BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Permainan First-Person Shooter (FPS) seperti Valorant dan Counter-Strike 2 merupakan salah satu genre game kompetitif yang sangat populer. Dalam permainan FPS, [1].Keadilan dan keseimbangan kompetitif menjadi aspek penting yang menentukan pengalaman bermain dan kepuasan pemain. Namun, praktik cheating, khususnya speed hack, sering kali mengganggu prinsip keadilan ini. [2].Speed hack adalah bentuk cheat di mana pemain dapat bergerak lebih cepat dari batas normal yang ditentukan oleh sistem permainan, sehingga memberikan keuntungan tidak adil dibanding pemain lain. [3].Namun, seiring meningkatnya popularitas game online kompetitif, muncul pula berbagai bentuk kecurangan atau cheating yang dilakukan oleh pemain untuk memperoleh keuntungan yang tidak adil. Salah satu bentuk kecurangan yang sering terjadi adalah speed hack, yaitu manipulasi kecepatan karakter atau permainan sehingga pemain dapat bergerak lebih cepat dibandingkan pemain lain secara tidak wajar. Hal ini tentunya merusak keseimbangan permainan dan menurunkan kualitas pengalaman bermain bagi pemain lainnya.[4]. Untuk mengatasi masalah tersebut, pengembang game menerapkan berbagai sistem anti-cheat guna mendeteksi dan mencegah tindakan kecurangan. Misalnya, Riot Vanguard anti-cheat yang digunakan pada Valorant serta Valve Anti-Cheat (VAC) yang digunakan pada Counter-Strike 2. Sistem ini bekerja dengan berbagai metode seperti pemantauan memori, validasi data permainan, serta analisis perilaku pemain. [5].Fenomena speed hack di game FPS memiliki dampak yang cukup serius. Selain merusak pengalaman bermain bagi pemain yang jujur, cheat ini juga dapat menurunkan tingkat kepercayaan terhadap game, mengurangi kepuasan pemain, dan memengaruhi reputasi pengembang game. Hal ini menjadi tantangan besar bagi pengembang game kompetitif, karena cheat seperti speed hack sulit sepenuhnya dicegah tanpa sistem anticheat yang efektif. (liputan6.com) [6].Untuk mengatasi kecurangan ini, pengembang game FPS telah menerapkan berbagai sistem anti-cheat. Valorant menggunakan Riot Vanguard, sistem anti-cheat berbasis kernel yang berfungsi untuk mendeteksi aktivitas mencurigakan, termasuk cheat yang memanipulasi kecepatan pemain. Sementara itu, Counter-Strike 2 menggunakan Valve Anti-Cheat (VAC) untuk memantau perilaku pemain dan

memastikan integritas permainan. Kedua sistem ini bertujuan untuk menjaga *fair play* dan mencegah *cheat* merusak ekosistem game. (en.wikipedia.org/wiki/Riot_Vanguard, en.wikipedia.org/wiki/Valve_Anti-Cheat) [7].Meski demikian, laporan komunitas menunjukkan bahwa *cheat* seperti *speed hack* masih terjadi, khususnya di server kompetitif, karena para pemain jahat selalu mencoba memanfaatkan celah yang ada. Hal ini menunjukkan bahwa meskipun ada sistem *anticheat* canggih, *cheat* tetap menjadi ancaman nyata bagi keseimbangan permainan. Oleh karena itu, penelitian mengenai teknik *anti-cheat* sederhana menjadi relevan, khususnya yang fokus pada validasi pergerakan pemain untuk mencegah *speed hack*. [8].Pendekatan ini dapat dijadikan model konseptual yang mudah diterapkan pada game FPS, sekaligus menjadi dasar akademis untuk studi lebih lanjut mengenai anti-cheat. (reddit.com/r/VALORANT) [9].Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis dan mensimulasikan teknik *anti-cheat* sederhana yang dapat mencegah *speed hack* pada game FPS, dengan studi kasus pada *Valorant* dan *Counter-Strike 2*. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan model *anti-cheat* berbasis validasi pergerakan pemain, yang bersifat konseptual dan aman secara akademis tanpa membongkar sistem *anti-cheat* asli dari game tersebut. [10]. Pada game *Counter-Strike 2*, sistem keamanan yang digunakan adalah ***Valve Anti-Cheat (VAC)*** yang dikembangkan oleh ***Valve Corporation***. Sistem ini bekerja dengan cara melakukan pemindaian terhadap file permainan dan memori sistem untuk mendeteksi program pihak ketiga yang berpotensi memberikan keuntungan tidak adil kepada pemain. VAC memiliki mekanisme ban tertunda *(delayed ban)*, yaitu pemain yang terdeteksi menggunakan cheat tidak langsung diblokir, tetapi akan diblokir pada waktu tertentu agar metode deteksi tidak mudah dipelajari oleh pembuat cheat. Sementara itu, pada game Valorant, sistem anti-cheat yang digunakan adalah ***Riot Vanguard anti-cheat*** yang dikembangkan oleh ***Riot Games***. Berbeda dengan VAC, Riot Vanguard menggunakan pendekatan yang lebih agresif dengan menjalankan driver pada level kernel *(kernel-level driver)* di sistem operasi. Hal ini memungkinkan sistem untuk memonitor aktivitas program secara lebih dalam sejak komputer dinyalakan, sehingga berbagai bentuk cheat termasuk manipulasi kecepatan permainan dapat dideteksi lebih awal. IEEE, “Anti-Cheat Mechanisms in Online Gaming Systems,” IEEE Xplore Digital Library, 2018.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaiamana karakteristik *speed hack* pada game FPS, khususnya pada Valorant dan *Counter-Strike* 2 (Fokus pada perilaku pemain yang bergerak melebihi kecepatan normal dan indikator anomali pergerakan.)
2. Teknik *anti-cheat* sederhana seperti apa yang dapat diterapkan untuk mendeteksi dan mencegah *speed hack* pada game FPS? (Fokus pada metode validasi pergerakan pemain berbasis *rule-based* atau *threshold*)
3. Seberapa efektif model *anti-cheat* sederhana dalam mendeteksi speedhack melalui simulasi pergerakan pemain? (Fokus pada evaluasi hasil simulasi dan kemampuan model dalam membedakan pemain normal dan pemain curang)
4. Apa rekomendasi pengembangan model *anti-cheat* sederhana yang aman dan praktis untuk diterapkan pada game FPS kompetitif? (Fokus pada aspek konseptual dan akademis, tanpa membongkar sistem *anti-cheat* asli.)

1.3 Batasan Masalah

Agar penelitian ini lebih fokus, praktis, dan aman secara akademis, maka batasan masalah penelitian ditetapkan sebagai berikut:

1. Studi kasus difokuskan pada game FPS Valorant dan Counter-Strike 2. Analisiss dilakukan secara konseptual dan simulatif, tanpa mengakses atau membongkar sistem anti-cheat asli (Riot Vanguard atau VAC).
2. Penelitian hanya menganalisis dan mensimulasikan *anti-cheat* sederhana berbasis validasi pergerakan pemain, menggunakan metode *rule-based* atau *threshold-based*. Sistem *anti-cheat* tingkat kernel atau client-side kompleks tidak diterapkan.
3. Data yang digunakan berasal dari simulasi pergerakan pemain pada game FPS sederhana atau data ilustratif, bukan data asli pemain Valorant/*Counter-Strike* 2. Fokus simulasi pada perbandingan antara pergerakan normal dan pergerakan yang melebihi batas kecepatan.Penelitian ini dilakukan dalam kondisi istirahat sambil duduk.
4. Penelitian ini menghasilkan model konseptual *anti-cheat* sederhana dan analisis efektivitasnya melalui simulasi. Tidak melakukan implementasi langsung ke server atau sistem game komersial.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis dan Mensimulasikan anti-cheat sederhana guna mendeteksi dan mencegah speed-hack pada game FPS, dengan studi kasus pada Valorant dan Counter-Strike 2, sehingga dapat menjaga keadilan dan kedeimbangan permainan.

2. Menganalisis karakteristik speed hack pada game FPS, khususnya pada Valorant dan *Counter-Strike* 2, untuk mengetahui perilaku pemain yang melebihi batas kecepatan normal.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah:

1. Memberikan kontribusi pengetahuan mengenai teknik *anti-cheat* sederhana khusus untuk mendeteksi *speed hack* pada game FPS.
2. Menjadi referensi atau dasar bagi penelitian selanjutnya mengenai pengembangan sistem *anti-cheat* secara konseptual.
3. Membantu mahasiswa atau peneliti lain dalam memahami analisis *cheat* dan metode simulasi *anti-cheat* pada game kompetitif