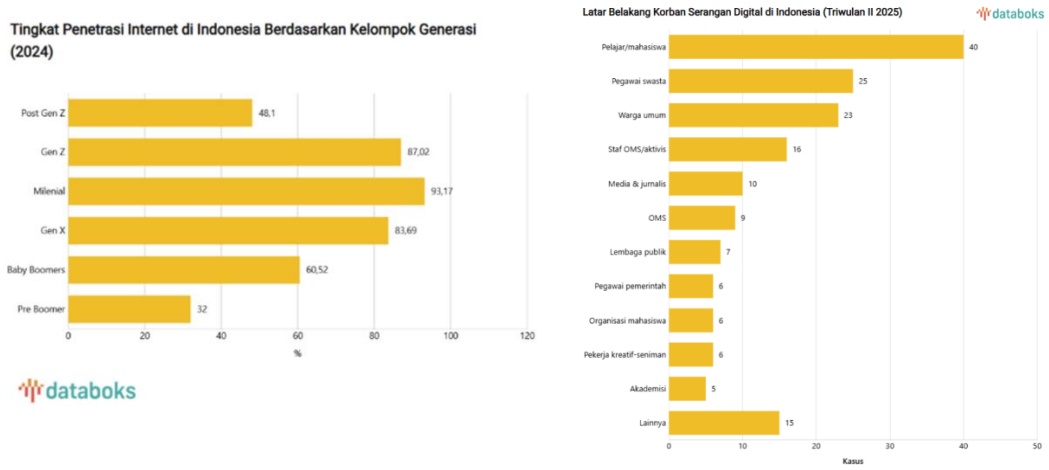
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Survei dari Asosiasi Penyelenggara Jasa Internet Indonesia menunjukkan bahwa jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 jiwa, dengan tingkat penetrasi sebesar 79,5% dari total populasi. Generasi milenial dan Generasi Z mendominasi kelompok pengguna ini, dengan angka penetrasi internet masing-masing mencapai 93,17% dan 87,02%. Namun, di balik tingginya angka penggunaan internet, laporan dari *Southeast Asia Freedom of Expression Network* menunjukkan bahwa pada kuartal II tahun 2025, pelajar dan mahasiswa justru menjadi korban terbanyak serangan siber (Gambar 1.1). Hal ini menunjukkan bahwa meskipun Generasi Z akrab dengan teknologi, mereka belum sepenuhnya memahami cara melindungi diri dari serangan siber.



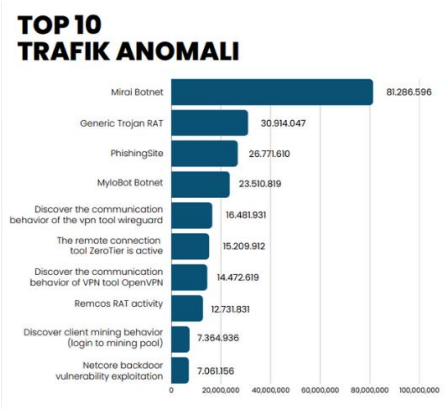
(a) (b)

Gambar 1. 1 (a) Grafik distribusi pengguna internet menurut kelompok generasi pada tahun 2024 (*Sumber:* Annur, 2024);
(b) Distribusi korban serangan digital berdasarkan latar belakang pada tahun 2025 (*Sumber:* Ridwan, 2025)

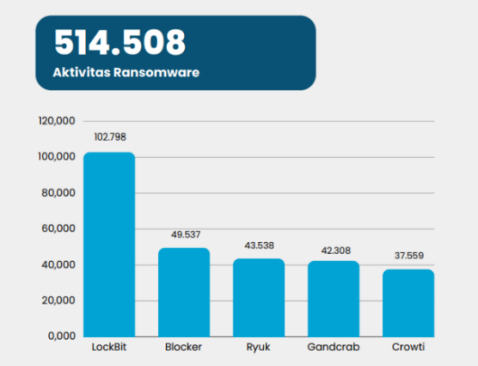
Badan Siber dan Sandi Negara mencatat bahwa total trafik anomali di Indonesia pada tahun 2024 mencapai 330.527.636 anomali. Jenis serangan yang paling sering terdeteksi adalah *Mirai Botnet*, dengan jumlah 81.286.596 trafik. Di urutan kedua

adalah *Generic Trojan RAT*, dengan 30.914.047 trafik anomali, yang mencakup aktivitas *backdoor* dan komunikasi dengan server *command and control* berbahaya, serta berpotensi digunakan sebagai sarana awal dalam penyebaran *ransomware*. Salah satu ancaman siber paling berbahaya saat ini adalah *ransomware*, yaitu jenis *malware* yang mengenkripsi data korban dan meminta tebusan agar akses terhadap data dapat dipulihkan. Berdasarkan hasil pemantauan ruang siber, tercatat sebanyak 514.508 aktivitas *ransomware* di Indonesia sepanjang tahun 2024. Dari jumlah tersebut, lima varian *ransomware* yang paling sering terdeteksi adalah *LockBit, Blocker, Ryuk, GandCrab,* dan *Crowti* (Gambar 1.2).

(a)



(b)

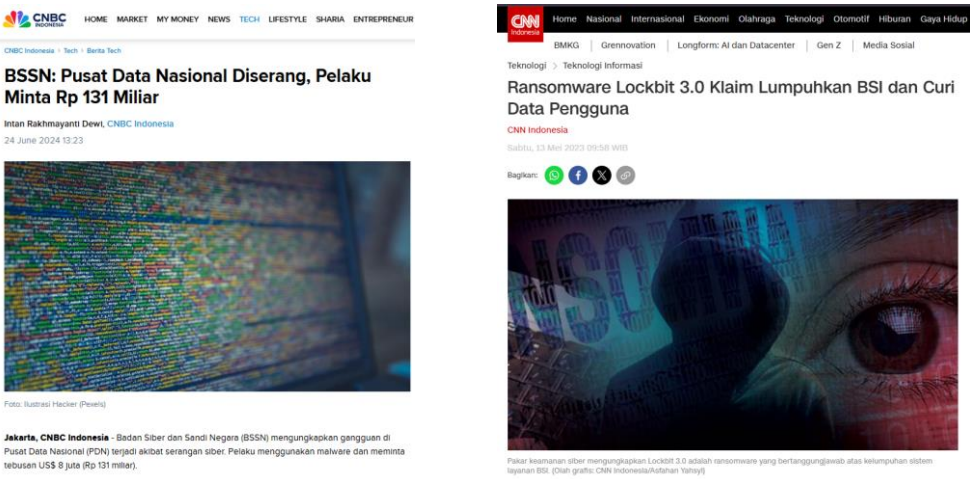


(c)

Gambar 1. 2 (a) Trafik Anomali Serangan Siber Indonesia; (b) Top 10 Trafik Anomali; (c) Aktivitas *Ransomware* di Indonesia Tahun 2024
(*Sumber:* Badan Siber dan Sandi Negara, 2024)

Ancaman *ransomware* semakin menjadi sorotan publik setelah insiden besar yang menimpa Pusat Data Nasional Indonesia pada 2024, di mana layanan imigrasi

dan 210 instansi pemerintahan lumpuh akibat serangan *LockBit 3.0 Brain Cipher* yang meminta tebusan senilai 131 miliar rupiah. Setahun sebelumnya, serangan *ransomware LockBit 3.0* juga melumpuhkan layanan Bank Syariah Indonesia, menyebabkan gangguan total pada ATM dan *mobile banking* selama beberapa hari. Serangan ini tak hanya berdampak pada operasional, tetapi juga mengakibatkan kebocoran 1,5 TB data berisi 15 juta informasi sensitif pengguna (Gambar 1.3). Kejadian ini menegaskan bahwa ketahanan terhadap serangan siber khususnya *ransomware* adalah kebutuhan strategis yang harus dimiliki oleh suatu institusi. Berdasarkan temuan (Kävrestad & Nohlberg, 2021), sebagian besar insiden keamanan siber terjadi akibat rendahnya pemahaman dan kesadaran pengguna terhadap ancaman siber. Hal ini menunjukkan bahwa keamanan siber bukan sekadar persoalan teknis, melainkan juga sangat bergantung pada kesadaran individu dan kemampuan mereka dalam mengambil keputusan yang bijak untuk mencegah ancaman siber (Zhang-Kennedy & Chiasson, 2021). Oleh karena itu, dibutuhkan sumber daya manusia yang memiliki keterampilan keamanan siber *ransomware*. Pelajar dan mahasiswa dari generasi Z memiliki peran strategis sebagai generasi yang tumbuh di tengah kemajuan teknologi dan berpotensi menjadi garda terdepan dalam membangun budaya sadar keamanan siber. Dengan pembekalan yang tepat, mereka tidak hanya mampu melindungi diri sendiri, tetapi juga turut memperkuat ketahanan siber nasional. Berdasarkan hal tersebut, dapat disimpulkan bahwa terdapat urgensi untuk meningkatkan keterampilan keamanan siber, khususnya *ransomware*, dari sudut pandang pengguna, khususnya pelajar dan mahasiswa dari Generasi Z.



Gambar 1. 3 (a) Berita insiden serangan *ransomware* terhadap Pusat Data Nasional Indonesia (*Sumber:* Dewi, 2024);
(b) Berita insiden serangan *ransomware* terhadap Bank Syariah Indonesia (*Sumber:* CNN Indonesia, 2023)

Untuk meningkatkan pemahaman masyarakat terhadap keamanan siber, telah dilakukan berbagai upaya, seperti pelatihan perlindungan data pribadi dan keamanan siber oleh (Maulindar & Hartanti, 2023), serta pengembangan media edukasi berbasis teknologi berupa video animasi bertema *cyber law* (Anugrah & Mahaputra, 2024). Namun, pendekatan-pendekatan tersebut cenderung bersifat teoritis dan belum secara optimal mengadopsi strategi praktis yang lebih efektif dalam membentuk keterampilan keamanan siber. Di sisi lain, pendekatan praktis terbukti lebih efektif dibandingkan metode teoritis dalam meningkatkan keterampilan keamanan siber (Sodikin & Hikmawan, 2023). Kondisi ini menunjukkan adanya kebutuhan untuk menjembatani kesenjangan antara teori dan praktik dalam pendidikan keamanan siber. Oleh karena itu, dibutuhkan inovasi media pembelajaran yang tidak hanya informatif, tetapi juga aplikatif dan mampu membangun kesadaran serta keterampilan keamanan siber secara nyata. Berdasarkan *Systematic Literature Review* yang dilakukan oleh Bakhsh dkk. (2022), *game* dinilai sebagai media pembelajaran yang dapat meningkatkan kemampuan pengambilan keputusan dan memungkinkan terjadinya transfer pengetahuan ke dalam situasi nyata melalui pendekatan pembelajaran berbasis pengalaman. Selain itu, *game* juga sangat sesuai dengan pendidikan tinggi karena

sejalan dengan minat generasi *digital native*. *Game* mampu melibatkan mahasiswa secara aktif, meningkatkan motivasi, serta mendukung hasil belajar yang lebih baik melalui lingkungan yang imersif dan interaktif. Temuan serupa dikemukakan oleh Choi-Lundberg dkk. (2023) melalui *Systematic Literature Review* yang ia lakukan bahwa *game* merupakan media pembelajaran yang efektif dalam pendidikan tinggi karena mampu memperkuat pemahaman kontekstual dan penerapan pengetahuan secara langsung. Sesuai teori Piaget, Generasi Z saat ini berada pada tahap operasional formal, di mana kemampuan berpikir abstrak, pemecahan masalah, dan pola pikir sistematis sudah berkembang (Iannace dkk., 2020). Dengan mekanisme interaktif, *game* dapat membantu mereka memahami ancaman siber dengan cara yang lebih menarik dan mendalam. Selain itu, *game* digital juga selaras dengan minat serta tren (Saglam dkk., 2023). Salah satu genre yang diminati oleh Generasi Z adalah *Visual Novel Interactive Game* (VNIG), yang berkembang sebagai media edukasi inovatif karena mampu menyampaikan materi secara kontekstual, aplikatif, dan imersif. Dengan pendekatan berbasis narasi interaktif dan alur bercabang, genre ini terbukti efektif dalam meningkatkan pemahaman konsep serta keterlibatan aktif pengguna dalam proses pembelajaran (Gkioulos & Chowdhury, 2021; Malegiannaki dkk., 2020; Zhang-Kennedy & Chiasson, 2021; Zhang, 2022).

Melihat potensi tersebut, pengembangan media pembelajaran berbasis *game* untuk edukasi serangan siber khususnya *ransomware*, menjadi sangat relevan dan strategis. Namun demikian, pengembangan sebuah media pembelajaran tidak dapat hanya berhenti pada aspek desain dan konten *game* semata, melainkan juga memerlukan perancangan evaluasi yang sistematis, termasuk penentuan indikator-indikator capaian yang mencerminkan hasil belajar setelah penggunaan media tersebut. Evaluasi ini penting untuk memastikan bahwa media tidak hanya menarik, tetapi juga efektif dalam mendukung tercapainya tujuan pembelajaran, sekaligus mendorong penguasaan keterampilan praktis yang dibutuhkan di dunia nyata. Oleh karena itu, penetapan indikator yang tepat menjadi krusial dalam mengukur keberhasilan media pembelajaran secara menyeluruh (Triyono, 2015; Hidayah & Mulyani, 2024). Indikator tersebut dapat diintegrasikan ke dalam sistem evaluasi adaptif yang memungkinkan terjadinya proses *adaptive learning*, dimana materi

dan tantangan dalam *game* disesuaikan dengan capaian dan kebutuhan belajar masing-masing pengguna, sehingga penguatan konsep dan keterampilan keamanan siber dapat dilakukan secara bertahap dan berorientasi pada perkembangan individu (Imhof dkk., 2020). *Literature review* yang dilakukan oleh Vasylyk dkk. (2024) membuktikan bahwa *adaptive learning* di pendidikan tinggi efektif dalam mencegah *learning loss* dan mengurangi kesenjangan pengetahuan. Pendekatan ini juga terbukti mampu meningkatkan penguasaan materi hingga 14–18%, sehingga dinilai sebagai strategi yang tepat untuk mengoptimalkan proses pendidikan di jenjang pendidikan tinggi (Pavlov dkk., 2024; Levin & Isakova, 2024). Namun, penerapan pendekatan ini dalam pengembangan media edukatif, khususnya yang berfokus pada keamanan siber, masih menemui berbagai tantangan. Kompleksitas materi serta rendahnya relevansi dengan konteks kehidupan nyata kerap membuat *game* edukatif menjadi kurang efektif, tidak berkelanjutan (*unsustainable*), dan gagal menciptakan pengalaman belajar yang mendalam maupun kondisi *flow* pada pemain (Jayakrishnan dkk., 2020; Maqsood & Chiasson, 2021). Selain itu, sebagian besar penelitian lebih berfokus pada edukasi keamanan siber secara umum, sementara pengembangan media pembelajaran yang secara khusus membahas topik *ransomware* masih sangat terbatas.

Berdasarkan permasalahan dan gap yang telah diidentifikasi, penelitian ini bertujuan untuk mengembangkan sebuah instrumen kuis adaptif untuk keterampilan keamanan siber *ransomware*, yang disusun berdasarkan indikator capaian tertentu. Namun, karena keamanan siber belum menjadi bagian dari kurikulum pendidikan nasional, indikator capaian dalam pengembangan media ini mengacu pada Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 11 Tahun 2020 tentang Kompetensi Keamanan Siber, Kerangka Kerja Indeks Literasi Digital 2021, serta hasil penelitian terdahulu dari Kim dkk. (2019) dan Tsani (2024). Instrumen kuis adaptif tersebut akan melalui analisis kuantitatif terstandarisasi lalu diintegrasikan ke dalam pengembangan *game* edukatif *Visual Novel Interactive Game* (VNIG) berjudul "Your Zero Hour". *Game* ini dirancang sebagai media pembelajaran komprehensif berbasis *adaptive learning* untuk meningkatkan

keterampilan keamanan siber *ransomware*, khususnya bagi kalangan pelajar dan mahasiswa dari Generasi Z.

1.2 Rumusan Masalah

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

1. Bagaimana hasil pengujian instrumen kuis adaptif untuk keterampilan keamanan siber *ransomware*?
2. Bagaimana hasil rancang bangun Your Zero Hour, *Visual Novel Interactive Game* berbasis *adaptive learning* sebagai media pembelajaran keamanan siber *ransomware*?
3. Bagaimana hasil pengujian kelayakan Your Zero Hour, *Visual Novel Interactive Game* berbasis *adaptive learning* sebagai media pembelajaran keamanan siber *ransomware*

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan penelitian ini adalah sebagai berikut:

1. Menguji instrumen kuis adaptif untuk keterampilan keamanan siber *ransomware*
2. Merancang dan mengembangkan Your Zero Hour, *Visual Novel Interactive Game* berbasis *adaptive learning* sebagai media pembelajaran keamanan siber *ransomware*
3. Menguji kelayakan Your Zero Hour, *Visual Novel Interactive Game* berbasis *adaptive learning* sebagai media pembelajaran keamanan siber *ransomware*

1.4 Manfaat Penelitian

Hasil penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Manfaat Teoretis

Penelitian ini dapat menjadi referensi dalam pengembangan media edukasi yang mengintegrasikan *adaptive learning* dalam *Visual Novel Interactive Game*, khususnya untuk pembelajaran keamanan siber.

2. Manfaat Praktis

Penelitian ini menghasilkan instrumen kuis adaptif untuk mengukur tingkat pemahaman pengguna terkait keamanan siber *ransomware*, serta *Visual Novel*

Interactive Game berbasis *adaptive learning* yang dirancang untuk meningkatkan pemahaman tersebut. Instrumen dan media pembelajaran ini dapat dimanfaatkan oleh pendidik sebagai sarana evaluasi sekaligus penyampaian materi secara interaktif, dan oleh pengembang teknologi pendidikan sebagai acuan dalam merancang atau mengintegrasikan fitur pembelajaran adaptif pada media serupa. Selain itu, VNIG juga dapat digunakan oleh pengguna internet secara mandiri untuk meningkatkan kesadaran dan pemahaman mengenai keamanan siber *ransomware*.

1.5 Ruang Lingkup Penelitian

Agar penelitian berjalan sesuai rencana dan mencapai tujuan yang diharapkan, ruang lingkup penelitian ditetapkan sebagai berikut:

1. Penelitian difokuskan pada pengembangan *Visual Novel Interactive Game* yang dirancang untuk perangkat komputer *desktop* berbasis sistem operasi Windows yang tidak menggunakan basis data eksternal dan tidak memerlukan koneksi internet untuk dijalankan. Ruang lingkup penelitian tidak mencakup pengembangan untuk platform *mobile* seperti Android dan iOS.
2. Tahapan pengujian pada penelitian ini terbatas pada pengujian kelayakan yang dilakukan melalui *Alpha testing* dan *Beta testing*. Penelitian ini belum mencakup tahapan uji coba terbatas, pengujian penerimaan (*user acceptance testing*), maupun uji efektivitas terhadap capaian pembelajaran.