BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Perkembangan teknologi informasi dan komunikasi telah mengubah masyarakat global, perkembangan ini membawa manfaat besar, namun juga membuka peluang bagi terjadinya tindak kejahatan siber yang semakin kompleks dan mendesak. Dengan populasi pengguna internet yang berkembang pesat, Indonesia juga tidak luput oleh ancaman kejahatan siber yang meningkat. Kejahatan siber adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet (Indra Safitri dalam (Maskun, 2022)). Perubahan pesat dalam ekosistem teknologi informasi dan komunikasi telah menciptakan peluang baru bagi para pelaku kejahatan siber untuk meningkatkan kompleksitas dan skala serangan mereka. Ancaman kejahatan siber yang merupakan bentuk ancaman perang era *modern* atau non-militer yang dapat memicu terjadinya disintegrasi bangsa melalui motif kepentingan individu atau kelompok tertentu (Ariyaningsih dkk., 2023).

Berdasarkan data yang dipublikasikan oleh Badan Siber dan Sandi Negara (BSSN), pada tahun 2023, tercatat adanya sebanyak 403.990.813 anomali trafik atau upaya mencurigakan untuk menyusup ke dalam lapisan keamanan siber di Indonesia. Angka yang signifikan ini menyoroti eskalasi ancaman terhadap keamanan siber di negeri ini yang masih sangat tinggi. Dalam laporan tersebut juga tertera sebaran indikasi insiden siber yang terjadi pada tahun 2023 dengan total sebanyak 625 kali, dimana indikasi yang paling banyak tercatat adalah *data breach* sebesar 85%, *distributed denial-of-service (DDOS)* 5%, *ransomware* 4%, *proaktif* 3% dan serangan lainnya sebesar 3%. Selain itu ada juga sebaran aduan siber yang terjadi selama tahun 2023 sebanyak 1417. Aduan siber yang masuk sepanjang tahun kemarin dan terbagi menjadi tiga belas

kategori dengan aduan yang paling banyak adalah *cybercrime* sebanyak 87%, *Web Defacement* 4%, *Vulnerability Indicator* 4%, *phising* dan *ransomware* masing-masing sebanyak 1%, serta serangan lainnya sebanyak 3%.

Berdasarkan kedua sebaran data tersebut, kasus *data breach* dan *cybercrime* masih sangat tinggi terjadi pada tahun 2023 yang lalu. *Data breach* merupakan insiden keamanan di mana data pengguna aplikasi telah diakses tanpa izin. Paling buruknya, data yang dicuri bisa diperjualbelikan seperti yang terjadi pada tahun 2022 lalu terjadi kasus *data breach* yang menimpa BPJS Ketenagakerjaan dengan total sebesar 18,5 juta data pengguna yang bocor dan dijual di sebuah forum gelap seharga 153 juta Rupiah. Kemudian kasus serupa terjadi pada Bank Syariah Indonesia (BSI) dengan total data yang tercuri sebanyak 1,5 TB yang didalamnya termasuk 15 juta data pengguna dan sandi untuk akses secara *internal* layanannya, selain itu juga termasuk didalamnya data pribadi para nasabah (CNN, 2023). Umumnya, *data breach* bisa terjadi melalui berbagai metode, seperti *phishing*, penyusupan *malware*, hingga penggunaan *software illegal* (Finaka dkk., 2022). Dampak terburuk bagi organisasi atau perusahaan yang mengalami kebocoran data adalah hilangnya kepercayaan publik, reputasi, tuntutan hukum, atau denda. Sementara bagi orang yang datanya dibocorkan adalah data tersebut digunakan sebagai bahan penipuan (Haurissa, 2022).

Selain *data breach*, tindak *cybercrime* juga masih sangat tinggi terjadi di kalangan masyarakat, salah satunya adalah *scamming* atau lebih biasa dikenal dengan penipuan *online*. Penipuan *online* merupakan salah satu keluhan yang umum dilaporkan oleh masyarakat terkait tindakan *cybercrime* seperti penipuan *online*, pencemaran nama baik, penyebaran data diri, peretasan, dll. (BSSN, 2023). *Scamming* atau penipuan *online* adalah praktik yang dilakukan secara digital dengan tujuan untuk mendapatkan informasi pribadi, keuangan, atau mengakses aset individu atau organisasi secara *ilegal*. Kejahatan *scamming* bisa menimpa siapa saja seperti yang terjadi pada salah satu mahasiswi Universitas Sebelas Maret yang mengalami kehilangan uang sebesar 7 juta Rupiah pada akun *mobile banking* yang ia miliki ketika hendak membayar uang kuliah (Dewi, 2019). Biasanya, penipuan *online* melibatkan manipulasi, tipu daya, atau

pemalsuan identitas untuk memanipulasi korban agar memberikan informasi sensitif atau melakukan tindakan tertentu yang menguntungkan pelaku penipuan (Juditha, 2015).

Peningkatan tindak kejahatan siber yang terjadi saat ini tidak dapat dilepaskan dari dampak teknologi dan luasnya akses internet. Pada tahun 2024, jumlah pengguna internet di Indonesia telah mencapai angka yang signifikan, mencapai 221,56 juta jiwa. Dari jumlah tersebut, *Gen-Z*, yang memiliki rentang usia 12-27 tahun, menonjol sebagai salah satu kelompok pengguna terbanyak, dengan persentase mencapai 87,02%. Informasi ini didasarkan pada hasil survei penetrasi pengguna internet yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) (Finaka dkk., 2024). Menurut penelitian yang dilakukan oleh Ryansyah dkk., (2023) secara umum pemahaman tentang keamanan siber di Indonesia bervariasi tergantung pada latar belakang pendidikan, tingkat kesadaran, dan eksposur terhadap materi keamanan siber. namun masih ada sebagian besar belum sepenuhnya menyadari berbagai jenis ancaman keamanan siber dan cara melindungi diri dari serangan tersebut. Kemudian dalam penelitian lain menyebutkan bahwa edukasi tentang keamanan siber belum dilakukan secara sistemastis sejak usia dini padahal pengguna internet di Indonesia cukup tinggi (Islami, 2017). Sunardi (2008) menjelaskan beberapa faktor yang menyebabkan *cybercrime* terjadi meliputi akses internet yang tidak terbatas, kelalaian pengguna komputer, kemudahan pelaksanaannya dengan risiko keamanan yang minim, serta tidak memerlukan peralatan yang canggih. Pemilihan pemahaman dan kesadaran terkait keamanan siber dijadikan sebagai strategi untuk mengatasi masalah ini, karena dapat berperan sebagai pertahanan utama bagi setiap individu dalam menghadapi serangan siber (Rohmah, 2022).

Game merupakan bentuk hiburan yang biasa digunakan untuk melepas penat, namun seiring berjalannya waktu *game* telah menjadi salah satu bentuk pendekatan yang inovatif dan efektif dalam konteks pendidikan, memperluas cakupan pembelajaran dengan cara yang menarik dan interaktif terutama untuk *game* bergenre *role-playing game* atau yang biasa dikenal sebagai *RPG*.

Pemilihan *game* bergenre *RPG* ini didasarkan kepada penelitian terdahulu yang dilakukan oleh Satria & Herumurti, (2021) bahwasannya *game* bertema *RPG* mempunyai aspek *mediocore* dalam efektivitas pemain dalam menerima materi pembelajaran.

RPG adalah jenis permainan di mana pemainnya akan mengambil peran sebagai karakter tertentu dalam suatu cerita atau dunia yang dibangun dalam permainan tersebut (Samuel Henry, 2010 dalam (Inayah, 2017)). Dengan menggunakan media pembelajaran *game* edukasi berbasis *RPG* mampu meningkatkan motivasi belajar siswa selama pembelajaran karena pemain dapat terlibat secara emosional dengan materi yang disampaikan dan memberikan pengalaman belajar yang unik sehingga memungkinkan penyesuaian dengan kecepatan gaya belajar seseorang, yang menghasilkan pembelajaran yang lebih efisien (Sholichah dkk., 2022). Selain itu, dalam penelitian yang dilakukan oleh Pramuditya dkk., (2017) penggunaan *game RPG* sebagai media pembelajaran memberikan dampak yang positif, karena dalam penggunaanya para pemain akan dilibatkan secara langsung dalam *game* sehingga menawarkan pembelajaran kontekstual dan imersif dimana pemain dapat belajar melalui skenario yang muncul dalam *game* yang meniru situasi nyata seperti kejahatan siber, sehingga membantu mereka untuk belajar membuat keputusan dan memecahkan masalah yang berkaitan dengan materi. Secara keseluruhan penggunaan media edukasi bebasis *game RPG* memberikan kontribusi positif yang signifikan terhadap pengalaman belajar, dengan meningkatkan motivasi dan keterlibatan peserta dalam proses pembelajaran sehingga menarik bagi audiens remaja yang membuatnya lebih baik dalam menarik perhatian dan minat daripada pendekatan pembelajaran secara konvensional (Saputra dkk., 2023).

Berdasarkan permasalahan yang telah dipaparkan maka peneliti bermaksud untuk melakukan pengembangan terhadap *game* bergenre *role playing game* sebagai media edukasi untuk membangun kesadaran terhadap tindak kejahatan siber yang dalam proses pengembangannya menggunakan metode *Game Development Life Cycle*.

1.2. Rumusan Masalah Penelitian

Berdasarkan latar belakang masalah yang telah dipaparkan sebelumnya, maka rumusan masalah dari penetian ini adalah sebagai berikut:

1.2.1. Bagaimana hasil pengembangan *game* bergenre *role playing game* menggunakan metode *Game Development Life Cycle*?

1.2.2. Bagaimana hasil analisis kualitas *game* bergenre *role playing game* untuk membangun kesadaran terhadap tindak kejahatan siber?

1.3. Batasan Masalah Penelitian

Kemudian berdasarkan rumusan masalah yang telah dipaparkan maka diperlukan batasan masalah untuk mencegah penelitian yang akan dilakukan melenceng dari rencana, sehingga mencapai tujuan penelitian. Di bawah ini terdapat beberapa parameter yang ditetapkan dalam penelitian ini, antara lain:

1.3.1. Pengembangan *game* edukasi dengan genre *Role Playing Game* berbasis *web*.

1.3.2. Penelitian ini akan menganalisis kualitas *game* dari aspek kemudahan pengguna.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini, yang didasarkan pada masalah yang telah disebutkan sebelumnya, adalah:

1.4.1. Untuk mengetahui hasil pengembangan permainan berjenis *Role Playing Game* yang berbasis desktop menggunakan metode *Game Development Life Cycle*.

1.4.2. Untuk mengetahui hasil analisis kualitas permainan berjenis *Role Playing Game* dalam membangun kesadaran terhadap tindak kejahatan siber.

1.5. Manfaat Penelitian

Melalui penelitian ini, diharapkan dapat memberikan manfaat teoritis dan manfaat praktis yang berguna antara lain sebagai berikut:

1.5.1. Manfaat Teoretis

Adapun manfaat teoritis dalam penelitian ini salah satunya adalah kontribusi yang dapat diberikan oleh penelitian ini pada pengembangan

ilmu pengetahuan, terutama dalam hal pengembangan media pembelajaran berbasis *game*. Dengan memperdalam pemahaman tentang bagaimana *game* dapat menjadi alat pembelajaran yang efektif, penelitian ini diharapkan dapat memberikan wawasan yang berharga bagi ilmu pengetahuan yang terkait. Selain itu, dengan menganalisis aspek-aspek teoritis yang mendasari penggunaan *game* sebagai media pembelajaran, penelitian ini dapat membuka jalan bagi pengembangan pendekatan yang lebih terarah dan efisien dalam proses pembelajaran.

1.5.2. Manfaat Praktis

1.5.2.1. Bagi Penulis

Diharapkan bahwa penelitian ini akan menjadi wadah bagi peneliti untuk mengembangkan diri dalam menerapkan pengetahuan, keterampilan, dan kemampuan yang telah diperoleh selama proses perkuliahan, serta diharapkan dapat menghasilkan manfaat yang bermanfaat bagi berbagai pihak yang terlibat.

1.5.2.2. Bagi Instansi

Sebagai kontribusi pada pengetahuan akademis melalui penambahan literatur dan pemahaman yang lebih mendalam dalam bidang pengembangan game edukatif dan kesadaran terhadap kejahatan siber, yang akan memperkaya basis pengetahuan kampus.

1.5.2.3. Bagi Peneliti lain

Penelitian ini diharapkan dapat menambah wawasan peneliti lain dengan memperluas pemahaman mereka tentang pengembangan *game* edukatif dan kesadaran terhadap kejahatan siber. Temuan dari penelitian ini dapat dijadikan sebagai panduan praktis dalam merancang dan mengimplementasikan solusi yang efektif dalam konteks pendidikan atau keamanan siber. Selain itu, hasil penelitian ini juga dapat menjadi sumber inspirasi bagi peneliti lain dalam mengeksplorasi topik terkait atau mengembangkan penelitian lanjutan di bidang ini.

1.6. Struktur Organisasi Skripsi

Struktur organisasi skirpsi yang digunakan pada penulisan skripsi yang berjudul "Pengembangan game bergenre role playing game untuk membangun kesadaran terhadap tindak kejahatan siber" ini merujuk pada panduan karya tulis ilmiah Universitas Pendidikan Indonesia tahun 2021, tersusun dari beberapa bab yang berurutan, yaitu:

1.6.1. BAB I Pendahuluan

Pada bab ini menjelaskan tentang latar belakang penelitian, rumusan masalah, Batasan masalah, tujuan dan manfaat penelitian yang dilakukan. Selain itu pada bab ini juga menyajikan struktur organisasi dari skripsi yang disusun.

1.6.2. BAB II Kajian Pustaka

Pada bab ini mengulas tentang teori-teori yang relevan dengan topik penelitian yang dilakukan seperti game, keamanan siber, kejahatan siber dan penelitian terdahulu.

1.6.3. BAB III Metode Penelitian

Pada bab ini menguraikan tentang jenis penelitian yang dilakukan, desain penelitian, tempat, populasi dan sampel penelitian, instrumen penelitian, Teknik pengumpulan data dan Teknik analisis data.

1.6.4. BAB IV Hasil dan Pembahasan

Pada bab ini mengulas tentang temuan dari pengembangan dan data-data hasil penelitian yang telah di interpretasi serta pembahasan temuan dari penelitian yang dilakukan.

1.6.5. BAB V Simpulan, Implikasi dan Rekomendasi

Pada bab ini menyimpulkan hasil dan temuan dari penelitian, memberikan implikasi serta memberikan saran dan rekomendasi kepada peneltian selanjutnya.