User Perceptions of Kernel-Level Anti-Cheat Systems: Privacy, Trust, and Ethical Considerations

Preslav Stoyanov, Jean-Paul Otten

January 16, 2026

Contents

Abstract

Kernel-level anti-cheat systems have become increasingly common in modern competitive online games, providing developers with powerful tools to detect cheating at the operating system's highest privilege level. However, this deep level of system access has sparked significant debate concerning privacy, security, and user trust. This research investigates user perceptions and ethical considerations surrounding kernel-level anti-cheat technologies through a systematic literature review. By synthesizing existing academic research, technical documentation, public discourse, and community perspectives, this study aims to provide a comprehensive analysis of how users evaluate the trade-off between fair gameplay and potential privacy risks, with particular attention to implications for students and technically literate users.

1 Introduction

This chapter introduces the research topic, outlines its significance within the academic and technological landscape, and provides an extensive contextual foundation for understanding kernel-level anti-cheat systems. The growing dependence on online multiplayer games has resulted in a parallel increase in cheat development, creating a persistent challenge for game developers and cybersecurity professionals. This introduction further elaborates on the problem framing, explores the historical and technical evolution of anti-cheat technology, and presents the research objectives and questions guiding this literature review.

1.1 Context and Background

With the rise of competitive online gaming, digital fairness has become a central issue for both the gaming industry and its user base. Games such as *Valorant*, *Apex Legends*, *Counter-Strike 2*, and *Fortnite* have built global ecosystems in which millions of players participate daily [4]. These ecosystems frequently involve ranked matchmaking, esports tournaments, financial incentives, and large communities that depend on integrity and equal opportunity. As a consequence, cheating—whether through aim-assist tools, wallhacks, memory manipulation, or macro automation—poses a significant threat to the sustainability and credibility of modern online gaming.

To fully appreciate the contemporary debate surrounding kernel-level anti-cheats, it is necessary to understand the historical evolution of cheat prevention within gaming ecosystems. In the early 2000s, online games relied on simple file integrity checks and heuristic detection methods. Titles such as early *Counter-Strike* versions used VAC (Valve Anti-Cheat), which operated entirely at user level [5]. While effective against basic cheats,

these tools were limited by architectural constraints and eventually became insufficient against increasingly complex attack vectors.

Traditional anti-cheat systems operated exclusively in user mode, where their capacities were significantly limited by the sandboxing and process isolation mechanisms of modern operating systems. Developers could detect injected code or monitor game files, but they were unable to observe low-level manipulations performed by increasingly sophisticated cheat programs. As competitive gaming scenes expanded, so did the value of cheating. High-stakes tournaments, ranking systems, and monetised accounts created strong incentives for cheat development [5]. As cheat development evolved, many cheat providers began exploiting drivers, manipulating kernel memory, or injecting code into system processes that conventional user-level anti-cheat systems could not detect [1].

In response, anti-cheat developers integrated more advanced methods at the user level:

- behavioural analysis and anomaly detection,
- signature-based scanning,
- machine learning models for identifying suspicious patterns,
- hardware ID tracking,
- process monitoring,
- network traffic analysis.

Yet, with user-level privileges, anti-cheat tools were always fundamentally limited. A user-level application cannot monitor kernel-level drivers, privileged memory spaces, or system-level hooks. It also cannot reliably detect rootkits designed to hide processes from the operating system [1]. This architectural asymmetry led developers to adopt kernel-level anti-cheats, creating a new paradigm in game security—one that offered unprecedented detection capabilities but introduced significant ethical and privacy dilemmas.

To address this evolving threat, game developers introduced **kernel-level anti-cheat systems**, which operate with `ring 0` privileges. This shift represented a profound technical transformation. By operating at the same privilege level as the operating system itself, kernel-level anti-cheats can monitor drivers, block unauthorised memory access, and detect rooting or tampering behaviours that would otherwise go unnoticed [1]. Examples include *Riot Vanguard*, *Easy Anti-Cheat*, and *BattlEye*, which have now become standard components of many major online titles [4].

However, this technological evolution did not occur without controversy. Multiple communities, cybersecurity analysts, and online technology publications have raised concerns regarding the fundamentally invasive nature of kernel-level software. Public discussions frequently compare kernel-level anti-cheats to rootkits due to their ability to

run constantly in the background, access sensitive system information, and interact with hardware components at an unrestricted level [1]. Many players have expressed discomfort with the idea of a video game installing a privileged driver that launches on system startup and maintains persistent access even when the game is not running [2].

Kernel-level anti-cheats have become a focal point for debates surrounding digital ethics. Several major concerns are frequently mentioned in academic and community discussions. **Privacy intrusion** is a primary concern: kernel-level drivers can, in principle, access virtually all system-level data. Even if anti-cheat developers claim to limit such access, the potential remains, and users must rely entirely on trust [3]. **Security vulnerabilities** represent another critical issue: a vulnerability in a kernel-level anti-cheat can compromise the entire system. Several security researchers have warned that poorly designed drivers could expose users to privilege escalation attacks [1]. **Transparency** concerns are widespread: many companies offer vague explanations about what their anti-cheat system does, how long it runs, what data it collects, or how that data is stored [3]. Additionally, the issue of **informed consent** arises when users are forced to choose between giving up privacy or losing access to a game they purchased [2]. Finally, because kernel-level anti-cheats behave similarly to rootkits, many users feel uncomfortable with such software running on personal devices, leading to **comparisons to malware** [1, 3].

Furthermore, online discussions on platforms like Reddit and GitHub provide extensive anecdotal evidence of fear, suspicion, or outright rejection of kernel-level anti-cheat requirements [2, 3]. Users commonly cite worries about privacy invasion, potential for misuse, transparency issues, and the possibility that vulnerabilities within the anti-cheat software could be exploited by malicious third-party actors. These concerns contribute not only to reduced trust in game developers but also to broader questions surrounding the ethics of such invasive technological interventions.

Despite these concerns, kernel-level anti-cheats have become increasingly prevalent. The database maintained by Levvvel [4] demonstrates a clear upward trend in the number of online games requiring these technologies, illustrating the perceived necessity within the industry. Given that students—particularly those studying informatics, cybersecurity, or related fields—represent a demographic highly likely to interact with such systems, their perceptions serve as an insightful indicator of broader public acceptance patterns.

At the same time, students possess greater-than-average technical literacy, allowing them to form more nuanced opinions on topics related to digital privacy, kernel security, operating-system architecture, and ethical technological deployment. Therefore, studying student perceptions yields data that is more informed than general consumer sentiment, while also reflecting the attitudes of the next generation of industry professionals.

This convergence of technological necessity, public controversy, and academic relevance highlights the importance of understanding the acceptance, trust, and concerns surrounding kernel-level anti-cheat technologies.

1.2 Research Problem

The widespread adoption of kernel-level anti-cheat systems has created a significant tension between the technical necessity of preventing cheating and the privacy and security concerns of users. While game developers increasingly rely on these systems to maintain competitive integrity, public discourse reveals substantial apprehension regarding their invasive nature and potential risks [1, 2, 3]. Despite the growing prevalence of kernel-level anti-cheats across major gaming titles [4], the existing body of knowledge on user perceptions remains fragmented across academic research, technical documentation, community discussions, and media coverage.

The existing literature encompasses technical security assessments, company whitepapers, anecdotal community discussions, and technology journalism, but lacks a systematic synthesis that comprehensively addresses user perceptions, ethical considerations, and the privacy-trust trade-offs involved. Understanding how users—particularly those with technical literacy, including students in cybersecurity and related fields—perceive, evaluate, and accept these technologies is crucial for developers, policymakers, and the academic community. This research aims to synthesize existing knowledge and identify gaps in understanding user perceptions, concerns, trust levels, and acceptance of kernel-level anti-cheat systems.

1.3 Research Objective

The primary objective of this research is to systematically review and synthesize existing literature on user perceptions of kernel-level anti-cheat systems in modern online games. Specifically, this study aims to:

1. Synthesize existing research and discourse on user awareness of kernel-level anti-cheat technologies and associated risks.

2. Analyse patterns in user acceptance and attitudes toward games requiring kernel-level anti-cheat systems as reflected in academic literature and public discourse.

3. Review and consolidate findings on privacy concerns, security worries, and trust in game developers among users.

4. Identify factors (technical knowledge, gaming habits, demographic characteristics) that influence user perceptions, as documented in existing research and discussions.

5. Examine how perceived invasiveness relates to acceptance of these technologies, based on existing evidence.

6. Identify gaps in current knowledge and areas requiring further empirical research.

1.4 Research Questions

Based on the research problem and objectives, the following research questions guide this literature review:

1. What do existing sources reveal about user awareness of kernel-level anti-cheat systems and their implications?
2. How do users evaluate the acceptability of kernel-level anti-cheat technologies in online games, according to existing research and discourse?
3. What are the primary concerns (privacy, security, transparency) that influence user perceptions, as documented in the literature?
4. What levels of trust do users place in game developers and companies that implement kernel-level anti-cheats, based on existing evidence?
5. What factors (technical knowledge, gaming experience, demographic characteristics) are associated with user acceptance or rejection of kernel-level anti-cheat systems in existing research?
6. What gaps exist in current understanding of user perceptions that require further empirical investigation?

1.5 Research Propositions

Based on the context, research problem, and objectives outlined above, the following propositions derived from existing literature guide this review:

- **P1:** Users with greater awareness of kernel-level anti-cheat systems exhibit higher levels of privacy concerns, as suggested by technical communities and cybersecurity discussions.
- **P2:** Users exhibit lower trust toward companies that implement kernel-level anti-cheats, as evidenced in public discourse and community discussions.
- **P3:** Users with greater technical knowledge express stronger concerns about kernel-level drivers, as reflected in cybersecurity and technical community perspectives.
- **P4:** Despite concerns, some users are willing to sacrifice privacy for fair gameplay, as indicated by continued adoption of games requiring kernel-level anti-cheat.
- **P5:** Higher perceived invasiveness negatively correlates with acceptance of kernel-level anti-cheat systems, as suggested by privacy-focused discussions and user complaints.

These propositions are explored through systematic analysis of existing literature, community discourse, and documented user reactions, rather than through primary data collection.

2 Methods

This chapter describes the methodological approach used to systematically review and synthesize existing literature on user perceptions of kernel-level anti-cheat systems.

2.1 Choice of Method

A **systematic literature review** is selected as the primary method due to:

- the fragmented nature of existing research across multiple domains (cybersecurity, ethics, gaming studies),
- the need to synthesize diverse sources including academic research, technical documentation, and public discourse,
- the ability to identify patterns and gaps in current understanding,
- time and resource efficiency compared to primary data collection,
- the value of providing a comprehensive overview for future research directions.

This approach allows for the integration of multiple types of sources, providing a holistic view of user perceptions while acknowledging the limitations of secondary data analysis.

2.2 Literature Search Strategy

The literature search was conducted using multiple strategies to ensure comprehensive coverage:

Academic Databases Academic sources were identified through searches in databases including Google Scholar, IEEE Xplore, ACM Digital Library, and university library databases. Search terms included combinations of: “kernel-level anti-cheat,” “anti-cheat privacy,” “game security privacy concerns,” “rootkit anti-cheat,” “Riot Vanguard,” and “gaming privacy ethics.”

Technical Documentation Official documentation and whitepapers from companies implementing kernel-level anti-cheat systems were reviewed, including Riot Games' Vanguard documentation, Epic Games' Easy Anti-Cheat materials, and BattlEye technical information.

Public Discourse Sources Community discussions and public discourse were examined through sources including:

- Technology journalism and news articles (e.g., XDA Developers, technology blogs),
- Community discussions on platforms like Reddit and GitHub,
- Video content from technical channels explaining kernel-level anti-cheat,
- Gaming industry databases tracking anti-cheat adoption.

These sources are methodologically appropriate for studying *user perceptions* rather than factual system behavior. Community discourse captures authentic user reactions, concerns, and attitudes that empirical surveys would measure, while providing access to discussions that may not be captured in formal research. Technology journalism offers expert analysis that reflects broader community perspectives, and platform discussions reveal unmediated user sentiment. This approach recognizes that perceptions themselves are valid research subjects, independent of technical accuracy, as they shape user decision-making and acceptance regardless of objective system characteristics.

2.3 Source Selection Criteria

Sources were included based on the following criteria:

- **Relevance:** Sources must address user perceptions, privacy concerns, trust, acceptance, or ethical considerations related to kernel-level anti-cheat systems.
- **Recency:** Preference given to sources from 2020 onwards, reflecting the recent proliferation of kernel-level anti-cheat systems, though historical context sources were also considered.
- **Credibility:** Sources include peer-reviewed academic work, official company documentation, reputable technology journalism, and substantial community discussions with clear authorship or attribution.
- **Accessibility:** Sources are publicly accessible or available through academic databases.

2.4 Data Extraction and Analysis

The review process involved:

1. Source Classification Sources were categorized by type: (1) academic research, (2) technical documentation, (3) technology journalism, (4) community discourse, and (5) industry data/statistics.

2. Thematic Analysis Content was analyzed to identify recurring themes related to:

- User awareness and knowledge of kernel-level anti-cheat systems
- Privacy concerns and perceived risks
- Trust in game developers and companies
- Acceptance and willingness to use games with kernel-level anti-cheat
- Factors influencing perceptions (technical knowledge, gaming habits, etc.)
- Ethical considerations and debates

3. Synthesis Findings from diverse sources were synthesized to identify patterns, contradictions, and consensus regarding user perceptions. The synthesis process involved:

- Comparing perspectives across different source types
- Identifying areas of agreement and disagreement
- Noting gaps in existing knowledge
- Examining how different user groups (technically literate vs. general users, students vs. broader demographics) are represented in the literature

2.5 Quality Assessment

Source quality was assessed using the following considerations:

- For academic sources: peer review status, methodology rigor, sample size and representativeness (where applicable).
- For technical documentation: official source status, technical accuracy, completeness of information.
- For journalism and community sources: author credibility, source verification, breadth of perspective represented.

Limitations of individual sources were acknowledged in the synthesis, particularly noting the predominance of anecdotal evidence in community discussions versus empirical research in academic literature.

2.6 Methodological Limitations

This literature review approach has several limitations:

- **Publication Bias:** Negative reactions or concerns may be overrepresented in public discourse, while positive acceptance may be underrepresented if users simply accept and continue using games.
- **Source Heterogeneity:** Combining academic research with community discourse creates challenges in comparability and quality assessment.
- **Temporal Limitations:** Perceptions may evolve rapidly as technologies mature and users become more familiar with kernel-level anti-cheat systems.
- **Lack of Primary Data:** The review cannot provide original empirical insights, only synthesis of existing knowledge.
- **Representativeness:** Community discourse sources may not represent all user perspectives, particularly those of less vocal or less technically engaged users.
- **Gaps in Literature:** Limited empirical research specifically on user perceptions means the review relies heavily on anecdotal evidence and theoretical discussions.

Despite these limitations, the literature review provides valuable synthesis of existing knowledge and identifies critical areas where empirical research is needed.

3 Results

This section presents the findings from the systematic literature review, synthesizing evidence from academic research, technical documentation, technology journalism, and public discourse on user perceptions of kernel-level anti-cheat systems.

3.1 User Awareness of Kernel-Level Anti-Cheat Systems

Evidence indicates significant variation in user awareness of kernel-level anti-cheat systems. Awareness levels correlate closely with technical literacy and engagement with gaming communities. According to the comprehensive database maintained by Levvvel [4], 338 games currently implement kernel-level anti-cheat software, indicating widespread industry adoption. However, evidence from community discussions suggests that many users remain unaware of what kernel-level anti-cheat entails or how it differs from traditional user-level protection [2].

Technical communities and cybersecurity-focused discussions demonstrate higher awareness levels. The GitHub Gist analysis by a cybersecurity researcher provides detailed

technical explanations that indicate users with technical backgrounds are more likely to understand the implications of kernel-level access [3]. These users demonstrate awareness of concepts such as Ring 0 privileges, rootkit-like behaviour, and system-level monitoring capabilities. In contrast, general gaming communities show lower awareness, with many users expressing surprise upon learning that anti-cheat software runs at the kernel level [2].

The YouTube explanation by PirateSoftware [5] suggests that educational content plays a crucial role in awareness. Users who engage with technical explanations demonstrate greater understanding of both the security benefits and privacy risks associated with kernel-level anti-cheat systems. However, even technically aware users often lack complete understanding of what data these systems can access or how long they remain active on systems [3].

A notable pattern emerges: users who discover kernel-level anti-cheat requirements often express surprise or concern, particularly when learning that drivers launch on system startup and maintain persistent access even when games are not running [2, 3]. This suggests that many users accept anti-cheat systems without full awareness of their operational characteristics or privacy implications.

3.2 Privacy Concerns and Perceived Risks

Privacy concerns emerge as the dominant theme across all examined sources. The fundamental issue centres on the unrestricted system access that kernel-level drivers provide. As the XDA Developers analysis emphasizes, kernel-level anti-cheat systems operate with the highest privilege level possible, granting them access to virtually all system-level data [1]. The GitHub Gist provides detailed technical analysis explaining that kernel-level drivers can "access and monitor everything on your system, including all processes, memory, network traffic, hardware, and sensitive data" [3].

Multiple sources consistently compare kernel-level anti-cheat systems to rootkits due to their operational similarities. Both operate at the kernel level, run continuously in the background, launch on system startup, and maintain persistent system access [1, 3]. This comparison generates significant concern among users, as rootkits are universally recognized as malicious software. As noted in the technical analysis, "kernel-level anti-cheat behaves almost identically to malware and rootkits" [3], which contributes to user discomfort and suspicion.

Security vulnerability concerns are extensively documented. The XDA Developers article warns that vulnerabilities in kernel-level drivers can compromise the entire operating system, as they operate at the same privilege level as the OS kernel itself [1]. Security researchers emphasize that poorly designed or compromised anti-cheat drivers could enable privilege escalation attacks, allowing malicious actors to gain complete system con-

trol [1]. The GitHub analysis highlights specific examples where kernel-level anti-cheat vulnerabilities have been exploited [3], reinforcing these concerns.

Transparency and data collection concerns feature prominently in user discussions. Multiple sources indicate that companies provide limited or vague information about what data their anti-cheat systems collect, how long they run, what they monitor, and how data is stored or transmitted [3, 2]. Users express frustration with the lack of transparency, noting that they must trust companies' claims about data limitations without verifiable evidence [2]. The GitHub Gist analysis notes that many users feel uncomfortable being unable to verify what information kernel-level drivers access or transmit [3].

The informed consent issue is repeatedly raised in community discussions. Users express discomfort with the binary choice presented: either accept kernel-level anti-cheat or lose access to games they have purchased [2]. This perceived lack of meaningful choice contributes to privacy concerns, as users feel coerced into accepting invasive software regardless of their comfort level with the privacy implications [2, 3].

3.3 Trust in Game Developers and Companies

Evidence indicates generally low trust levels toward game developers and companies implementing kernel-level anti-cheat systems. Community discussions consistently express skepticism about developers' claims regarding data collection, system monitoring, and security practices [2]. The Reddit discussion on EA's anti-cheat system exemplifies widespread distrust, with users questioning why games require such invasive software and expressing suspicion about potential misuse of kernel-level access [2].

Transparency appears to be a critical factor influencing trust. Sources indicate that companies providing detailed technical documentation and clear explanations about their anti-cheat systems face less skepticism than those offering vague or minimal information [3]. However, even when companies attempt transparency, users with technical backgrounds express doubts about verifiability, noting that claims about data limitations cannot be independently verified [3].

The proprietary nature of most kernel-level anti-cheat systems contributes to trust issues. Users cannot inspect the code or verify security implementations, leading to what the GitHub analysis describes as "blind trust in companies with varying security track records" [3]. This lack of verifiability is particularly concerning to technically literate users, who are accustomed to open-source software where code can be audited.

Historical context influences trust levels. Companies with poor privacy track records or previous security incidents face heightened skepticism. Community discussions suggest that users' general trust in gaming companies has decreased due to kernel-level anti-cheat requirements [2]. However, some sources note exceptions: companies that have invested in transparent communication and security documentation receive relatively higher trust,

though skepticism remains the dominant sentiment.

The forced adoption model significantly impacts trust. Users express resentment toward being required to install kernel-level drivers as a condition of accessing purchased games [2]. This requirement, combined with the inability to opt out while retaining game access, erodes trust by suggesting that companies prioritize their interests over user privacy and choice.

3.4 Acceptance and Willingness to Use

Despite widespread privacy concerns and low trust levels, evidence suggests that many users ultimately accept kernel-level anti-cheat systems due to limited alternatives. The Levvvel database documenting 338 games using kernel-level anti-cheat indicates significant adoption across the industry [4]. This suggests that users either accept these systems or abandon games they wish to play.

Community discussions reveal a complex acceptance pattern. Many users express concerns but continue playing games with kernel-level anti-cheat because they value fair gameplay and have few alternatives [2]. This suggests a willingness to trade privacy for competitive integrity. However, the trade-off is often made reluctantly rather than enthusiastically. As one Reddit discussion notes, users feel "stuck between wanting fair games and wanting privacy" [2].

The prevalence of Easy Anti-Cheat, found in 155 games including major titles like Fortnite and Apex Legends [4], indicates that users accept these systems when bundled with popular games. However, acceptance does not necessarily indicate approval. Many discussions suggest users "grudgingly accept" rather than "enthusiastically embrace" kernel-level anti-cheat [2]. This distinction between behavioural acceptance and attitudinal approval is crucial: users may use systems they disapprove of when alternatives are unavailable.

Factors influencing acceptance include game popularity, competitive gaming engagement, and lack of viable alternatives. Users heavily invested in specific games or competitive scenes appear more willing to accept kernel-level anti-cheat than casual players [2]. However, some users report completely avoiding games that require kernel-level anti-cheat, suggesting that privacy concerns do lead to rejection in some cases [2, 3].

Notable exceptions to acceptance patterns exist. Technically literate users, particularly those in cybersecurity and related fields, demonstrate higher rejection rates [3]. These users more frequently cite privacy and security concerns as reasons to avoid games with kernel-level anti-cheat, suggesting that technical knowledge correlates with lower acceptance levels.

3.5 Factors Influencing Perceptions

Technical knowledge emerges as the strongest predictor of perception patterns across all sources examined. Users with cybersecurity or technical backgrounds consistently express stronger concerns about kernel-level anti-cheat systems compared to general users [3]. The GitHub technical analysis, written from a cybersecurity perspective, demonstrates the depth of concern among technically literate users, who understand the full implications of kernel-level access [3].

Technically knowledgeable users demonstrate greater awareness of security vulnerabilities, privacy implications, and system risks. They are more likely to question company transparency claims, understand rootkit comparisons, and recognize potential attack vectors. These users frequently cite their technical understanding as the reason for privacy concerns and lower acceptance levels [3].

Gaming habits and engagement levels also influence perceptions. Competitive and professional gamers, despite often having technical knowledge, demonstrate higher acceptance rates due to their investment in fair gameplay and professional opportunities [2]. Casual gamers show more variability, with some expressing strong privacy concerns while others remain indifferent if they are unaware of the technical details [2].

Awareness of security incidents or vulnerabilities significantly impacts perceptions. Users who learn about kernel-level anti-cheat vulnerabilities or security breaches express heightened concerns [1]. The XDA article documenting security risks influences perceptions by providing concrete examples of potential dangers [1].

Prior experience with anti-cheat systems shapes perceptions. Users who have experienced false positives, performance issues, or system problems with kernel-level anti-cheat express more negative perceptions than those without such experiences [2]. Negative experiences appear to amplify privacy and security concerns.

Cultural and regional factors may influence perceptions, though evidence is limited. The Levvvel database shows regional variations in anti-cheat adoption, with Korean-developed games frequently using nProtect GameGuard or XIGNCODE3 [4], suggesting different acceptance patterns in different markets. However, the sources examined primarily reflect Western perspectives, limiting cross-cultural analysis.

3.6 Comparative Analysis: Technical vs. Non-Technical Users

A clear divide exists between technically literate users and general users regarding kernel-level anti-cheat perceptions. This division is particularly relevant for students in technical fields, who represent an important demographic likely to interact with these systems while possessing elevated technical awareness.

Technically literate users, including students in cybersecurity, computer science, and engineering fields, demonstrate markedly different perception patterns compared to gen-

eral users. The GitHub Gist analysis provides a representative technical perspective, demonstrating deep concern about security implications, privacy risks, and system vulnerabilities [3]. These users understand kernel architecture, privilege levels, and security implications, leading to more critical evaluations.

Technical users are significantly more likely to:

- Recognize and articulate specific security risks (privilege escalation, driver vulnerabilities, system compromise)
- Question transparency claims and demand verifiable evidence
- Compare kernel-level anti-cheat to rootkits and malware based on technical understanding
- Express willingness to avoid games requiring kernel-level anti-cheat
- Identify potential attack vectors and exploitation risks

In contrast, general users demonstrate:

- Lower awareness of technical implications
- Greater reliance on company statements and trust
- More acceptance based on perceived necessity for fair gameplay
- Less understanding of security risks and privacy implications
- Greater variability in concerns, often driven by anecdotal experiences rather than technical knowledge

The XDA Developers article, written for a technically informed audience, emphasizes security risks and technical concerns [1], reflecting the priorities of technically literate users. In contrast, general gaming community discussions on Reddit show mixed perspectives, with many users expressing concerns based on privacy discomfort rather than technical understanding [2].

Students in technical fields occupy an intermediate position: they possess growing technical knowledge that enables critical evaluation, while simultaneously representing current users of gaming systems. This makes their perceptions particularly valuable for understanding how technical literacy shapes acceptance and concern patterns. As technical knowledge increases, privacy and security concerns typically increase while acceptance decreases [3, 2].

3.7 Gaps in Existing Research

Despite extensive discussion in technical communities and public discourse, significant gaps exist in empirical research on user perceptions of kernel-level anti-cheat systems. This literature review identifies several critical areas requiring further investigation.

Empirical User Perception Studies The most significant gap is the lack of quantitative empirical research on user perceptions. While community discussions and technical analyses provide valuable insights, systematic survey-based or experimental studies measuring user awareness, concerns, trust, and acceptance are largely absent. Research quantifying these variables across different user demographics would provide valuable empirical grounding for current observations.

Student-Specific Research While students, particularly those in technical fields, represent an important demographic, no focused empirical research specifically examines student perceptions. Studies investigating how students in cybersecurity, computer science, and related fields evaluate kernel-level anti-cheat systems would address the specific research interest in this demographic while providing insights into how technical education shapes privacy and security perspectives.

Longitudinal Studies All existing sources provide cross-sectional perspectives. Longitudinal research examining how perceptions evolve over time, particularly as users become more familiar with kernel-level anti-cheat or after security incidents, would provide valuable insights into perception dynamics and long-term acceptance patterns.

Cross-Cultural Analysis The sources examined primarily reflect Western perspectives, with limited analysis of regional differences. The Levvvel database shows varied adoption patterns (e.g., Korean markets favouring nProtect GameGuard and XIGNCODE3 [4]), suggesting potential cultural or regional differences in acceptance that warrant investigation.

Trust Dynamics While trust appears critical to acceptance, little empirical research examines trust formation, factors influencing trust levels, or how transparency initiatives impact trust. Understanding trust dynamics would help developers balance security needs with user acceptance.

Privacy-Fairness Trade-offs The literature consistently notes a privacy-fairness trade-off, but no empirical studies quantify how users evaluate this trade-off or what factors influence their willingness to sacrifice privacy for fair gameplay. Research examining

decision-making processes and trade-off evaluations would address a central question in the debate.

Impact of Security Incidents While sources note that security vulnerabilities affect perceptions, no research systematically examines how specific incidents influence user perceptions, trust, or acceptance. Understanding incident impact would inform risk communication and transparency strategies.

Effectiveness vs. Privacy The literature focuses primarily on privacy concerns but provides limited discussion of whether kernel-level anti-cheat actually provides superior effectiveness compared to user-level alternatives. Research comparing effectiveness alongside privacy costs would enable informed cost-benefit evaluations.

These gaps highlight opportunities for future empirical research that would significantly advance understanding of user perceptions and inform both industry practices and policy considerations.

4 Discussion

This discussion synthesizes findings from the literature review, interprets their implications, and addresses the research questions and propositions guiding this investigation. Synthesized evidence reveals a complex landscape of user perceptions marked by significant concerns, reluctant acceptance, and a clear divide between technically literate and general users.

4.1 Interpretation of Key Findings

Evidence indicates that user perceptions of kernel-level anti-cheat systems are predominantly negative. These perceptions are driven primarily by privacy concerns, security risks, and trust issues. However, despite these concerns, widespread adoption (338 games implementing kernel-level anti-cheat [4]) suggests that users ultimately accept these systems, often reluctantly, due to limited alternatives and desire for fair gameplay.

Technical literacy emerges as the strongest determinant of perception patterns. Users with technical backgrounds, including students in cybersecurity and related fields, demonstrate heightened awareness of risks, stronger privacy concerns, and lower acceptance levels compared to general users. This finding supports Proposition P3, suggesting that technical knowledge correlates with stronger concerns about kernel-level drivers, as reflected in technical community discussions [3].

The privacy-fairness trade-off represents a central tension in user perceptions. Users value both competitive integrity and privacy, but existing systems force a binary choice

that favours gameplay access over privacy preferences. This supports Proposition P4: despite concerns, many users sacrifice privacy for fair gameplay, though the sacrifice appears reluctant rather than enthusiastic [2].

4.2 Addressing Research Questions

Research Question 1: User Awareness Evidence indicates significant variation in awareness levels. Technically literate users demonstrate substantially higher awareness than general users. Many users remain unaware of kernel-level anti-cheat characteristics until they encounter specific requirements or engage with technical discussions. Awareness correlates strongly with engagement with technical communities and educational content [5, 3].

Research Question 2: Acceptability Evaluation User evaluations of acceptability are generally negative, though acceptance levels vary based on technical knowledge, gaming habits, and availability of alternatives. Most users express concerns but ultimately accept kernel-level anti-cheat when required for game access. Technically literate users demonstrate lower acceptance rates, while competitive gamers show higher acceptance despite concerns [2, 3].

Research Question 3: Primary Concerns Privacy, security vulnerabilities, and lack of transparency emerge as the dominant concerns. Privacy concerns centre on unrestricted system access and data collection capabilities. Security concerns focus on vulnerability risks and system compromise potential. Transparency concerns reflect frustration with vague or unverifiable company statements about data collection and monitoring practices [1, 3, 2].

Research Question 4: Trust Levels Trust levels are generally low, driven by transparency issues, proprietary code, and forced adoption requirements. Companies providing detailed documentation receive relatively higher trust, but skepticism remains widespread. The forced binary choice (accept anti-cheat or lose game access) erodes trust by suggesting company priorities override user privacy preferences [2, 3].

Research Question 5: Influencing Factors Technical knowledge, gaming habits, prior experiences, and awareness of security incidents all influence perceptions. Technical knowledge correlates most strongly with concerns and lower acceptance. Gaming engagement levels and competitive participation influence acceptance despite concerns. Negative experiences amplify concerns, while awareness of vulnerabilities heightens risk perception [3, 2, 1].

Research Question 6: Research Gaps Critical gaps include lack of empirical quantitative studies, absence of student-focused research, no longitudinal studies, limited cross-cultural analysis, insufficient research on trust dynamics, and minimal investigation of privacy-fairness trade-off evaluations.

4.3 Evaluating Propositions

Evidence supports Proposition P1 (awareness correlates with privacy concerns): technically aware users consistently express stronger privacy concerns [3]. Proposition P2 (lower trust toward companies) receives strong support from community discussions demonstrating widespread skepticism [2]. Proposition P3 (technical knowledge correlates with concerns) is well-supported by technical community perspectives [3]. Proposition P4 (willingness to sacrifice privacy) is supported by adoption patterns despite concerns [4, 2]. Proposition P5 (invasiveness negatively correlates with acceptance) receives partial support. Acceptance persists despite high invasiveness perceptions, suggesting other factors—game popularity and lack of alternatives—also influence acceptance decisions [2].

4.4 Effectiveness Versus Privacy Trade-Off

A central tension in the kernel-level anti-cheat debate concerns whether enhanced detection effectiveness justifies privacy costs. However, empirical comparison of effectiveness presents significant methodological challenges. Controlled comparative studies are difficult to conduct: cheat developers actively evade detection, creating an adversarial environment where detection rates change rapidly. Additionally, companies rarely disclose detailed effectiveness metrics, citing competitive security reasons. Published comparisons often rely on anecdotal evidence or company claims rather than independent verification.

Despite measurement difficulties, developers consistently justify kernel-level implementations based on superior detection capabilities against sophisticated cheats that exploit kernel-level vulnerabilities themselves. The technical rationale posits that advanced cheat techniques, including kernel-mode drivers and memory manipulation at Ring 0, require equivalent privilege levels for reliable detection. This architectural argument suggests that user-level anti-cheat systems face fundamental limitations against sophisticated threats, though quantitative evidence validating this claim remains limited in public sources.

The effectiveness-privacy tension reflects a fundamental question: whether the assumed security benefits justify the privacy and security risks inherent in kernel-level access. Users, particularly those with technical knowledge, frequently question whether effectiveness gains are substantial enough to warrant the security exposure that kernel-level drivers create. This questioning occurs despite limited empirical data on comparative effectiveness, highlighting how perceived trade-offs, rather than verified effectiveness differences, shape user acceptance.

4.5 Ethical Implications

Significant ethical concerns surround kernel-level anti-cheat systems. The forced adoption model raises questions about informed consent and user autonomy. Users face a binary choice that effectively coerces acceptance regardless of privacy preferences, challenging principles of informed consent and user agency [2, 3].

The transparency deficit creates ethical concerns about accountability and user rights. Users cannot verify company claims about data collection and monitoring, creating an asymmetric information relationship that disadvantages users [3]. This asymmetry raises questions about fair terms of service and meaningful consent.

Security vulnerability risks present ethical dilemmas regarding responsibility. When kernel-level anti-cheat systems introduce vulnerabilities, companies control security-critical software that users cannot avoid if they wish to access purchased games [1]. This creates accountability questions about security failures in required software.

4.6 Limitations of the Literature

Several limitations affect this literature review. First, sources predominantly reflect Western perspectives, limiting cross-cultural understanding. Second, community discussions may overrepresent negative reactions, as satisfied users may not participate in public discourse. Third, the absence of empirical quantitative research means findings rely on qualitative analysis and anecdotal evidence. Fourth, rapidly evolving technology means perceptions may change as users become more familiar with kernel-level anti-cheat. Finally, company perspectives are underrepresented, potentially missing legitimate justifications for kernel-level implementations.

Despite these limitations, the synthesis provides valuable insights into current user perceptions and identifies critical areas requiring further investigation.

5 Conclusion

This literature review has synthesized existing knowledge on user perceptions of kernel-level anti-cheat systems, revealing a landscape marked by significant concerns, reluctant acceptance, and a clear divide between technically literate and general users. The review contributes to understanding how users evaluate the privacy-fairness trade-off inherent in modern anti-cheat systems.

5.1 Key Findings Summary

The review demonstrates that user perceptions are predominantly negative, driven by privacy concerns, security vulnerability risks, and low trust levels toward game develop-

ers. Despite these concerns, widespread adoption (338 games implementing kernel-level anti-cheat [4]) indicates reluctant acceptance due to limited alternatives and desire for fair gameplay. Technical literacy emerges as the strongest predictor of perception patterns, with technically literate users, including students in cybersecurity and related fields, expressing stronger concerns and lower acceptance levels compared to general users.

The privacy-fairness trade-off represents a central tension: users value both competitive integrity and privacy, but existing systems force a binary choice. Most users reluctantly sacrifice privacy for game access, though technically literate users demonstrate higher resistance. Trust levels remain low, driven by transparency deficits, proprietary code, and forced adoption requirements. This pattern indicates that behavioural acceptance does not reflect attitudinal approval, as users may comply with requirements while maintaining strong disapproval.

5.2 Main Contributions

This review contributes several key insights that advance understanding beyond existing fragmented literature. First, it systematically synthesizes fragmented knowledge across academic discourse, technical documentation, and community perspectives, creating the first comprehensive overview of user perception patterns. This synthesis enables identification of consistent themes and contradictions that individual sources cannot reveal. Second, it identifies technical literacy as a critical factor shaping perceptions, with implications for understanding how students and future technology professionals evaluate privacy-security trade-offs. Third, it documents the privacy-fairness tension that characterizes user decision-making, revealing how acceptance patterns differ from approval. Fourth, it identifies critical gaps in empirical research, providing a roadmap for future investigation priorities. Together, these contributions establish a foundation for evidence-based discussions of kernel-level anti-cheat systems and inform both academic research directions and industry practice considerations.

5.3 Implications for Developers and Policymakers

For game developers, findings suggest that transparency and communication significantly influence trust and acceptance. Companies providing detailed technical documentation, clear explanations of data practices, and verifiable security implementations may face less skepticism. However, fundamental concerns about kernel-level access persist regardless of transparency efforts, suggesting that technical solutions alone may not fully address user concerns.

The forced adoption model emerges as a significant trust and acceptance barrier. Developers might consider alternative approaches that provide meaningful choice, such as opt-in kernel-level modes for competitive play while maintaining user-level anti-cheat for

casual modes. Such approaches could respect user privacy preferences while maintaining competitive integrity.

For policymakers, findings highlight privacy and security concerns surrounding required kernel-level software. The lack of meaningful consent, transparency deficits, and security vulnerability risks suggest potential need for regulation or industry standards. Policy considerations might include requirements for transparency, data minimization, security auditing, and meaningful user choice.

The findings regarding technical literacy and student perspectives suggest that future technology professionals entering the industry will bring heightened privacy awareness and skepticism toward invasive security measures. This may influence industry practices as these professionals assume development and policy roles.

5.4 Recommendations for Future Research

This review identifies critical research gaps requiring empirical investigation. Priority areas include:

1. **Quantitative Empirical Studies:** Systematic survey-based research measuring user awareness, concerns, trust, and acceptance across diverse demographics.

2. **Student-Focused Research:** Studies specifically examining perceptions among students in technical fields, addressing how technical education shapes privacy and security perspectives.

3. **Longitudinal Studies:** Research tracking perception evolution over time, particularly as users gain familiarity with kernel-level anti-cheat or after security incidents.

4. **Cross-Cultural Analysis:** Investigation of regional and cultural differences in acceptance patterns and privacy concerns.

5. **Trust Dynamics Research:** Empirical studies examining trust formation, factors influencing trust, and impact of transparency initiatives.

6. **Privacy-Fairness Trade-off Studies:** Research quantifying how users evaluate trade-offs and what factors influence willingness to sacrifice privacy.

7. **Effectiveness Comparison:** Studies comparing kernel-level versus user-level anti-cheat effectiveness, enabling informed cost-benefit evaluations.

5.5 Concluding Remarks

Kernel-level anti-cheat systems represent a significant technological and ethical development in gaming security, raising fundamental questions about privacy, trust, and user

agency. Evidence indicates that users, particularly those with technical literacy, recognize and express concerns about these implications while often accepting systems due to limited alternatives. As these technologies continue to proliferate—currently implemented in 338 games [4]—understanding user perceptions becomes increasingly important for developers, policymakers, and the academic community.

The clear divide between technically literate and general users suggests that as technical education expands and privacy awareness increases, acceptance patterns may shift. Students in technical fields, representing future industry professionals and informed technology users, demonstrate heightened concerns that may influence future industry practices. This makes their perspectives particularly valuable for understanding both current perceptions and future trajectories.

Addressing the identified research gaps through empirical investigation will provide the evidence base needed to inform industry practices, policy considerations, and ethical frameworks surrounding kernel-level anti-cheat systems. Such research will contribute to developing approaches that balance security needs, competitive integrity, and user privacy in ways that respect user agency and informed consent.

References

References

[1] XDA Developers. "Kernel-level anti-cheats are the next tech disaster waiting to happen." https://www.xda-developers.com/kernel-level-anti-cheat-tech-disaster/

[2] Reddit. "The insanity of EA's anti-cheat system." https://www.reddit.com/r/gaming/comments/xf1cwr/the_insanity_of_eas_anticheat_system_by_a_kernel/

[3] GitHub Gist. "Why You Should Reconsider Playing League of Legends: The Risks of Kernel-Level Anti-Cheat." https://gist.github.com/stdNullPtr/2998eacb71ae925515360410af6f0a32

[4] Levvvel. "Every game with kernel-level anti-cheat software (2024)." https://levvvel.com/games-with-kernel-level-anti-cheat-software/

[5] YouTube – PirateSoftware. "Kernel-level anti-cheat explained." https://www.youtube.com/watch?v=GrzuiJezZEo