1. Introduction

- **Context & Background**
  - Explain what anti-cheat systems are and why they exist.
  - Describe the rise of competitive online gaming and the problem of cheating.
  - Define **kernel-level anti-cheat** vs **user-level anti-cheat**.
  - Mention examples: Vanguard (Valorant), Easy Anti-Cheat, BattlEye, etc.
- **Problem Statement**
  - The main issue: Kernel-level anti-cheats run at the highest privilege level in the OS — raising security and ethical concerns.
- **Research Questions**
  - How does kernel-level anti-cheat work compared to user-level anti-cheat?
  - What are the potential security risks?
  - Is it worth exposing system data for a cheat-free experience?
  - Is kernel-level anti-cheat ethical?
- **Hypothesis**
  - Example: *“Kernel-level anti-cheat systems provide stronger protection against cheaters than user-level ones, but pose significant security and ethical trade-offs.”*

---

2. Methods

- **Research Methodology**
  - Literature review: analyze technical papers, cybersecurity reports, and case studies (e.g., Riot Vanguard, ESEA, Valorant).

    - Comparative analysis: compare architecture and performance of kernel-level vs user-level systems.
    - Ethical analysis: use frameworks (like utilitarianism or rights-based ethics) to evaluate privacy impact.
- **Data Sources**
    - Technical documentation, whitepapers, academic papers, online security communities, and player feedback.

---

3. Results

- **Technical Comparison**
    - Table showing differences between user-level and kernel-level:
        - Access level
        - Detection rate
        - Resource use
        - Risk of exploitation
    - Example findings: Kernel-level provides deeper access to detect cheats but also allows potential abuse or exploits.
- **Security Risks Identified**
    - Potential for rootkit-like behavior.
    - Vulnerability to privilege escalation attacks.
    - Lack of transparency or user control.
- **Community and Ethical Findings**
    - Player trust issues.

    - Debate over “freedom vs fairness” in gaming.

---

4. Discussion

- **Interpretation of Results**
    - Summarize which level performs better technically.
    - Discuss whether the benefits (fair play) justify the risks (privacy, data security).
- **Ethical Perspective**
    - Is it ethical for companies to install drivers that can monitor system-level processes?
    - Compare to real-world analogies (e.g., antivirus permissions vs game anti-cheat).
- **Considerations**
    - Transparency, informed consent, opt-in mechanisms, and open communication by developers.

---

5. Evaluation

- **Answer Your Research Questions**
    - Provide a clear conclusion to each of your listed questions.
- **Limitations**
    - Lack of public data on proprietary anti-cheat systems.
    - Potential bias in player opinions.
- **Future Work**
    - Propose safer anti-cheat designs (sandboxing, AI-based detection, etc.).

6. References

Use a proper reference style (APA/IEEE) for:

- Official documentation (Riot Vanguard, BattleEye, Easy Anti-Cheat).
- Academic research on kernel security.
- News articles about anti-cheat controversies.