ABSTRACT

CHEAT DETECTION IN COUNTER-STRIKE 2 USING LONG SHORT-TERM MEMORY NETWORKS

Moehammad Azzriel Ilham
21/477994/PA/20724

The widespread use of cheating software, such as aimbots, triggerbots, and spinbots, poses a great threat to the player experience in online competitive first-person shooter (FPS) games, particularly in Counter-Strike 2 (CS2). This undergraduate thesis focuses on detecting aim-assistance cheats by analyzing player aiming behavior extracted from gameplay demo recordings.

A custom parser was developed using the demoparser2 library, enabling extraction of detailed, tick-based gameplay data, including pitch, yaw, player positions, weapon types, kill distances, and player velocities. To enhance the potential of this data, a comprehensive feature engineering was performed, transforming it into 79 distinct motion-based and contextual features. These include angular velocity, acceleration, jerk, aim stability, snap intensity, positional jumpiness, and weapon-specific details. A Long Short-Term Memory (LSTM) neural network was trained on a balanced dataset comprising of 2212 labeled gameplay segments, split into training (70%), validation(15%), and test(15%) sets using stratified sampling.

The final model achieved an accuracy of 77%, with balanced precision and recall, effectively minimizing false positives and reliably identifying cheating behaviors. Early stopping was employed to prevent overfitting, which would stop training when validation loss stopped improving. These results demonstrate the feasibility and potential effectiveness of machine learning-based behavioral analysis for cheat detection in FPS games, laying the foundation for future integration into real-time anti-cheat systems and moderation tools within competitive esports environments.

Keywords: CS2, Cheat Detection, LSTM, Cheating Software, Parsing, Player Behavior