# PROPOSAL PROYEK DESAIN INOVASI SOFTWARE DEVELOPMENT

## Gamifikasi sebagai Media Edukasi untuk Meningkatkan Kesadaran Masyarakat terhadap Ancaman Serangan DDoS


**Kelompok : 41**

**Anggota Kelompok:**

**1. Mukhammad Dito Okviansyah Ramadhan Putra – 255150200111013**

**2. Azka Syahrabbani – 255150200111054**

**3. Muhammad Fatahillah Al Fadli - 255150207111008**

**4. Naira Ayudhya Binastana – 255150200111062**

**5. Arin Alexia - 25515020711106**

**DEPARTEMEN TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS BRAWIJAYA**


**2025**

# DAFTAR ISI

# ABSTRAK

Ketergantungan masyarakat pada teknologi digital diiringi dengan meningkatnya ancaman siber, khususnya serangan Distributed Denial of Service (DDoS) yang dapat melumpuhkan layanan *online* dan menimbulkan kerugian serius. Meskipun ancaman ini merajalela, kesadaran dan literasi keamanan siber masyarakat Indonesia masih tergolong rendah. Pendekatan edukasi konvensional sering dianggap kurang menarik. Oleh karena itu, penelitian ini mengusulkan gamifikasi—penerapan elemen permainan dalam konteks non-permainan—sebagai solusi inovatif untuk meningkatkan motivasi, partisipasi, dan efektivitas pembelajaran keamanan siber.

Penelitian ini bertujuan untuk (1) Menerapkan konsep gamifikasi dalam merancang media edukasi interaktif tentang serangan DDoS, dan (2) Mengevaluasi efektivitas media tersebut dalam meningkatkan pemahaman dan kewaspadaan masyarakat terhadap ancaman DDoS.

Metode yang digunakan dalam perancangan adalah Prototyping yang bersifat iteratif, melibatkan tahapan Analisis Kebutuhan, Perancangan Konsep (meliputi sistem poin, *leaderboard*, dan *reward*), Pengembangan Prototipe menggunakan *software* seperti Figma dan Unity/HTML5, serta Pengujian dan Evaluasi terbatas. Efektivitas media akan diukur melalui perbandingan hasil pre-test dan post-test untuk menilai peningkatan pengetahuan, serta analisis metrik *engagement* (tingkat penyelesaian modul dan durasi sesi) dan kuesioner pengalaman pengguna.

Prototipe aplikasi/game edukatif yang dihasilkan diprediksi akan menunjukkan hasil positif, ditandai dengan kenaikan skor post-test sebesar 20-30% dibandingkan pre-test pada responden. Selain itu, penggunaan elemen gamifikasi diharapkan dapat menghasilkan *completion rate* yang tinggi (target lebih dari 50% ) dan mendorong adopsi perilaku pencegahan sederhana oleh pengguna. Hasil ini diharapkan memberikan kontribusi praktis dalam menyediakan alat sosialisasi yang menarik dan memperkuat literatur mengenai efektivitas gamifikasi dalam literasi keamanan digital.

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Aktivitas masyarakat kini semakin bergantung pada internet, baik dalam bidang pendidikan, ekonomi, maupun layanan publik. Namun, di balik kemudahan tersebut, muncul pula berbagai ancaman keamanan siber yang dapat mengganggu stabilitas sistem digital. Salah satu ancaman yang cukup berbahaya dan sering terjadi adalah serangan Distributed Denial of Service (DDoS), yaitu upaya untuk melumpuhkan suatu layanan atau server dengan membanjirinya menggunakan lalu lintas data dari banyak sumber secara bersamaan.

Serangan DDoS dapat menimbulkan dampak serius, seperti gangguan layanan daring, hilangnya data penting, dan kerugian ekonomi bagi individu maupun organisasi. Meskipun ancaman ini semakin sering terjadi, tingkat kesadaran masyarakat terhadap bahaya DDoS masih tergolong rendah. Banyak pengguna internet belum memahami bagaimana serangan ini bekerja, apa dampaknya, serta bagaimana cara mencegahnya. Kurangnya literasi digital dan keamanan siber menjadi salah satu penyebab utama rendahnya kesiapan masyarakat menghadapi ancaman semacam ini.

Upaya edukasi terkait keamanan siber sebenarnya telah dilakukan melalui berbagai media seperti seminar, artikel, atau pelatihan daring. Namun, pendekatan tersebut sering dianggap kurang menarik, terutama bagi generasi muda yang lebih menyukai metode pembelajaran interaktif. Untuk itu, dibutuhkan cara yang lebih inovatif dalam menyampaikan materi edukasi, salah satunya melalui gamifikasi.

Gamifikasi adalah penerapan elemen-elemen permainan dalam konteks non-permainan, dengan tujuan meningkatkan motivasi, partisipasi, dan efektivitas pembelajaran. Melalui gamifikasi, proses edukasi dapat menjadi lebih menarik dan mudah dipahami, sehingga pesan yang ingin disampaikan dapat diterima dengan lebih baik oleh masyarakat.

Penelitian atau pengembangan ini sejalan dengan Tujuan Pembangunan Berkelanjutan (Sustainable Development Goals / SDGs) poin 4, yaitu Pendidikan Berkualitas, yang menekankan pentingnya memastikan pendidikan yang inklusif, adil, dan berkualitas serta mendukung kesempatan belajar sepanjang hayat bagi semua orang. Penerapan gamifikasi sebagai media edukasi tentang ancaman DDoS merupakan bentuk inovasi dalam pendidikan yang mendorong peningkatan literasi digital dan kesadaran keamanan siber. Dengan meningkatnya pengetahuan masyarakat mengenai ancaman digital, mereka dapat menggunakan teknologi secara lebih aman, bijak, dan bertanggung jawab.

Dengan demikian, pengembangan gamifikasi sebagai media edukasi tidak hanya berkontribusi dalam peningkatan kesadaran masyarakat terhadap serangan DDoS, tetapi juga mendukung tercapainya SDG 4 dengan menyediakan metode pembelajaran yang kreatif, partisipatif, dan relevan dengan tantangan dunia digital saat ini.

## 1.2 Rumusan Masalah

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

1. Bagaimana konsep gamifikasi dapat diterapkan sebagai media edukasi untuk meningkatkan kesadaran masyarakat terhadap ancaman serangan DDoS?
2. Bagaimana merancang dan mengembangkan media edukasi berbasis gamifikasi yang efektif untuk menyampaikan materi tentang serangan DDoS?
3. Bagaimana mekanisme gamifikasi diterapkan dalam proses edukasi agar masyarakat dapat lebih memahami ancaman serangan DDoS?

## 1.3 Tujuan

Tujuan dari penelitian ini adalah:

1. Menerapkan konsep gamifikasi sebagai media edukasi untuk meningkatkan kesadaran masyarakat terhadap ancaman serangan DDoS.
2. Merancang dan mengembangkan media pembelajaran interaktif berbasis gamifikasi tentang serangan DDoS.
3. Mengevaluasi efektivitas media gamifikasi dalam meningkatkan pemahaman dan kewaspadaan masyarakat terhadap ancaman DDoS.

## 1.4 Manfaat

Adapun manfaat yang diharapkan dari penelitian atau pengembangan ini adalah:

### a. Manfaat Teoritis

1. Memberikan kontribusi terhadap pengembangan literatur mengenai penerapan gamifikasi dalam bidang edukasi, khususnya pada topik keamanan siber.
2. Menjadi dasar bagi penelitian selanjutnya yang berfokus pada pemanfaatan teknologi interaktif dalam pembelajaran keamanan digital.

### b. Manfaat Praktis

1. Menyediakan media pembelajaran yang menarik dan interaktif bagi masyarakat untuk memahami ancaman DDoS.
2. Meningkatkan kesadaran dan kesiapan masyarakat dalam menghadapi potensi serangan siber.
3. Dapat digunakan oleh lembaga pendidikan, organisasi, maupun instansi pemerintah sebagai alat sosialisasi dan edukasi keamanan siber.

# BAB II
# TINJAUAN PUSTAKA

## 2.1 Pengertian Gamifikasi

Gamifikasi adalah sebuah konsep dimana aspek permainan dibawa atau diterapkan ke dalam konsep non permainan, dengan tujuan untuk meningkatkan semangat dan motivasi peserta atau siswa dalam mempelajari sesuatu. Secara umum gamifikasi merupakan praktik menerapkan konsep permainan seperti kompetisi, poin, hadiah, dan tantangan untuk diterapkan ke dalam platform yang bukan permainan seperti web pembelajaran dll. Tujuannya adalah untuk meningkatkan motivasi, keterlibatan, dan partisipasi dengan cara yang menyenangkan. Dengan gamifikasi, aktivitas yang mungkin terasa monoton atau kurang menarik dapat menjadi lebih menarik dan lebih diingat.

Menurut Luthfi (2023), Manfaat dari Gamifikasi dalam proses pembelajaran adalah antara lain:

1. Membantu meningkatkan motivasi peserta/siswa, karena dalam Gamifikasi, terdapat konsep dari permainan seperti penghargaan (berupa poin, reward, badges), tantangan

(challenge) dan misi (mission). Elemen-element tersebut dapat meningkatkan motivasi peserta/siswa untuk memperoleh poin tertinggi,akibatnya peserta/siswa mendapatkan manfaat ilmu

2. Pengukuran nilai dan progress yang jelas, dengan adanya konsep seperti penghargaan dan papan skor maka kita bisa mengukur seberapa paham siswa dengan terukur dan jelas

### 2.2 Pengertian DDoS

DDoS atau Distributed Denial of Service (Penolakan Layanan Terdistribusi) merupakan salah satu serangan siber yang umum terjadi di dunia maya. Serangan DDoS bertujuan untuk mengganggu situs web dan server agar pengguna sah tidak bisa mengaksesnya.

Dilansir dari Microsoft Security selama serangan DDoS, seri data bot, atau botnet, membanjiri situs web atau layanan dengan permintaan http dan lalu lintas. Pada dasarnya, beberapa komputer menyerbu satu komputer selama serangan, sehingga mengusir pengguna yang sah. Akibatnya, layanan dapat terganggu selama jangka waktu tertentu. Peretas mungkin juga dapat menyusup ke database selama serangan dan mengakses informasi sensitif. Serangan DDoS dapat mengeksploitasi kerentanan keamanan dan menargetkan titik akhir apa pun yang dapat dijangkau, secara publik, melalui internet. Serangan DDoS dapat berlangsung berjam-jam, atau bahkan hari. Serangan cyber ini juga dapat menyebabkan beberapa gangguan selama serangan tunggal. Perangkat pribadi dan perangkat bisnis rentan terhadap serangan tersebut.

### 2.3 Kesadaran Masyarakat Terhadap Serangan Siber

Di Indonesia kesadaran masyarakat terhadap serangan siber di dunia maya masih cenderung rendah, dilansir dari web KOMDIGI yang mengambil penelitian yang dilakukan oleh Communication and Information System Security Research Center (CISSReC) di sembilan kota besar Indonesia hanya 33 persen yang secara praktis mengikuti himbauan dari KOMDIGI, inin menjelaskan bahwa banyak masyarakat yang masih tidak aware atau sadar akan bahayanya serangan siber

Beberapa bukti rendahnya kesadaran masyarakat adalah dengan adanya beberapa kasus serangan siber masif yang pernah viral di Indonesia, seperti serangan hacker Bjorka pada tahun 2024 yang menargetkan data djp (Direktorat Jenderal Pajak) dan membocorkan sekitar 6,6 juta data wajib pajak warga Indonesia termasuk Nomor Pokok Wajib Pajak (NPWP), serta informasi pribadi lainnya yang sangat sensitif. Ini membuktikan bahwa kesadaran masyarakat terhadap serangan siber sangat rendah.

# BAB III
# METODOLOGI DAN SOLUSI

## 3.1 Metodologi Perancangan

Metodologi yang digunakan dalam pengembangan proyek ini adalah metode *Prototyping*. Pendekatan ini dipilih karena sesuai untuk proyek yang menekankan pada interaksi pengguna dan desain antarmuka yang menarik, seperti dalam pengembangan media edukasi berbasis gamifikasi. Melalui metode ini, proses perancangan dilakukan secara iteratif dengan melibatkan pengguna dalam setiap tahap untuk memperoleh umpan balik yang berkelanjutan.

Adapun tahapan metodologi perancangan yang dilakukan adalah sebagai berikut:

1. Analisis Kebutuhan
   Pada tahap ini dilakukan identifikasi masalah dan kebutuhan pengguna terhadap media edukasi mengenai ancaman serangan DDoS. Kebutuhan diperoleh melalui studi literatur, observasi terhadap kasus-kasus serangan siber, serta analisis terhadap tingkat kesadaran masyarakat terhadap keamanan digital.
2. Perancangan Konsep dan Desain Awal (Prototyping)
   Tahap ini meliputi perancangan konsep gamifikasi yang akan diterapkan, seperti sistem poin, *leaderboard*, *quiz*, dan *reward*. Desain awal antarmuka (UI/UX) dibuat menggunakan Figma, untuk menggambarkan alur permainan dan interaksi pengguna dengan materi edukasi.
3. Pengembangan Prototipe
   Berdasarkan desain yang telah dibuat, dilakukan pembuatan prototipe interaktif menggunakan Unity atau platform berbasis web (seperti HTML5/JavaScript) untuk menampilkan simulasi cara kerja game edukatif tersebut. Prototipe ini berfungsi sebagai representasi awal media gamifikasi yang nantinya dapat diuji oleh pengguna.
4. Pengujian dan Evaluasi
   Prototipe diuji secara terbatas kepada sejumlah responden yang mewakili target pengguna, seperti mahasiswa atau masyarakat umum. Pengujian bertujuan untuk menilai tingkat keterlibatan (*engagement*), kemudahan penggunaan (*usability*), serta pemahaman pengguna terhadap materi keamanan siber yang disampaikan. Hasil evaluasi dijadikan dasar untuk melakukan penyempurnaan desain dan fitur.
5. Revisi dan Finalisasi
   Berdasarkan hasil evaluasi, dilakukan perbaikan terhadap aspek visual, mekanik permainan, dan efektivitas penyampaian materi edukatif. Prototipe yang telah disempurnakan kemudian siap untuk diimplementasikan dan digunakan sebagai media pembelajaran.

Tools dan Perangkat yang Digunakan:

1. Software Desain: Figma (untuk desain UI/UX)
2. Software Pengembangan: Unity / Construct 3 / HTML5
3. Alat Bantu Dokumentasi: Microsoft Word, Google Drive

4. Perangkat Uji: Laptop/PC, smartphone, dan jaringan internet

Metodologi ini memungkinkan tim pengembang untuk menghasilkan solusi yang tidak hanya inovatif, tetapi juga relevan dengan kebutuhan pengguna, serta dapat diuji dan diperbaiki secara berkelanjutan hingga mencapai hasil yang optimal.

## 3.2 Solusi

Solusi yang diusulkan dalam proyek ini adalah pengembangan media edukasi berbasis gamifikasi yang bertujuan untuk meningkatkan kesadaran masyarakat terhadap ancaman serangan DDoS dan pentingnya keamanan siber.

### 1. Penjelasan Solusi Utama

Solusi utama yang dikembangkan adalah aplikasi/game edukatif interaktif yang menggabungkan elemen permainan seperti tantangan (*challenges*), poin, *leaderboard*, dan penghargaan (*badges*). Dalam permainan ini, pengguna akan diberikan serangkaian skenario dan kuis yang berkaitan dengan konsep dasar keamanan siber, cara kerja serangan DDoS, serta langkah-langkah pencegahannya.

### 2. Cara Kerja Solusi

a. Pengguna memulai permainan dengan memilih tingkat kesulitan dan mengikuti alur cerita edukatif yang menggambarkan simulasi serangan DDoS.

b. Setiap level berisi penjelasan interaktif dan kuis singkat yang menguji pemahaman pengguna.

c. Sistem poin dan *reward* diberikan sebagai motivasi untuk menyelesaikan tantangan dengan benar.

Setelah menyelesaikan semua level, pengguna akan memperoleh sertifikat digital atau skor akhir sebagai indikator tingkat pemahaman mereka terhadap materi keamanan siber.

### 3. Manfaat Solusi

a. Bagi masyarakat: meningkatkan kesadaran dan pemahaman terhadap ancaman DDoS secara menyenangkan dan interaktif.

b. Bagi lembaga pendidikan: menjadi alternatif media pembelajaran yang inovatif untuk memperkenalkan topik keamanan siber.

c. Bagi pemerintah dan instansi keamanan digital: mendukung program literasi digital nasional dengan pendekatan yang lebih modern dan efektif.

### 4. Batasan Solusi

- Prototipe yang dikembangkan masih berfokus pada edukasi dasar mengenai DDoS dan belum mencakup semua jenis ancaman siber.

- Aplikasi bersifat simulatif dan edukatif, sehingga tidak mencakup fitur teknis seperti sistem deteksi atau perlindungan nyata terhadap serangan.

- Pengujian masih dilakukan dalam skala terbatas dan belum diuji secara luas di masyarakat umum.

Dengan solusi ini, diharapkan masyarakat dapat memahami ancaman serangan DDoS dengan cara yang lebih menarik dan mudah dipahami, sehingga meningkatkan literasi digital dan keamanan siber di lingkungan masyarakat Indonesia.

# BAB IV
# HIPOTESIS HASIL

Bab ini menggambarkan hipotesis hasil atau perkiraan terhadap keluaran yang akan diperoleh dari pelaksanaan proyek "Gamifikasi sebagai Media Edukasi untuk Meningkatkan Kesadaran Masyarakat terhadap Ancaman Serangan DDoS." Hipotesis mencakup prediksi keluaran utama, pencapaian tujuan, dan kesesuaian hasil dengan kajian pustaka yang telah dibahas pada Bab I–II. Berdasarkan pendekatan prototyping dan pengujian pengguna terbatas (Bab III), hasil yang diharapkan bersifat praktis dan dapat dievaluasi melalui metrik pengetahuan, keterlibatan (engagement), dan adopsi perilaku pencegahan.

## 4.1 Prediksi Keluaran Utama

Solusi yang dirancang diprediksi akan berjalan sesuai rancangan awal baik dari sisi teknis maupun fungsional. Dengan menggunakan Figma untuk desain, dan Unity / HTML5 (prototype interaktif) untuk pengembangan, keluaran utama yang diprediksi meliputi:

1. Prototype aplikasi/game edukatif interaktif yang mengandung: level skenario DDoS, kuis interaktif, sistem poin, badge, dan leaderboard.
2. Dokumentasi desain & teknis: file Figma (UI/UX), kode prototipe dasar (Unity/HTML5), serta panduan penggunaan singkat.
3. Modul evaluasi terstruktur: instrumen pre-test dan post-test untuk mengukur pengetahuan mengenai DDoS; kuesioner pengalaman pengguna (Likert) untuk usability dan kepuasan; serta log engagement untuk metrik penggunaan.
4. Laporan evaluasi pilot yang merangkum hasil tes, metrik engagement, feedback pengguna, dan rekomendasi perbaikan.

Secara fungsional, solusi ini diharapkan dapat:

1. Menyajikan materi tentang konsep DDoS dan langkah pencegahan dalam bentuk yang mudah dipahami melalui simulasi dan kuis singkat.

2. Meningkatkan motivasi belajar melalui elemen gamifikasi sehingga pengguna lebih terdorong menyelesaikan modul.
3. Menghasilkan data evaluatif (pre/post) yang dapat dipakai untuk menilai efektivitas intervensi.

### 4.2 Pencapaian Tujuan

Berdasarkan tujuan yang dirumuskan pada Bab I, proyek ini diperkirakan akan menghasilkan pencapaian berikut:

1. Meningkatkan pengetahuan pengguna tentang DDoS
   Diharapkan terdapat kenaikan skor rata-rata post-test dibanding pre-test. Target peningkatan 20–30%.
2. Meningkatkan keterlibatan pengguna dengan materi keamanan siber
   Indikator: completion rate modul, rata-rata waktu per sesi, dan jumlah interaksi (jawaban kuis, penggunaan fitur). Target rekomendasi: completion rate ≥ 50% pada pengujian pilot.
3. Memfasilitasi adopsi perilaku pencegahan sederhana
   Melalui kuesioner follow-up singkat, diharapkan >30% responden melaporkan telah melakukan minimal satu tindakan pencegahan (misalnya memperbarui password, memahami pentingnya konfigurasi firewall dasar) setelah menggunakan aplikasi.
4. Menghasilkan prototipe yang dapat diiterasi
   Prototipe siap untuk fase pengembangan lanjutan (penyempurnaan berdasarkan umpan balik) dan dokumentasi untuk replikasi atau integrasi ke program edukasi kampus/komunitas.
5. Memberi kontribusi praktis dan rekomendasi kebijakan
   Laporan akhir akan menyertakan rekomendasi implementasi gamifikasi dalam program literasi digital di tingkat institusi atau komunitas.

Metode evaluasi yang digunakan untuk menguji pencapaian tujuan meliputi uji perbedaan pre/post (paired t-test atau alternatif non-parametrik), analisis korelasi antara metrik engagement dan peningkatan skor, serta analisis kualitatif dari feedback pengguna untuk memahami aspek usability dan efektivitas pedagogis.

### 4.3 Kesesuaian dengan Kajian Pustaka

Berdasarkan tinjauan pustaka (Bab II) tentang gamifikasi dan literatur terkait *game-based learning* serta edukasi keamanan siber, hasil yang diprediksi diperkirakan selaras dengan temuan sebelumnya yang menyatakan bahwa elemen permainan dapat:

1. Meningkatkan motivasi intrinsik dan retensi informasi (teori *self-determination* dan *game-based learning*).

2. Menjadikan materi yang teknis lebih mudah diakses oleh audiens non-teknis melalui visualisasi dan simulasi interaktif.

Proyek ini akan memperkuat relevansi tersebut dalam konteks keamanan siber (khususnya DDoS) dengan memberikan bukti praktis berupa data pre/post serta metrik engagement. Dari sisi teori, pendekatan ini konsisten dengan konsep pembelajaran aktif dan pembelajaran berbasis pengalaman. Dengan demikian proyek ini diharapkan:

1. Mendukung literatur yang menunjukkan efektivitas gamifikasi dalam edukasi non-formal.
2. Memberikan bukti empiris baru pada konteks literasi keamanan siber masyarakat Indonesia, yaitu bahwa gamifikasi dapat meningkatkan kesadaran dan tindakan pencegahan terhadap ancaman seperti DDoS.
3. Menjadi referensi praktis bagi institusi pendidikan atau penyelenggara literasi digital yang ingin mengadopsi metode gamifikasi.

## DAFTAR PUSTAKA

Waskitojati, L. (2023). Mengenal Gamification (Gamifikasi). Dipublikasikan pada 21 September 2023.

Primacs. (2024, November 14). *Kasus-kasus Cyber Crime Terbesar yang Pernah Terjadi di Indonesia*. Primacs. Diperoleh dari https://www.primacs.co.id/post/kasus-kasus-cyber-crime-terbesar-yang-pernah-terjadi-di-indonesia

[Pusat Data dan Informasi, Kominfo]. (2020, Agustus 26). *Riset: Kesadaran Keamanan Siber di Masyarakat Masih Rendah*. Kementerian Komunikasi dan Informatika Republik Indonesia. Diperoleh dari https://www.komdigi.go.id/berita/sorotan-media/detail/riset-kesadaran-keamanan-siber-di-masyarakat-masih-rendah

**Microsoft.** (n.d.). *Apa itu Serangan DDoS?* Microsoft Security. Diperoleh dari https://www.microsoft.com/id-id/security/business/security-101/what-is-a-ddos-attack

## LAMPIRAN