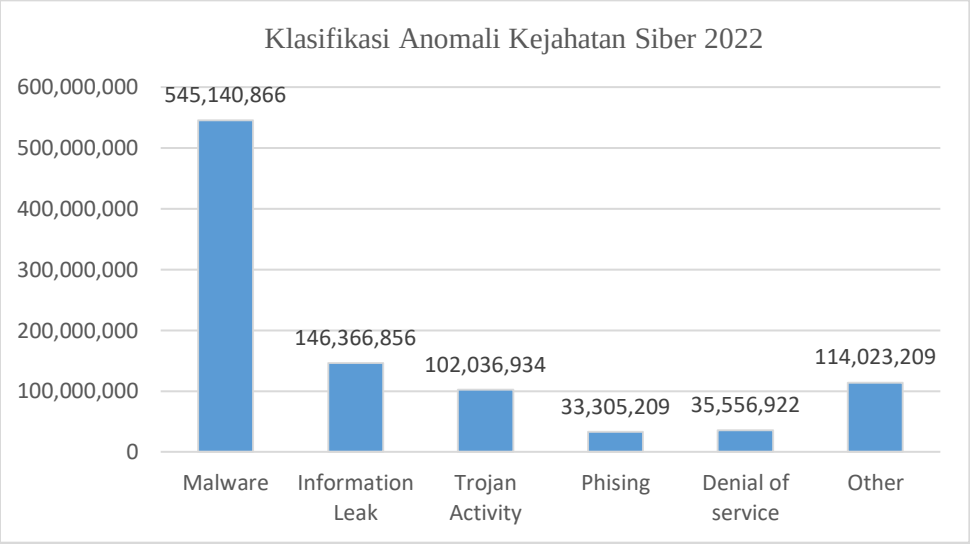
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi tidak hanya memindahkan aktivitas positif ke dalam komputer dan internet, tetapi juga kejahatan. Kejahatan dunia maya atau *cybercrime* sudah banyak terjadi diberbagai penjuru dunia, salah satunya Indonesia. Menurut catatan Badan Siber dan Sandi Negara (BSSN) sudah terjadi 976.429.996 anomali *traffic* atau usaha yang mencurigakan untuk menginfeksi keamanan siber di Indonesia pada tahun 2022. Dari jumlah tersebut, mayoritasnya adalah aktivitas serangan *malware*. Pelaksana tugas (Plt) Direktorat Keamanan Siber BSSN, Andi Yusuf dalam seminar nasional "*Today and Tomorrow's Cybersecurity Talent: Issue and challenges*" menyebutkan dari keseluruhan anomali *traffic*, yang paling banyak berupa aktivitas serangan *malware* sebanyak 55,83%, kemudian *information leak* 14,99%, dan aktivitas trojan 10,45%.



Gambar 1.1 Klasifikasi Anomali Kejahatan Siber 2022.

Sumber: BSSN (2022)

Berdasarkan data tersebut jenis *cybercrime* berupa *malware* merupakan tindak kejahatan siber yang paling sering terjadi di Indonesia, seperti aplikasi lacak paket dan undangan pernikahan *online* yang disisipi virus untuk mencuri data dan mengambil kendali perangkat korban, dikutip dari Andi Nugroho pada laman *Cyberthreat.id* 28 Januari 2023. Banyak korban yang terjerat dalam kasus ini dan

menimbulkan keresahan pada masyarakat. *Malware* (*Malicious Software*) adalah perangkat lunak berbahaya yang dibuat dengan maksud untuk menginfeksi sistem dan melakukan aktivitas yang merugikan pemiliknya. Dampak negatif yang ditimbulkan oleh *malware* dapat bervariasi, mulai dari menghambat kinerja sistem hingga menyebabkan kerusakan dan kehilangan data penting yang disimpan dalam sistem (Manoppo dkk., 2020). Selain itu terdapat banyak kejahatan siber lain yang tersebar di masyarakat, salah satunya *phising*. *Phising* adalah kejahatan yang bertujuan untuk menangkap informasi yang sangat sensitif seperti *username, password* dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya dan biasanya berkomunikasi secara elektronik. *Phising* biasanya langsung menyerang psikologis sehingga korban mempertimbangkan konten yang mereka baca atau dengar menjadi penting (Abroshan dkk., 2021).

Berbagai tindak kejahatan ini beroperasi pada jaringan internet yang telah digunakan oleh 210 juta penduduk Indonesia pada tahun 2022 menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), dimana tingkat penetrasi internet di kelompok usia 15-18 tahun merupakan yang terbesar hingga mencapai 99,16%. Menurut penelitian yang dilakukan Prabowo (2021), tingkat pengetahuan siswa SMP-SMA terkait *cybersecurity* masih sangat rendah karena tidak adanya materi pengajaran ataupun pelatihan mengenai hal tersebut. Dalam penelitian lain, terkait tantangan implementasi strategi keamanan siber Indonesia berdasarkan *Global Cyber security Index* disebutkan bahwa edukasi publik terhadap keamanan siber belum diterapkan secara sistemastis dimulai dari usia dini (Islami, 2017), hal ini membuat mereka rentan mengalami serangan kejahatan siber. Terdapat beberapa faktor penyebab lain terjadinya *cybercrime*, seperti akses internet yang tak terbatas, sistem kemanan jaringan yang lemah, dan kelalaian pengguna. Peningkatan pemahaman dan kesadaran terkait keamanan siber dipilih untuk menjadi solusi dari permasalahan ini karena dapat menjadi pertahanan utama tiap individu dalam menghadapi serangan siber (Jin dkk., 2018), terlebih lagi tindak kejahatan di dunia maya akan sulit diidentifikasi jika tidak memiliki pemahaman (Wash, 2020).

Penelitian ini akan menggunakan media *game* edukasi berbasis *mobile* yang pada penelitian Hadiprakoso dan Satria (2022) menunjukkan bahwa aplikasi gamifikasi dapat meningkatkan kesadaran keamanan siber siswa SMA di Jakarta.

Dengan genre *game* yang dipilih yaitu *Role Playing Game* (RPG) karena dapat meningkatkan motivasi siswa dalam belajar dan memahami materi pelajaran (Rasyid dkk., 2020), selain itu *game* RPG juga menunjukkan dampak positif terhadap hasil belajar siswa (Ciampa, 2018). *Role Playing Game* (RPG) merupakan salah satu jenis *game* pilihan karena memasukkan unsur- unsur penceritaan yang kompleks serta seni peran yang membuat pemain merasa seperti menjadi tokoh yang diperankan dalam *game* tersebut (Ginting dan Ramadhan, 2018), sehingga pemain akan mendapatkan pengalaman secara langsung terkena *cybercrime* melalui media simulasi. Metode simulasi dapat memberikan pengalaman belajar yang nyata seperti kondisi sesungguhnya dengan penyelesaian-penyelesaian yang ditawarkan berkaitan dengan masalah yang ada sehingga dapat meningkatkan pengetahuan siswa (Rahayu dkk., 2022).

Berdasarkan permasalahan yang telah dipaparkan peneliti bermaksud untuk melakukan rancang bangun *Role Playing Game* untuk membangun resistensi terhadap *cybercrime* yang dalam proses perancangannya menggunakan metode *Game Development Life Cycle.*

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dari penelitian ini adalah:

1. Bagaimana rancangan *game* edukasi bergenre *Role Playing Game* dengan metode *Game Development Life Cycle*?
2. Bagaimana implementasi *game* edukasi bergenre *Role Playing Game* dalam upaya membangun resistensi terhadap *cybercrime*?

1.3 Batasan Masalah Penelitian

Berdasarkan rumusan masalah tersebut diperlukan batasan masalah agar penelitian tidak menyimpang dari rencana, sehingga tujuan dari penelitian dapat dicapai. Berikut beberapa batasan dari penelitian ini, yaitu:

1. Perancangan *game* edukasi bergenre *Role Playing Game* berbasis android.
2. Implementasi rancangan *game* edukasi dalam upaya membangun resistensi terhadap *cybercrime*.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini berdasar pada masalah di atas adalah sebagai berikut:

1. Merancang *game* edukasi bergenre *Role Playing Game* berbasis android sebagai media pembelajaran dengan metode *Game Development Life Cycle*.
2. Mengetahui hasil implementasi *game* edukasi bergenre *Role Playing Game* dalam membangun resistensi terhadap *cybercrime*.

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat secara teoritis dan praktis. Adapun manfaat yang diperoleh dari penelitian ini yaitu:

1. Manfaat Teoritis

Secara teori penelitian ini bermanfaat sebagai pengembangan ilmu pengetahuan bagi mahasiswa dan peneliti selanjutnya, khususnya dalam perancangan *game* edukasi.

2. Manfaat Praktis

Pada penerapannya, hasil penelitian ini dapat bermanfaat bagi para siswa untuk membantu memperdalam pemahaman dan cara menangani *cybercrime* terutama *malware* dan *phising*.

1.6 Struktur Organisasi Skripsi

Struktur organisasi dalam skripsi ini dapat dijabarkan sebagai berikut:

1. Bab I Pendahuluan: membahas latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan struktur organisasi skripsi.
2. Bab II Kajian Pustaka: membahas mengenai konsep dan kajian pustaka yang menjadi dasar teori penelitian ini.
3. Bab III Metode Penelitian: membahas desain penelitian, populasi dan sampel, instrument penelitian, prosedur penelitian, serta analisis data.
4. Bab IV Hasil dan Pembahasan: berisi hasil rancangan *game* yang dibuat, pengolahan dan analisis data, serta pembahasan penelitian.
5. Bab V Simpulan, Implikasi, dan Rekomendasi: membahas mengenai kesimpulan yang didapatkan selama penelitian dan rekomendasi terhadap penelitian berikutnya.