Cyber Security in Online Games: Cheating Detection and Prevention

Salma Fedora - 18217007
Sistem Teknologi Informasi, Sekolah Teknik Elektro dan Informatika (STEI), Institut Teknologi Bandung, Bandung, Indonesia

Abstrak - Di era modern ini, *game online* menjadi salah satu kegiatan yang lumrah dilakukan di kalangan masyarakat, baik oleh anak-anak maupun dewasa, ditambah lagi dengan peningkatan pesat kemampuan *hardware*, *software*, dan internet dalam menunjang kenyamanan dalam bermain *game online*. Hal tersebut memacu para *game developer* untuk mengembangkan lebih banyak *game* lagi. Namun, dampak yang ditimbulkan adalah meningkatnya masalah *cyber security*, yang diantaranya adalah maraknya perilaku *cheating* dan *hacking* dari pihak yang tidak bertanggung jawab. Masalah ini menyebabkan kerugian besar bagi *gamer* maupun *game developer*. Agar tercapai empat aspek tradisional keamanan - kerahasiaan, integritas, ketersediaan, dan keaslian sistem, dibutuhkan suatu teknik keamanan yang baik dalam mengembangkan dan mengoperasikan game online. Makalah ini akan menjelaskan berbagai macam jenis *cheating*, cara pendekatan untuk mendeteksi para *cheater* dan *hacker,* serta bagaimana cara untuk mencegahnya.

1. PENDAHULUAN

Dengan pesatnya perkembangan teknologi dan internet, *game online* menjadi salah satu aplikasi paling populer di internet [6]. Namun, tidak dipungkiri kecurangan telah menjadi fenomena penting dalam *game* saat ini. Penelitian terbaru menunjukkan bahwa menyontek sebenarnya adalah masalah baru lagi, masalah

keamanan utama untuk game komputer online [5]. Melalui *loophole* atau celah keamanan yang tidak memadai*, online cheating* menjadi marak dalam dunia *game* [1]. Oleh karena itu, dibutuhkan sebuah penelitian terhadap kasus *online cheating* sehingga dapat menguntungkan studi keamanan dalam aplikasi internet, khususnya dalam bidang *online game*.

Namun, studi dalam *online cheating* belum dipelajari secara menyeluruh seperti yang diharapkan. Hal ini disebabkan oleh tiga faktor; *online cheating* merupakan topik yang relatif baru dalam dunia *cyber security*, banyaknya variasi *online game* membuat fenomena ini menjadi lebih rumit, serta banyaknya kecurangan berbeda telah ditemukan tetapi sering diklasifikasikan dengan serangan keamanan biasa [2].

Sebagian besar kasus *online cheating* terjadi karena buruknya desain keamanan dalam *game* [2]. Hal ini menunjukkan bahwa banyak pengembang *game* yang tidak memiliki keahlian dalam bidang keamanan. Padahal, hal tersebut sangatlah penting untuk bertahan dari serangan *cheater*. Dengan demikian, dibutuhkan suatu kolaborasi yang baik antara pihak pengembang dengan spesialis keamanan, sehingga tidak hanya membentuk desain sistem yang baik agar dapat meminimalkan kemungkinan eksploitasi, namun juga dapat membantu mengidentifikasi sisa kecurangan yang ada selama sistem evaluasi.

Makalah ini menyajikan tentang klasifikasi *online cheating*, disertai dengan penyajian berbagai metode untuk mencegah dan mengatasi perilaku *online cheating* dengan harapan bahwa pembahasan ini dapat meningkatkan pemahaman masyarakat tentang fenomena *online cheating*.

2. CHEATING AND HACKING IN ONLINE GAMES

Dalam perilaku *cheating* dan *hacking* dalam *online game*, banyak sekali dampak buruk yang ditimbulkan, mulai dari pencurian data dan informasi pemain, penolakan layanan, kegagalan integritas, penyamaran, hingga pelanggaran keadilan [2]. Beragamnya bentuk perilaku kecurangan membuat semakin banyak cara untuk mengeksploitasi *loophole* dalam sistem. Oleh karena itu, pihak pengembang harus mengenal jenis-jenis kecurangan sehingga dapat bergerak dengan cepat dalam mengatasi perilaku *cheating* dan *hacking*. Berikut ini adalah penjelasan tentang bentuk-bentuk kecurangan, teknik peretasan, serta implementasi dari kecurangan itu sendiri.

2.1. CHEATING FORMS

Kecurangan dalam *game online* dibagi menjadi 15 bentuk [2], diantaranya adalah sebagai berikut.

1. ***Cheating due to misplace trust*** terjadi ketika *cheater* menyalahgunakan kepercayaan pengguna terhadap sistem dengan cara memodifikasi data dan/atau kode dari sisi *client*. Biasanya, kecurangan ini terjadi karena kepercayaan yang berlebih terhadap keamanan sebuah sistem. Padahal, tidak ada sistem yang 100% aman di dunia ini. Umumnya kecurangan ini dilakukan dalam *single player games*.
2. ***Cheating by collusion*** terjadi ketika para pemain bekerja sama untuk mencapai objektif game, namun dengan melakukan kecurangan. Kecurangan ini dapat terjadi karena gagalnya implementasi interaksi manusia-komputer pada fase operasional dalam sistem *game*. Biasanya, kecurangan ini dilakukan dalam *multiplayer games* yang memiliki peringkat atau *rank*.
3. ***Cheating by abusing game procedure*** terjadi ketika *cheater disconnect* atau keluar dari *game* ketika menyadari bahwa mereka akan kalah dalam suatu *game*, sehingga mereka dapat menghindari kekalahan. Hal ini disebabkan oleh buruknya sistem permainan serta tidak diberlakukannya sistem *punishment* terhadap orang yang meninggalkan *game* sebelum permainan berakhir. Dampak dari kecurangan ini adalah mengakibatkan ketidakadilan bagi pemain lainnya. Biasanya, kecurangan ini dilakukan dalam *multiplayer games* yang memiliki peringkat atau *rank*.
4. ***Cheating related to virtual assets***. Dalam *game online*, seringkali terdapat barang virtual yang hanya bisa didapatkan apabila pemain memiliki waktu dan kemampuan bermain *game* yang bagus, sehingga mereka cenderung untuk membeli barang tersebut untuk bisa mendapatkannya dengan cepat. Namun, hal tersebut mengakibatkan celah bagi para penipu untuk mendagangkan barang virtual di situs lelang seperti eBay ataupun di aplikasi *e-Commerce* seperti Tokopedia, sehingga mereka menerima uang nyata untuk barang

virtual tersebut tetapi tidak pernah mengirimkannya ke pelanggan sesuai dengan persetujuan awal.

5. ***Cheating due to machine intelligence***. Kecerdasan buatan juga dapat menjadi alat untuk memperoleh keunggulan dalam sebuah game secara curang. Kecurangan ini dapat terjadi apabila *game* memungkinkan untuk dimodelkan sebagai *computational problem*.
6. ***Cheating by modifying client infrastructure via graphic driver***. Dengan modifikasi pada *graphic driver*, *cheater* dapat membuat suatu benda menjadi transparan. Akibatnya, *cheater* dapat mengetahui posisi pemain lain dalam *game* yang seharusnya tertutupi oleh benda tersebut.
7. ***Cheating by denying services to peer players*** terjadi ketika *Cheater* melakukan *flooding* ke koneksi jaringan korban, sehingga menimbulkan kesan seakan terjadi gangguan pada koneksi jaringan. Dampak yang ditimbulkan adalah melambatnya respons yang diterima oleh korban atau *lagging*. Kecurangan ini dapat terjadi karena buruknya desain sistem.
8. ***Timing cheating*** ini umumnya terjadi pada *real-time online games. Cheater* dengan sengaja menunda aksinya sendiri sampai ia mengetahui gerakan apa yang akan dilakukan oleh lawannya. Kemudian, *cheater* memberikan pesan pada waktu yang “tepat” kepada lawannya
9. ***Cheating by compromising passwords***. Kata sandi merupakan hal yang krusial dalam menjaga keamanan data serta otorisasi pemain dalam sebuah *game*. Dengan mengetahui kata sandi korban, *cheater* dapat mengalami pencurian barang dalam *game*, harta benda, bahkan informasi pribadi. Hal ini dapat diatasi dengan pemberian prosedur dan panduan rinci dalam pemilihan kata sandi oleh pihak pengembang *game*.
10. ***Cheating due to lack of secrecy***. Karena kurangnya kerahasiaan sistem, *cheater* dapat menipu dengan menguping paket dan menyisipkan, menghapus, atau memodifikasi acara permainan atau perintah yang dikirimkan melalui jaringan. Kecurangan ini dapat mengakibatkan pencurian data pribadi.

11. ***Cheating due to lack of authentication.*** Jika tidak ada mekanisme yang tepat untuk mengotentikasi server *game* ke *client*, *cheater* dapat mengumpulkan ID dan kata sandi dari pemain sah dengan cara membuat server *game* yang palsu.
12. ***Cheating by exploiting a bug or loophole.*** Kecurangan ini dilakukan dengan mengeksploitasi bug atau celah yang ada dalam *game*, tanpa melakukan modifikasi apapun terhadap kode atau data. Konsekuensi dari kecurangan ini beragam, mulai dari ketidakadilan antar pengguna sampai dengan kerugian material yang dialami oleh pihak pengembang *game*.
13. ***Cheating by compromising game servers*** terjadi ketika *cheater* mendapatkan akses untuk memodifikasi server *game* yang bersangkutan sehingga dapat mengubah konfigurasi sesuai yang diinginkan. Akibatnya, terjadi pelanggaran integritas yang mengeksploitasi ketidakmampuan dasar desain sistem.
14. ***Cheating related to internal misuse*** terjadi ketika administrator *game* yang memiliki akses untuk mengelola sistem menyalahgunakan hak istimewanya untuk melakukan pelanggaran integritas. Contoh dari pelanggaran ini adalah modifikasi *database game*.
15. ***Cheating by social engineering.*** Dengan membuat korban percaya dengan suatu hal yang menarik atau dengan membuat korban percaya dengan suatu hal yang bersifat mengganggu, *Cheater* menipu pemain lain agar meyakini bahwa mereka perlu menyerahkan data diri mereka berupa ID dan kata sandi.

Dari jenis-jenis kecurangan tersebut, dapat dibentuk **tabel distribusi bentuk kecurangan dalam matriks kerentanan-konsekuensi** yang menggambarkan dampak kerentanan *cyber security* apa saja yang ditimbulkan.

	Info Theft	*Service Denial*	*Integrity Failure*	*Masquerade*	*Fairness Violation*
Design inadequacy in the game system	1, 2, 10	7	1	11	3, 5, 8, 12

Design inadequacy in the underlying system		7	6, 13		
Vulnerability in player	9, 15				4
Vulnerability in insider			14		

Tabel 1 . Distribusi bentuk kecurangan dalam matriks kerentanan-konsekuensi

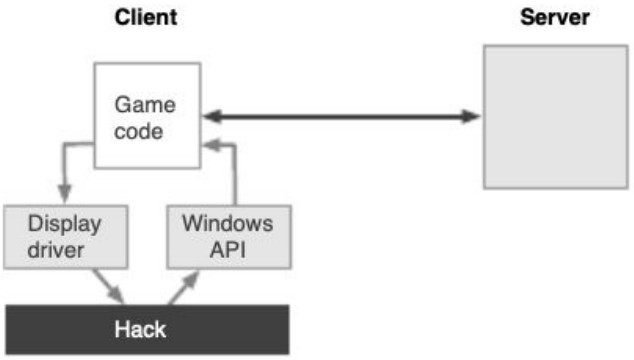
Berdasarkan matriks tersebut, dapat disimpulkan bahwa sebagian besar jenis *online game* adalah tentang pencurian informasi, modifikasi karakteristik permainan yang ilegal, pelanggaran keadilan, dan pengeksploitasian kelemahan dalam sistem permainan.

Pencurian identitas virtual terjadi ketika seorang pemain di dunia nyata memperoleh kendali atas *avatar* pemain lain dengan meretas, mengeksploitasi celah, rekayasa sosial, dan cara lainnya. Pencurian identitas dapat menyebabkan aksi pelanggaran lain, yaitu *impersonation* atau berpura-pura menjadi orang lain. Di sini, aspek sosial dieksploitasi oleh *cheater* sehingga mereka mendapatkan keuntungan lebih untuk avatar mereka. Dampak yang ditimbulkan sangatlah berbahaya, karena dapat menimbulkan dampak finansial dan kerugian pribadi yang serius [4].

2.2. HACKING TECHNIQUES

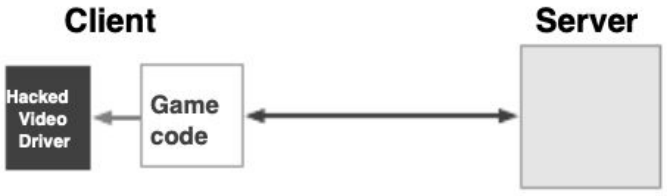
Terdapat berbagai macam cara untuk melakukan kecurangan dalam *game*, diantaranya adalah dengan melakukan *hacking. Hacking* dapat berupa modifikasi pada kode *game* maupun *environment*-nya*,* serta memiliki tingkat kompleksitas dan efektivitas yang berbeda [1]. Berikut ini adalah teknik-teknik *hacking* yang kerap dilakukan.

1. ***Hard-coded hacks*** diimplementasikan dengan memodifikasi dan mengganti kode pada *file client* yang telah diinstal. Teknik ini mudah dideteksi karena kode *game* diubah secara langsung oleh *hacker*.
2. ***External hacks***. Berbeda dengan teknik *hard-coded hacks*, teknik ini tidak mengubah kode *client* secara langsung. Sebaliknya, teknik ini mempengaruhi *game* melalui sebuah perantara tertentu.



Gambar 1. External Hacks

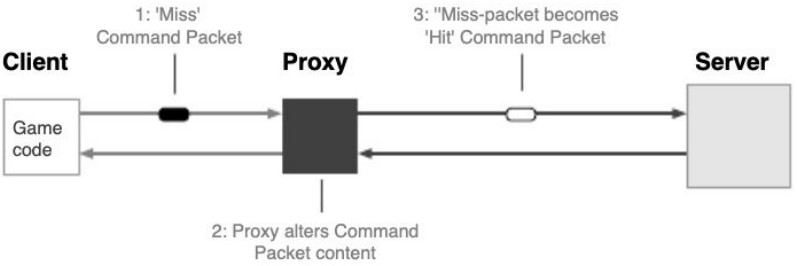
3. ***Environment hacks*** melibatkan perubahan *environment* atau lingkungan komputasi tempat *client* berjalan dengan tujuan untuk melakukan *cheating*. Berbeda dengan *hard-coded hack*, teknik ini tidak mengubah kode apapun dalam *game*. Teknik ini juga berbeda dengan *external hack* karena tidak adanya proses unik dan independen yang terlibat. Umumnya, teknik ini memodifikasi *driver* dengan membuat suatu objek menjadi semi transparan.



Gambar 2. Environment Hacks

4. ***Hook Hacks*** menjalankan game melalui proses *harness*, bukan dari *game executable*. Dengan menggunakan *harness*, *hook* dapat membaca, mengontrol, dan memasukkan data ke lokasi memori game. *Hook* diprogram untuk mengetahui lokasi memori yang penting, seperti posisi pemain.
5. ***Packet tampering*** merupakan teknik yang memodifikasi isi konten dari paket. Berbeda dengan teknik-teknik sebelumnya, teknik ini sama sekali tidak mengubah kode *game* maupun *environment*. Dalam implementasi teknik ini, dibentuk sebuah mesin eksternal yang bertindak sebagai server *proxy* ke sistem *client*. Server tersebut akan menjalankan program untuk memeriksa paket yang masuk dan keluar. Kemudian, server tersebut akan mempelajari bagaimana keadaan dari

game-world yang sedang dijalankan. Dengan cara ini, *proxy* dapat membangun informasi dasar, sepert posisi pemain di *game* tersebut. *Packet tampering* merupakan teknik yang paling kompleks, namun paling susah dideteksi.



Gambar 3. Packet Tampering

2.3. CHEATING IMPLEMENTATION

Padai bagian sebelumnya, telah dijelaskan teknik-teknik untuk melakukan kecurangan dengan *hacking*. Bagian ini membahas secara singkat proses eksploitasi game pada tingkat selanjutnya, yaitu implementasi *cheat* yang umum dilakukan [1, 8, 9].

1. ***Wall hacking*** memungkinkan *cheater* untuk melihat dinding secara tembus pandang, sehingga ia dapat pergerakan pemain lain dan memberi kerugian besar bagi pemain lainnya.
2. ***Aim-bots*** - biasa digunakan dalam *game* bergenre *first-person-shooter* (FPS), implementasi ini berfungsi untuk memberikan kemampuan dalam membidik pemain lain dengan tepat.
3. ***ESP*** memberikan *cheater* akses ke informasi yang seharusnya bersifat rahasia, sehingga memberikan ketidakadilan bagi pemain lain. Contohnya adalah memberikan informasi lokasi musuh di peta yang seharusnya bersifat *hidden*.
4. ***Bang-hacking*** memberikan kekebalan terhadap efek *blinding* dari *grenade* dalam game *first-person-shooter* (FPS).
5. ***Content-based cheats*** memodifikasi konten *in-game*, seperti *texture* dalam *game*.
6. ***Camera hack*** memungkinkan *cheater* untuk melihat tempat yang jauh dari posisinya dalam *game* sehingga mereka dapat merespons *event* dengan lebih cepat. Dalam DOTA 2, 1,1% dari pemain pernah menyalahgunakan *hack* ini.

3. CHEATING DETECTION AND PREVENTION APPROACH

Banyaknya jenis dan cara untuk melakukan *online cheating* membuat pihak pengembang harus lebih waspada dan inovatif dalam mengembangkan sistem deteksi dan pencegahan *online cheating*. Oleh karena itu, mereka telah mengembangkan cara-cara berikut untuk mendeteksi dan mencegah kecurangan yang terjadi dalam *game.*

3.1. DELAYED BAN

Alat pendeteksi kecurangan tradisional memiliki kemampuan yang terbatas dalam mendeteksi dan mencegah kecurangan. Faktanya, *cheater* dapat dengan mudahnya berpindah dari satu eksploitasi ke eksploitasi lainnya ketika kecurangan mereka terdeteksi.

Dengan demikian, digunakanlah sistem *delayed ban*, yaitu sistem yang dapat menunda penangkapan *cheater* dalam upaya untuk menangkap lebih banyak pemain ilegal. Namun, teknik ini juga kurang terotomatisasi, membutuhkan intervensi manual (misalnya: administrator perlu meminta dan memeriksa tangkapan layar secara manual untuk bukti kecurangan), serta sangat *game-specific*. Contoh pihak pengembang *game* yang menggunakan sistem ini adalah Valve [10].

3.2. BEHAVIOURAL-MONITORING APPROACH TO AUTOMATED CHEAT DETECTION

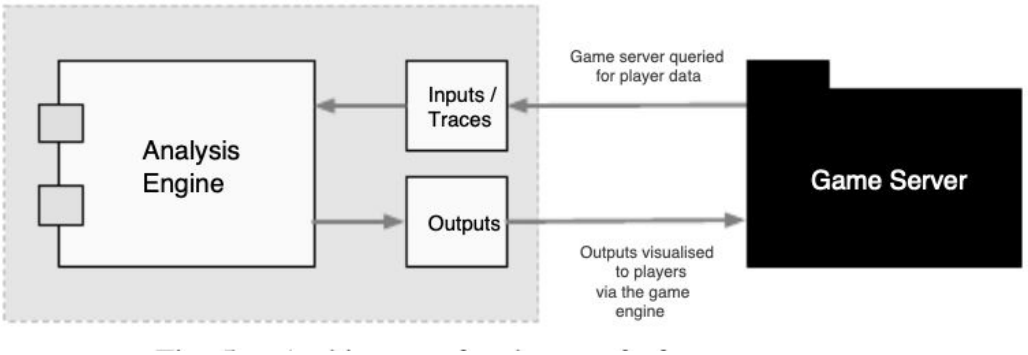
Dengan sistem ini, kecurangan dapat dideteksi dengan memerhatikan perilaku *real-time* para pemain. Selain itu, dilakukan juga pemantauan waktu dan analisis gerakan dari pemain di dalam *game*. Berdasarkan pada hipotesis sentral, pemain yang terlibat dalam kecurangan akan menunjukkan perilaku yang secara signifikan dapat dibedakan dari perilaku pemain normal [1].

Behavioral detection ini sangat berkaitan dengan *intrusion detection*, sehingga sistem bergantung pada dua strategi; pengenalan *signature* dan klasifikasi perilaku dengan menggunakan analisis statistik untuk mengidentifikasi perilaku anomali dalam jaringan, perangkat lunak, ataupun aplikasi [1].

3.3. PROOF-OF-CONCEPT SYSTEM

Proof-of-concept system ini dikembangkan sebagai *plugin* server *source-engine* untuk memonitor para pemain di dunia *game*, dan dirancang untuk mengimplementasikan *cheat-detection* melalui analisis perilaku pemain

yang telah diuraikan pada bagian 3.2 [1]. Tujuan dari *proof-of-concept system* untuk menyediakan implementasi sesederhana mungkin dengan efektivitas yang menjanjikan. Untuk mencapai tujuan tersebut, sistem ini dirancang hanya untuk menangani satu jenis cheat, yaitu wall-hacking dalam *game first-person-shooter (FPS).* Meskipun masih dalam tahap pengembangan, namun sistem ini mempunyai masa depan yang menjanjikan untuk *cyber security* dalam *online games*.



Gambar 4. Architecture of proof-of-concept system

Gambar di atas menunjukkan tentang gambaran *high-level* implementasi arsitektur dari sistem. *Analysis engine* dipisahkan dari interaksi ke *game server* secara langsung. Komunikasi antar game-*server* terjadi melalui lapisan interaksi yang terdiri dari komponen input dan komponen output. Komponen input dirancang khusus untuk *engine* tertentu, yang kemudian akan berinteraksi langsung dengan data pemain yang berasal dari *game-engine*. Lalu, dilakukan *world-trace* berdasarkan kondisi *game* sehingga sistem dapat menentukan informasi yang diperlukan. Semua proses tersebut diformat dan diteruskan ke *analysis engine*. Sementara, komponen output bertanggung jawab untuk meneruskan *cheat-score* yang dikeluarkan untuk pemain ke *game-server* sehingga pemain tersebut dapat ditindaklanjuti.

Plugin dari sistem ini menggunakan konsep '*trace*': *Plugin* harus dapat mendeteksi dengan tepat apa yang sedang dilihat oleh pemain, pada saat kapan pun, dan objek apa yang ada di dunia *game* tersebut. Dalam *wall-hack-detecting proof-of-concept,* dibutuhkan dua jenis *trace filter*, yaitu *world filter* dan *entity filter* [1].

Untuk mengetahui pemain mana yang melakukan kecurangan, maka sistem harus mengetahui 'karakteristik apa sajakah yang dapat diamati sehingga memungkinkan suatu sistem untuk membedakan pemain yang

bermain dengan sah dan pemain yang curang?' Dari situlah kemudian muncul hasil empat metrik berikut yang menunjukkan perbedaan yang jelas di antara keduanya [1].

1. ***Frequency of illegal traces***: Suatu *illegal trace* didefinisikan sebagai *trace* atau vektor antara garis pandang pemain yang diamati ke musuh, namun *trace* tersebut melewati *opaque world material* sebelum mencapai model lawan. Pemain yang tidak melakukan kecurangan hanya dapat menemukan pemain di balik tembok secara kebetulan, sementara *wall-hacker* cenderung untuk melacak musuh dari balik dinding.
2. ***Distance to world material***: Bagi seorang *wall-hacker*, material di dunia *game* (seperti dinding) tidak akan menghalangi pandangan *cheater*. Sedangkan, pemain yang tidak melakukan kecurangan akan cenderung fokus pada titik terjauh dalam peta. Oleh karena itu, dihipotesiskan bahwa para *wall-hacker* akan menunjukkan perilaku aneh menatap dinding dalam waktu yang lama.
3. ***Distance to illegal traces***: Dihipotesiskan bahwa jarak ke *illegal trace* akan lebih kecil secara rata-rata untuk pemain *wall-hacker* daripada untuk pemain yang sah
4. ***Consecutivity of illegal traces***: Dihipotesiskan bahwa konsistensi *illegal trace* jauh lebih tinggi untuk para *wall-hacker* jika dibandingkan dengan pemain yang tidak melakukan kecurangan.

3.4. ANTI CHEAT ARTIFICIAL INTELLIGENCE

Sebagaimana dengan AI pada umumnya, kualitas *anti-cheat AI* ditentukan oleh banyaknya sampel dan data - semakin banyak sampel, semakin tinggi pula akurasi AI ini dalam mendeteksi kecurangan. Sistem ini menerapkan sistem *behavioural-monitoring approach* dengan cara mendeteksi perilaku pemain yang tidak wajar selama bermain dalam game.

Untuk mengklasifikasikan perilaku *cheating* dan memperkirakan akurasi deteksi AI, biasanya dibutuhkan para ahli yang meninjau secara acak kasus yang "mencurigakan" secara manual. Kemudian, mereka membuat keputusan - apakah terjadi kecurangan atau tidak? Menurut ahli statistik, teknik ini disebut dengan *acceptance sampling* [8]. Namun, terkadang masih ada kasus terjadinya *false positive* - suatu kondisi ketika sistem keliru menyalahkan pemain karena curang.

Contoh produk yang menggunakan sistem ini adalah GOSU.AI, sebuah AI untuk mendeteksi kecurangan dalam DOTA 2. GOSU.AI menggunakan teknik bernama *anomaly detection*: sebuah algoritma yang mempelajari sampel dari permainan yang normal, sehingga dapat mendeteksi perilaku yang mencurigakan apabila terjadi suatu deviasi. Selain itu, mereka juga membandingkan *skill* pemain dengan waktu total bermain, serta melihat pergerakan kursor *mouse* [9].

3.5. MEMORY-SCANNING

Memory-scanning melibatkan pemeriksaan isi memori yang digunakan oleh game secara real-time untuk mengetahui apabila terdapat *cheat-hook*.

3.6. AUTHORISATION-SERVERS

Dalam metode ini, pihak pengembang menyediakan suatu server akun yang menunjukkan pengguna mana yang terpercaya dengan cara melakukan identifikasi dan otentikasi. Pengguna yang terpercaya diizinkan untuk terhubung dengan server. Dengan demikian, pihak pengembang dapat memastikan bahwa pemain yang terhubung tidak masuk *blacklist* karena pernah melakukan tindakan kecurangan sebelumnya.

3.7. CONTENT-HASHING

Untuk mendeteksi perubahan pada file atau konten *game*, server *game* dapat meminta *hash* dari kumpulan file *game* tertentu, lalu membandingkan *hash* tersebut dengan *hash* yang seharusnya.

3.8. SCREENSHOTTING

Administrator dari pihak pengembang dapat mengamati dan meminta *screenshot* dari layar pemain kapanpun. Hasil dari *screenshot* tersebut akan dievaluasi oleh administrator apakah terjadi kecurangan dalam permainan tersebut.

3.9. API/DRIVER SCAN

Paket *anti-cheat Cheating-Death* berfungsi untuk memindai aktivitas di *graphic driver* sebelum meluncurkan *game* di *harness*, sehingga dapat memantau eksploitasi *driver* dan berbasis API.

3.10. GOOD GAME DESIGN

Tidak hanya melulu dalam berbentuk alat, desain *game* yang bagus, dari sisi kode maupun dari segi mekanisme *reward,* pun dapat mengatasi dan mengurangi kecurangan.

Dengan kode yang rapi, kemungkinan terjadinya *bug* dan *loophole* untuk dieksploitasi *cheater* pun dapat menurun. Selain itu, *cheater* cenderung untuk menempuh jalan pintas untuk menempuh *objective* yang harus dicapai. Jika diterapkan pemberian *reward* berdasarkan *milestone* yang ditempuh, maka pemain cenderung lebih berusaha untuk bermain *game* tanpa menggunakan *cheat* sehingga mendapatkan *reward* yang lebih banyak.

3.11. GOVERNMENT RULES ON CYBER SECURITY VIOLATION

Tak bisa dipungkiri, jika ada peraturan yang tegas untuk pelanggaran *cyber security*, maka pelaku akan lebih takut untuk melakukan hal-hal tersebut karena hukuman yang membuat jera pelaku.

Di Indonesia, undang-undang yang mengatur tentang *cyber security* adalah UU No. 11 Tahun 2008 dan PP No. 82 Tahun 2012 sebagai Dasar Keamanan Siber dan Pertahanan Siber Semesta [7]. Lebih jelasnya lagi, UU No. 11 Tahun 2008 ini menjelaskan tentang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Pemerintah No. 82 Tahun 2012 menjelaskan tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. Kemudian, terdapat Pasal 15 UU ITE yang mengatur bahwa Penyelenggara Sistem Elektronik harus menyelenggarakan sistem elektroniknya secara aman, andal, dan bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya [7]. Artinya seluruh Penyelenggara Sistem Elektronik, terlepas apakah sistem itu digunakan untuk kepentingan pemerintahan, komersial, atau pribadi harus menyelenggarakan sistemnya secara andal, aman dan bertanggung jawab. Dengan demikian, perbuatan curang dalam bentuk *cheating related by virtual assets* dapat diatasi.

3.12. SOCIALIZATION

Beberapa *cheater* kerap mengandalkan ketidakawasan pemain dalam kehidupan nyata maupun *virtual*, seperti penipuan berupa penjualan *virtual assets* yang palsu dan penipuan melalui *social engineering*. Oleh karena itu, pihak pengembang perlu mensosialisasikan peraturan dan peringatan bahwa para pemain harus berhati-hati dalam melakukan segala transaksi ataupun kegiatan yang dilakukan di luar *game* dan situs sah *game* tersebut.

4. KESIMPULAN

Online game masih sangat terbuka akan peluang untuk terjadinya berbagai macam kecurangan. Kecurangan dalam *online game* sebagian besar disebabkan oleh kegagalan keamanan dalam sistem. Selain empat aspek tradisional keamanan - kerahasiaan, integritas, ketersediaan, dan keaslian sistem, keadilan pun menjadi salah satu aspek yang vital, sehingga penegakan keadilan merupakan perspektif yang baik untuk memahami peran keamanan dalam mengembangkan dan mengoperasikan *online game*. Diperlukan pula pencegahan dari eksternal, seperti desain *game* yang bagus, dukungan dari pemerintah berupa peraturan untuk mencegah perbuatan pelanggaran *cyber security,* serta diadakannya sosialisasi ke masyarakat agar tidak mudah tertipu oleh *virtual asset cheater*. Kedepannya, masih banyak lagi cara yang dapat ditelusuri dan dikembangkan lebih lanjut untuk menekan tindakan pelanggaran dalam *game*. Dengan demikian, penulis yakin bahwa perilaku *cheating* dan *hacking* akan lebih cepat terdeteksi dan teratasi dengan baik, dan juga *cyber security* dalam *game online* akan menjadi lebih baik kualitasnya.

5. REFERENSI

[1] Laurens, Peter & Paige, Richard & Brooke, Phillip & Chivers, Howard. (2007). A Novel Approach to the Detection of Cheating in Multiplayer Online Games. Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS. 97-106. 10.1109/ICECCS.2007.11.

[2] Yan, Jeff & Randell, Brian. (2005). A systematic classification of cheating in online games. 1-9. 10.1145/1103599.1103606.

[3] Duh, Henry & Chen, Vivian. (2009). Cheating Behaviors in Online Gaming. 5621. 567-573. 10.1007/978-3-642-02774-1_61.

[4] Brooke, Phillip & Paige, Richard & Clark, John & Stepney, Susan. (2004). Playing the game: cheating, loopholes, and virtual identity. ACM SIGCAS Computers and Society. 34. 3. 10.1145/1052791.1052794.

[5] Yan, J., & Choi, H. (2002). Security issues in online games. *The Electronic Library, 20*, 125-133.

[6] S McCreary and K Claffy. (2000). Trends in Wide Area IPTraffic Patterns: A View from A mes Internet Exchange, in Proceedings of the ITC Specialist Seminar on IP Traffic Modeling, Measurement and Management, Monterey, CA, USA.

[7] Kementrian Komunikasi dan Informatika RI, 2016, Kebijakan Keamanan dan Pertahanan Siber, viewed April 2020, https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/

[8] GOSU.AI, 2018, GOSU.AI Against Dota 2 Cheaters, viewed April 2020, https://gosu.ai/blog/dota2/gosu-ai-against-dota-2-cheaters/

[9] GOSU.AI, 2019, We are sick and tired of cheaters in Dota 2! And we declare WAR on them, viewed April 2020, https://gosu.ai/blog/dota2/gosuai_vs_cheaters/

[10] Valve Software Inc., http://www.valvesoftware.com