating that affect competative integrity. This case study investigate the use of anti-cheat technology and cybersecurity implemented in gaming ecosystem focusing on effectiveness and limitations.It highlights various types of cheating methods such as aimbots wallhack and account hijacking and examine how game devolopers and tournament orgnizers can tackle this threats by technical and policy based solutions. This case study will analyze the impact of cheating on player trudt, game balance and viablity of eSports. By studying real world examples and current industry practices this research will show the need of continouse innovation in cybersecurity to protect the digital competition.

This study explores the growing challenges of cheating and cybersecurity threats in the rapidly expanding esports and online gaming industry. As competitive gaming gains global popularity, maintaining fairness and integrity has become increasingly difficult due to the emergence of sophisticated cheating techniques such as aimbots, wallhacks, botting, and account hijacking. In addition, cybersecurity threats like Distributed Denial-of-Service (DDoS) attacks, phishing, and account breaches further compromise the gaming ecosystem.

The research adopts a qualitative case study approach, analyzing major games such as Valorant, Counter-Strike 2, and Fortnite, along with real-world esports incidents like the "Forsaken" cheating scandal. It evaluates the effectiveness of modern anti-cheat systems, including kernel-level solutions like Vanguard, signature-based systems like VAC, and third-party platforms such as FACEIT and ESEA. The study also examines the evolution of cheating techniques and the ongoing arms race between cheat developers and security systems.

Findings indicate that advanced anti-cheat technologies significantly reduce cheating incidents but are not entirely foolproof. While proactive systems like kernel-level anti-cheat tools show higher effectiveness, they raise concerns regarding user privacy and system access. Additionally, the research highlights the importance of strong cybersecurity frameworks in preventing external threats such as DDoS attacks, which continue to target esports events.

The study concludes that maintaining trust, fairness, and long-term sustainability in esports requires continuous innovation in anti-cheat technologies, standardized tournament security protocols, and collaboration between developers, organizers, and regulatory bodies. Despite certain limitations in data accessibility, this research emphasizes the critical need for robust cybersecurity strategies to safeguard the future of competitive gaming.

Keywords: eSports, cybersecurity, anti-cheat, gaming, technology ,DDos, VALVE, Kernel

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 affordable internet (Hero Vired, 2023). eSports has transformed into a global phenomenon with 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 organizations like Cloud9 and FaZe Clan operate with structures rivaling traditional sports teams (Heath, 2023). The COVID-19 pandemic accelerated the industry's growth, and with younger fans now entering the workforce, esports is continued economic expansion (Schudey et al., 2023).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

As online platforms expand cheating techniques become more sophisticated, cheating and cybersecurity have emerged as critical concerns in the gaming industry. According to Aviv, Byrne, and Bellovin (2009), gamers may readily take advantage of flaws in gaming systems as digital surroundings change, frequently giving them unfair advantages. Due to social dynamics and security flaws, cheating habits can spread swiftly across online gaming communities as players see and imitate dishonest behavior (Kim & Tsvetkova, 2021). Cybersecurity solutions frequently fall short in preventing cheating, which has serious consequences for game integrity and fairness (Parks et al., 2017). Furthermore, the absence of efficient regulatory frameworks to keep an eye on and discourage cyber-cheating makes these problems worse and is a continuous challenge for game producers (Aviv et al., 2009).

In online gaming, cheating and cybersecurity have grown to be major issues, especially in well-known games like Fortnite, Valorant, and Counter-Strike: Global Offensive (CS2). The HAWK framework, which use machine learning to identify cheating activities, has demonstrated potential in CS2 for detecting and reducing unfair acts (Zhang et al., 2024). With its Vanguard anti-cheat technology, which detects and stops unwanted changes at the kernel level, Valorant has achieved significant progress against cheaters (Warren, 2024). The creation of Virtual Machine Introspection Cheats (VICs), which may avoid conventional detection techniques, shows that Fortnite still has cheating issues in spite of these attempts (Karkallis & Blasco, 2025).

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 (Warren, 2024). The Anti-Cheat (VAC) technology from Valve uses behavioral analysis and signature scanning to identify and prohibit cheaters (Valve, 2023). In competitive settings, these techniques aid in preserving trust and minimizing unfair advantages. Anti-cheat technologies need to change as cheating techniques get more sophisticated. They now play a part in more general 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 on online gaming settings. The study looks at the instruments and strategies used to identify and stop unfair gaming. It looks into how cheating methods have changed over time and their technological underpinnings. Evaluating how well existing security solutions handle these attacks is the aim. It also takes into account the difficulties developers encounter in upholding fair play. The study assesses the wider ramifications for user safety and trust. All things considered, it emphasizes how crucial robust cybersecurity is for gaming.

LITRETURE REVIEW

Types of Cheating in Online Gaming

Online game cheating has become a recurring problem, with individuals using a variety of strategies to obtain 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 especially dangerous in competitive settings since they can skew player rankings and detract from other players' experiences, claims (Trend Micro,2019). Furthermore, boosting—the practice of low-skilled players paying high-ranked ones to inflate their rankings—has become an increasingly significant issue. Huang and Chen (2019) discovered that by rewarding players who depend on outside assistance rather than their own abilities, boosting not only compromises the integrity of ranking systems but also has an adverse effect on the game's fairness.

Using automated software to carry out monotonous chores in a game is known as botting, and it may be especially harmful in games that depend on resource farming or grinding. The prevalence of botting in multiplayer online role-playing games (MMORPGs), where automated bots provide players an unfair edge by avoiding the game's time-consuming duties, was brought to light by (Liao et al,2020). 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 (Chen and Ong, 2016), these "glitches" are frequently taken advantage of in high-stakes situations, which makes it difficult to keep the game balanced.

Along with these software-based tricks, Distributed Denial-of-Service (DDoS) assaults are being utilized more often to interfere with online gaming by flooding game servers with traffic, which causes latency or crashes. The increasing usage of DDoS assaults in competitive gaming, when players try to interfere with opponents' games in order to obtain a tactical edge, was highlighted by Quago (2023). In addition to impairing gameplay, this type of cheating puts online platforms' and game creators' security procedures to the test.

Motivations and Social Impact of Cheating

There are many different reasons why people cheat, including societal and personal ones. According to Lee et al. (2021), online gamers are more prone to cheat if they have greater levels of competitive drive,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

less self-control, and more hostility. This is consistent with earlier study by Kuss et al. (2021), who hypothesized that in competitive gaming situations, cheating is frequently motivated by a desire for prestige and recognition. Furthermore, a major contributing factor to cheating behavior is social influence. Players are more inclined to cheat when they witness others cheating, according to Cheng et al. (2019), especially in settings where cheating is accepted or viewed as a way to obtain an advantage over rivals.

Furthermore, research on rationalization by Chen and Wu (2015) 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 own dishonest behavior. Additionally, Breen (2020) pointed out that the anonymity offered by online gaming platforms lowers accountability by enabling gamers to conduct dishonestly without fear of serious social or legal repercussions. These results demonstrate the intricate interactions that exist between social dynamics, personal motives, and the larger cheating culture in gaming groups.

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 like aimbots and wallhacks at the fundamental system level (O'Connor, 2024). 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 necessity of striking a compromise between user privacy and efficient cheat detection (Zengler, 2021).

Cybersecurity Threats in Esports

Numerous cybersecurity risks, such as DDoS attacks, phishing, account theft, and espionage, are present for esports firms. DDoS assaults are designed to overload servers, resulting in outages and interfering with broadcasting or gaming. For example, such attacks resulted in match cancellations for League of Legends Champions Korea (LCK), causing serious harm to their reputation (Clyde & Co, 2024). 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 serious issue (Lauver, 2021). The industry's susceptibility to cyberattacks is further shown by the fact that 81% of esports companies recognize the growing necessity for strong security measures (Lauver, 2021).

Regulatory Efforts and Industry Responses

Organizations like the Esports Integrity Coalition (ESIC) were founded in response to the growing difficulties in order to encourage moral conduct and fight corruption in the esports sector. With the goal of maintaining the integrity of esports tournaments, ESIC tackles problems including match-fixing, software cheating, DDoS attacks, and doping (Smith, 2016). Despite these initiatives, leagues and organizations are not required to participate in ESIC, which results in inconsistent enforcement and regulation throughout the sector (Czegledy, 2021).

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 cheat in first-person shooter games like CS2 by simulating human expert recognition processes using machine learning approaches. Studies have demonstrated that HAWK captures cheaters who could avoid conventional detection techniques with promising efficiency and little performance overhead (Zhang et al., 2024). In a similar vein, AI-powered systems use face recognition technology to track player activity and make sure that only allowed players participate. The integrity of esports competitions can be improved by these technologies' ability to identify unapproved players, keep an eye on player presence, and stop the employment of dishonest tactics during games (Reply, 2020).

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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

PROPOSED METHODOLOGY

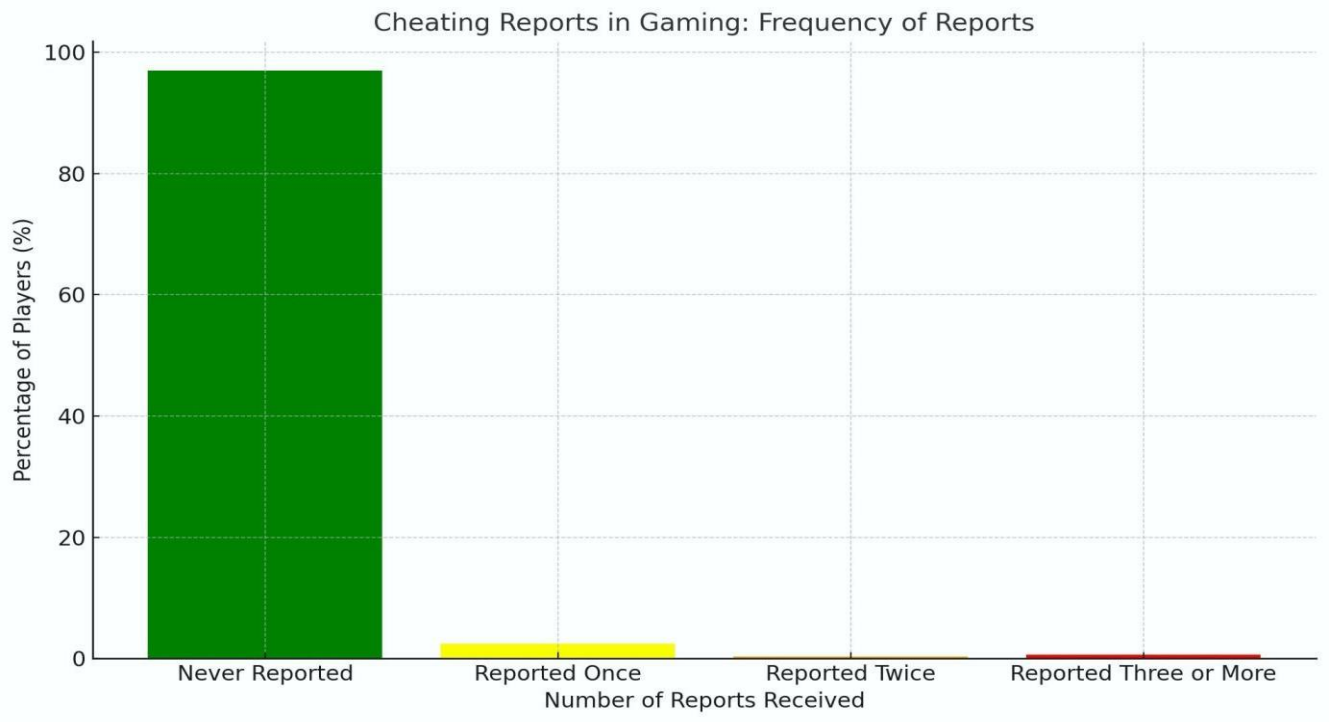
The study uses a qualitative case study methodology to investigate cybersecurity and anti-cheat technology in the game business, specifically in the esports space. The research relies on a variety of data sources, such as interviews, content analysis, news articles, and developer updates.

Design of Research

Case Studies and Data Analysis

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 vangaurd(ACS) implemetation 97% of the players never even received a single report. 3% of players that have been reported for cheating, more than 80% of them have only ever been reported by a single player. 90% have been reported by fewer than 3 players.

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 isn't 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.

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.

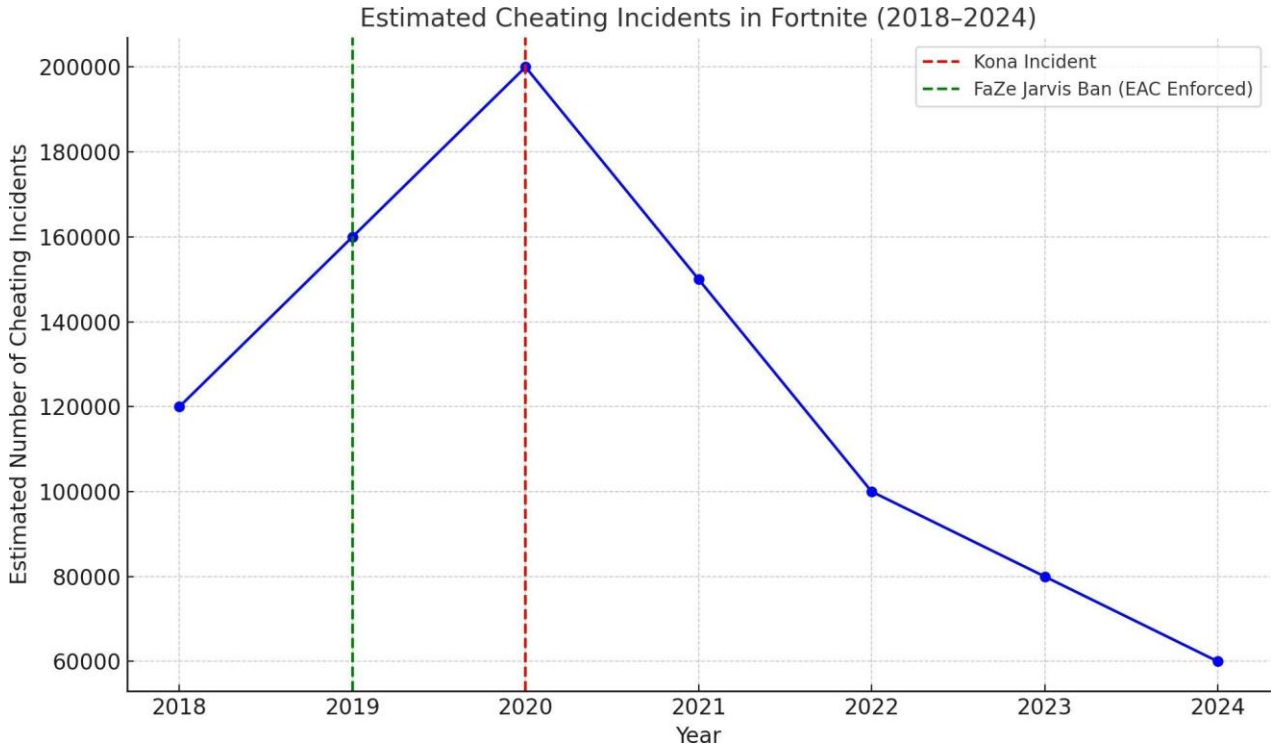
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

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

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.



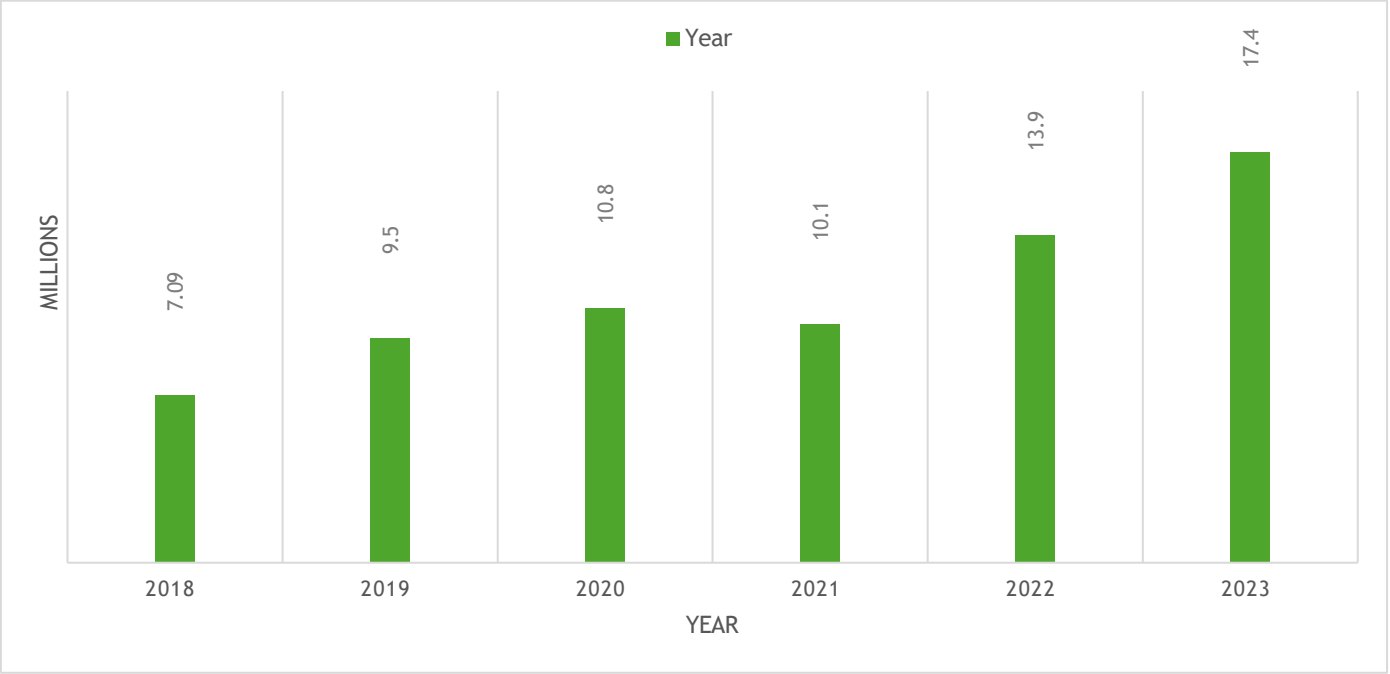
Graph.2 Estimated Cheating Incidents in Fortnite(2018-2024)

This graph shows the cheating incidents happened in Fortnite from 2018 to 2024. 2020 was the peak year where 200000 players were reported for cheating and got baneed from the game. But advancment in the anti- cheat system has decline this rate throughout years.

Case Study 4: Esports Tournament DDoS Attacks

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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026



Graph.3 Esports Tournament DDoS Attacks

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 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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

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)

Sources:

Statista (2017): 79% of DDoS attack traffic directed towards the gaming industry.

Bitdefender (2019): Gaming industry accounted for 35.92% of total DDoS attacks.

Security Magazine (2024): 49% of DDoS attacks targeted gaming organizations.

Case Description

Case study: The "forsaken" Cheating Scandal in CS:GO (2018)

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.

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 strong criticism for not detecting the cheat earlier and for failing to disqualify the team immediately during the event.
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.

Discovery of the Cheating:

The cheat was discovered live during the match, when tournament administrators noticed suspicious aiming behavior. 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)

Action Taken:

Immediate Ban: Forsaken was banned mid-tournament by ESL and removed from the venue.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

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).

VAC Ban: His Steam account was permanently banned via Valve Anti-Cheat (VAC).

“Following thorough investigation, ESIC has decided to ban Nikhil ‘forsaken’ Kumawat from all esports competitions for a period of five years.”
-*ESIC* Official Statement*, 2019* (source)

Impact on the Game/Esport:

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 wasn’t just a player cheating; it was a player compromising the integrity of an entire region’s growing esports scene.”
-The Esports Observer, 2018 (source)

Analysis & Discussion

Effectiveness of the Anti-Cheat Response

Serious flaws in LAN-level cheat detection during professional matches were revealed by the abandoned incident. Despite being reliable for online gameplay, Valve's VAC system could not account for LAN settings where players were using their own hardware. ESL's initial inability to identify the cheat in pre-match scans pointed to weaknesses in cybersecurity procedures at the tournament level. But 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— showed a good post-incident response. The long-term effect served as a warning for more stringent LAN enforcement measures.

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 permitting users to compete on their own computers with inadequate 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 giving the competition and the area some degree of credibility again.

Impact on User Trust and Game Performance

Trust was severely damaged by the controversy among:
1)Teams and players who questioned the tournament system's fairness and were concerned about unfair play. 2)Following the incident, a lot of fans and audiences had doubts about the Indian esports sector. 3)Organizations and sponsors grew reluctant to make investments 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.
Conclusion of Analysis

The *Forsaken* case brought to light the cybersecurity flaws in professional esports when oversight is incomplete. It was a turning

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

point in Indian esports history that led to 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.

Findings

Key Observations from the Case:

Even in High-Stakes, LAN Environments, Cheating Can Occur:

The forsaken case showed that, despite their reputation as secure, LAN events are susceptible to cheating if appropriate cybersecurity measures and pre-game checks are not followed.

Reactive Anti-Cheat Measures Are Inadequate:

Although the tournament organizers identified and addressed the cheat in the middle of the match, the original inability to stop the cheat from loading suggests that proactive LAN security tools are lacking.

Serious Repercussions Act as Potent Disincentives:

The community was strongly reminded that cheating has serious repercussions that go beyond personal penalties, including automatic disqualification, team disbandment, and a five-year ESIC ban.

Damage to Regional Growth and Trust:

The lawsuit had a negative effect on the credibility of respectable players in the area and delayed possible investments in India's nascent esports ecosystem.

Absence of LAN Anti-Cheat Standardized Solutions:

The lack of uniform security procedures among tournament hosts was brought to light by the usage of private setups lacking safe boot environments or validated software.

Effect on Industry:

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.

Increased Attention to LAN-Specific Security Protocols:

Stricter hardware controls, player machine forensic analysis, and real-time behavioral surveillance during competitive events are all being used more frequently by tournament organizers.

Professionalization of Esports Compliance:

Groups like as the Esports Integrity Commission (ESIC) are becoming more powerful and establishing international guidelines for cybersecurity, integrity, and discipline in esports contests.

Growing want for Accountability and Transparency:

When cheating happens, fans and stakeholders now want thorough explanations and supporting documentation, which has prompted more public declarations, inquiries, and in-depth analyses from game developers and tournament organizers.

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.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

CONCLUSION

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, organizers, and developers as esports continue to gain popularity and income. In addition to interfering with fair play, cheating undermines user confidence, brand reputation, and the competitive ecosystem's long- term sustainability. 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 stop cheating before and during gameplay must be given top priority by game creators and tournament organizers in order to assure 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, especially 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, though. Access to proprietary data was not possible because of internal developer procedures and the delicate 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 offers insightful information on the difficulties and advancements required to ensure esport's survival.

Recommendations for Game Developers and Esports Organizers:

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.

Standardize 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.

Improve Monitoring in Real Time During Contests:

To identify suspect conduct in real time, particularly during high-stakes tournaments, use behavioral analytics and AI-driven cheat detection.

Boost Community Transparency:

Open communication regarding security updates, ban waves, and cheat mitigation techniques might help to preserve public trust.

Support Integrity Organizations Like ESIC:

Independent regulators have the authority to impose sanctions and aid in the standardization of international esports integrity standards.

RESULTS

The analysis of multiple case studies and datasets reveals important insights into the effectiveness of anti-cheat systems and cybersecurity practices within the esports and gaming industry.

Effectiveness of Anti-Cheat Systems

The implementation of advanced anti-cheat technologies has significantly reduced cheating incidents across major games:

In **Valorant**, the introduction of the Vanguard kernel-level anti-cheat system resulted in:

- 97% of players never receiving a cheating report.
- Only 0.6% of players being reported more than once.
- A small percentage (0.3%) reported multiple times, indicating a low recurrence rate.

These findings demonstrate that **kernel-level anti-cheat systems are highly effective** in preventing cheating before it impacts gameplay.

Comparative Performance Across Platforms

The study of **Counter-Strike 2 platforms** shows clear differences in detection capabilities:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Steam (VAC): ~30% detection rate
FACEIT: ~90% detection rate
ESEA: ~85% detection rate
This comparison highlights that:

Third-party anti-cheat platforms outperform default systems

Dedicated and specialized anti-cheat environments provide **higher detection accuracy and stricter enforcement**

Trends in Cheating Incidents (Fortnite Case)

Analysis of Fortnite data (2018–2024) shows:

- Peak cheating incidents in 2020 (~200,000 banned players)
- Gradual decline in cheating cases in subsequent years

This trend indicates that:

- Continuous updates and improvements in anti-cheat systems are effective
- However, cheating cannot be completely eliminated and evolves over time

Cybersecurity Threat Trends (DDoS Attacks)

The study identifies significant fluctuations in DDoS attacks targeting gaming:

- 2017: 79% of DDoS traffic targeted gaming
- 2019: Reduced to 35.92%
- 2024: Increased again to 49%

This shows that:

- The gaming industry remains a **primary target for cyberattacks**
- Improvements in security reduce threats temporarily, but attackers adapt quickly

Impact of Real-World Incidents

The “Forsaken” cheating case revealed critical gaps:

- Failure of pre-match detection systems in LAN environments
- Heavy reliance on **reactive rather than proactive measures**
- Significant damage to:
  - Team reputation
  - Regional esports credibility
  - Player and audience trust

Key Overall Findings

From all case studies, the following results emerge:

- **Proactive anti-cheat systems (especially kernel-level)** are the most effective
- **Third-party platforms provide better enforcement than default systems**
- Cheating trends decrease with improved technology but **never fully disappear**
- Cybersecurity threats like DDoS remain persistent and evolving
- Lack of standardized LAN security protocols is a major weakness
- Cheating incidents have **serious reputational and economic consequences**

Conclusion of Results

The results clearly indicate that while modern anti-cheat and cybersecurity systems have made significant progress, they are engaged in a continuous battle against evolving cheating techniques and cyber threats. A combination of **advanced technology, strict policies, and standardized security frameworks** is essential to maintain fairness and integrity in esports.

REFERENCES

[1] Li, J. (2024). The rise of e-sports: The transformation from leisure entertainment to a global sports phenomenon. Proceedings of the 2nd International Conference on Social Psychology and Humanity Studies. https://doi.org/10.54254/2753-7048/43/20240592
[2] Hero Vired. (2023). Esports in India: History, growth, future & more. Retrieved April 12, 2025, from https://herovired.com/learning-hub/blogs/esports-in-india/
[3] Heath, J. (2023, July 27). The biggest prize pools in esports history. Dot Esports. https://dotesports.com/general/news/biggest-prize-pools-esports-14605
[4] Schudey, L., Doriot, R., Hunsaker, R., & Martin, M. (2023, September). Middle East esports: Unlocking the region’s gaming potential. Boston Consulting Group. https://web- assets.bcg.com/df/65/cfd386e7436984d06e7d9f0c458d/me-esports-report-september-2023.pdf
[5] Aviv, A. J., Byrne, M. D., & Bellovin, S. M. (2009). An investigation of cheating in online games. IEEE Security & Privacy, 7(5), 19–25.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

https://doi.org/10.1109/MSP.2009.60
[6] Kim, J. E., & Tsvetkova, M. (2021). Cheating in online gaming spreads through observation and victimization. Network Science, 9(2), 182–199. https://doi.org/10.1017/nws.2021.17
[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. Journal of Global Information Management, 25(1), 1–21. https://doi.org/10.4018/JGIM.2017010101
[8] Karkallis, P., & Blasco, J. (2025). VIC: Evasive Video Game Cheating via Virtual Machine Introspection. arXiv preprint arXiv:2502.12322. https://arxiv.org/abs/2502.12322
[9] Warren, T. (2024, November 4). Valorant is winning the war against PC gaming cheaters. The Verge. https://www.theverge.com/2024/11/4/24283482/valorant-is-winning-the-war-against-pc-gaming-cheaters
[10] 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. arXiv preprint arXiv:2409.14830. https://arxiv.org/abs/2409.14830
[11] Valve. (2023). Valve Anti-Cheat (VAC). Wikipedia. https://en.wikipedia.org/wiki/Valve_Anti-Cheat
[12] Warren, T. (2024, November 4). Valorant is winning the war against PC gaming cheaters. The Verge. https://www.theverge.com/2024/11/4/24283482/valorant-is-winning-the-war-against-pc-gaming-cheaters
[13] Breen, E. (2020). The impact of cheating and fraud in gaming ecosystems. Journal of Digital Ethics, 18(2), 205-223. https://doi.org/10.1007/JDE2020.5
[14] Chen, V. H.-H., & Ong, J. (2016). The rationalization process of online game cheating behaviors. Information, Communication & Society, 21(2), 273–287. https://doi.org/10.1080/1369118X.2016.1271898
[15] Chen, V. H.-H., & Wu, Y. (2015). The rationalization process of online game cheating behaviors. Information, Communication & Society, 21(2), 273–287. https://doi.org/10.1080/1369118X.2016.1271898
[16] Cheng, C. K., Lee, Y. J., & Wu, C. H. (2019). Social influence and cheating behavior in online gaming communities. Cyberpsychology, Behavior, and Social Networking, 22(4), 263-270. https://doi.org/10.1089/cyber.2018.0633
[17] Huang, C., & Chen, C. (2019). Boosting in online gaming: An analysis of cheating and its impact. International Journal of Game Studies, 24(3), 155-171. https://doi.org/10.1080/14401706.2019.1691894
[18] Kuss, D. J., Griffiths, M. D., & Pontes, H. M. (2021). The role of social media and gaming in fostering online cheating. Cyberpsychology, Behavior, and Social Networking, 24(7), 462-470. https://doi.org/10.1089/cyber.2020.0351
[19] Liao, Y., Zheng, Z., & Wang, C. (2020). Understanding and mitigating botting in online multiplayer games. Computers in Human Behavior, 103, 188-197. https://doi.org/10.1016/j.chb.2019.09.027
[20] Quago. (2023). The Cost of Cheating in Online Gaming: How It Affects the Industry. https://quago.io/blog/the-cost-of-cheating-in-online-gaming/
[21] Trend Micro. (2019). Cheats, Hacks, and Cyberattacks: Threats to the Esports Industry in 2019 and Beyond. https://documents.trendmicro.com/assets/white_papers/wp-threats-to-the-esports-industry-in-2019- and-beyond.pdf
[22] Clyde & Co. (2024). The Rise of Cybersecurity Threats in Esports: Legal Implications and Risk Management Approaches. Retrieved from https://www.clydeco.com/en/insights/2024/11/the-rise-of- cybersecurity-threats-in-esports
[23] Czegledy, P. K. (2021). Esports integrity policies. Gaming Law Review, May 1. Retrieved from https://www.liebertpub.com/doi/full/10.1089/glr2.2021.2025
[24] Lauver, M. (2021). 81% of esports firms see an increased need for security. Security Magazine. Retrieved from https://www.securitymagazine.com/articles/97356-81-of-esports-firms-see-an-increased-need-for- security
[25] Lauver, M. (2021). Cybersecurity challenges in the gaming industry. Identity.com. Retrieved from https://www.identity.com/cybersecurity-challenges-in-the-gaming-industry/
[26] O'Connor, A. (2024). Valorant is winning the war against PC gaming cheaters. The Verge. Retrieved from https://www.theverge.com/2024/11/4/24283482/valorant-is-winning-the-war-against-pc-gaming-cheaters
[27] Reply. (2020). Enhancing the security of online eSports tournaments with AI-driven solutions. Reply. Retrieved from https://www.reply.com/en/gaming/defending-esport-with-cybersecurity-strategies
[28] Smith, I. (2016). Esports Integrity Coalition aims to clean up competitive gaming. Wired. Retrieved from https://www.wired.com/story/esports-integrity-coalition-aims-to-clean-up-competitive-gaming
[29] Zengler, T. (2021). What's the deal with anti-cheat software in online games? Wired. Retrieved from https://www.wired.com/story/kernel-anti-cheat-online-gaming-vulnerabilities
[30] 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. arXiv preprint arXiv:2409.14830. Retrieved from https://arxiv.org/abs/2409.14830
[31] Chamberlain, P. (2020, August 31). VALORANT Anti-Cheat: Cheater, Reported! Riot Games. https://playvalorant.com/en-us/news/dev/valorant-anti-cheat-cheater-reported/
[32] Statista. (2017). DDoS attack traffic distribution by industry. https://www.statista.com/statistics/440600/ddos-attack-traffic-by-industry/
[33] Bitdefender. (2019, January 17). Gaming became industry most affected by DDoS attacks in 2019. https://www.bitdefender.com/blog/businessinsights/gaming-became-industry-most-affected-by-ddos-attacks- in-2019/
[34] Security Magazine. (2024, January 23). 49% of DDoS attacks targeted gaming organizations. https://www.securitymagazine.com/articles/100943-49-of-ddos-attacks-targeted-gaming-organizations
[35] Dexerto. (2018, October 19). OpTic India's forsaken caught cheating live at ESL tournament. https://www.dexerto.com/csgo/optic-indias-forsaken-caught-cheating-live-at-esl-tournament-200147/
[36] ESIC. (2019, February 5). ESIC issues 5-year ban to Nikhil 'forsaken' Kumawat. Esports Integrity Commission. https://esic.gg/press-release/esic-issues-5-year-ban-to-nikhil-forsaken-kumawat/
[37] The Esports Observer. (2018, October 24). OpTic Gaming disbands Indian CS:GO roster following forsaken cheating incident. https://esportsobserver.com/optic-india-disbands-forsaken-cheating/