This is an auto-generated Threat Modeling Report, assembled by GPT-4 Threat Modeling Agents. The system reviews the specified application architecture. It applies the STRIDE methodology to each component, providing a thorough evaluation of potential security threats, but may still contain errors.

Executive Summary

The STRIDE analysis of our game app's architecture unearthed critical security issues: a spoofing risk within user authentication, a tampering threat to in-app purchases, potential for sensitive data leaks, and vulnerability to Denial of Service (DoS) attacks. Top priorities for immediate action are: Implementing multi-factor authentication to counteract spoofing. Enhancing encryption for in-app transactions to prevent tampering. Securing data transfers to avert information leaks. Fortifying the leaderboard server against DoS attacks. Addressing these concerns is crucial for maintaining robust security and user trust. Immediate remediation will not only protect users but also fortify the app's integrity and market reputation."

Results

Component	Threats	Mitigations