**LAPORAN PROYEK AKHIR**

**LAPORAN PROYEK AKHIR**

**LAPORAN PENGEMBANGAN PRODUK PROYEK AKHIR**

**Chatbot CyberFox Platform Edukasi Keamanan Internet untuk Anak**

**-**

**Anak**

**/**

**PA 2**

**Disusun Oleh:**

**13323027**

**:**

**Pahala Putra Tambunan**

**13323006**

**:**

**Jhon Prima**

**Panjaitan**

**13323047**

**:**

**Agita Rahel Panjaitan**

**PROGRAM STUDI D3 TEKNOLOGI KOMPUTER**

**FAKULTAS VOKASI**

**INSTITUT TEKNOLOGI DEL**

1



**HALAMAN JUDUL LAPORAN PROYEK AKHIR**

LAPORAN PROYEK AKHIR



LAPORAN PENGEMBANGAN PRODUK PROYEK AKHIR

Chatbot CyberFox Platform Edukasi Keamanan Internet untuk Anak - Anak / PA2

**Disusun Oleh:**

|  |  |  |
| --- | --- | --- |
| **13323027** | **:** | **Pahala Putra Tambunan** |
| **13323006** | **:** | **Jhon Prima Panjaitan** |
| **13323047** | **:** | **Agita Rahel Panjaitan** |

PROGRAM STUDI D3 TEKNOLOGI KOMPUTER FAKULTAS VOKASI INSTITUT TEKNOLOGI DEL

2025

**DAFTAR ISI**

[BAB I 8](#_Toc200439446)

[PRODUCT REQUIREMENT SPECIFICATION 8](#_Toc200439447)

[(SPESIFIKASI KEBUTUHAN PRODUK) 8](#_Toc200439448)

[1.1 PENDAHULUAN 8](#_Toc200439449)

[1.1.1. Tujuan Penulisan Dokumen 9](#_Toc200439450)

[1.1.2. Latar Belakang Produk 9](#_Toc200439451)

[1.1.3. Tujuan Produk 9](#_Toc200439452)

[1.1.5. Manfaat Produk 11](#_Toc200439453)

[1.1.6. Definisi dan Singkatan 12](#_Toc200439454)

[1.1.7. Referensi 12](#_Toc200439455)

[1.2. DESKRIPSI UMUM PRODUK 13](#_Toc200439456)

[1.2.1. Permasalahan dan Persoalan 13](#_Toc200439457)

[1.2.5. Deskripsi Kebutuhan Produk 14](#_Toc200439458)

[1.2.7. Metodologi dan Tools Pengembangan 16](#_Toc200439459)

[BAB II 18](#_Toc200439460)

[PROJECT PLANNING (PP) (PERENCANAAN PENGEMBANGAN PRODUK) 18](#_Toc200439461)

[2.1. PENDAHULUAN 18](#_Toc200439462)

[2.2.DESKRIPSI PROYEK 18](#_Toc200439463)

[2.2.1. Project Organization 18](#_Toc200439464)

[2.2.2. Work Breakdown Structure (WBS 19](#_Toc200439465)

[2.2.3. Budget 19](#_Toc200439466)

[2.2.4. Tools 20](#_Toc200439467)

[2.2.5. Resiko dan Hambatan 21](#_Toc200439468)

[BAB III 22](#_Toc200439469)

[PRODUCT DESIGN (PD) (DESAIN PENGEMBANGAN PRODUK) 22](#_Toc200439470)

[3.1.PENDAHULUAN 22](#_Toc200439471)

[3.2. DESKRIPSI PRODUK DESIGN 23](#_Toc200439472)

[3.2.1. Proses Bisnis Fungsi Login 23](#_Toc200439473)

[3.2.2. Proses Bisnis Fungsi Register 23](#_Toc200439474)

[3.2.3. Proses Bisnis Fungsi Mengirimkan Pertanyaan 23](#_Toc200439475)

[3.2.4. Proses Bisnis Fungsi Menampilkan Dashboard Admin 24](#_Toc200439476)

[3.2.5. Use Case Diagram 24](#_Toc200439477)

[3.2.6. User Characteristic 25](#_Toc200439478)

[3.2.7. Sequence Diagram 25](#_Toc200439479)

[3.2.8. Sequence Diagram System 25](#_Toc200439480)

[3.2.9. Entity Relationship Diagram (ERD) 26](#_Toc200439481)

[3.2.10 Conceptual Data Model (CDM) 27](#_Toc200439482)

[3.2.11 WireFrame Halaman Login 27](#_Toc200439483)

[3.2.12. Wireframe Halaman Chatbot 27](#_Toc200439484)

[3.2.13. High-Level Architecture (HLA) 28](#_Toc200439485)

[3.2.15 Database Schema 39](#_Toc200439486)

[3.2 Modifikasi RAG Menggunakan Langchain untuk Proyek CyberFox 42](#_Toc200439487)

[3.2.1 Tujuan Modifikasi 42](#_Toc200439488)

[BAB IV 43](#_Toc200439489)

[PENGEMBANGAN PRODUK) 43](#_Toc200439490)

[4.1.PENDAHULUAN 43](#_Toc200439491)

[4.2.DESKRIPSI 43](#_Toc200439492)

[4.2.1. Prinsip Implementasi 43](#_Toc200439493)

[4.2.2. Lingkungan Pengembangan Terintegrasi (IDE) 44](#_Toc200439494)

[4.2.3 Hasil Implementasi 45](#_Toc200439495)

[BAB V 52](#_Toc200439496)

[PRODUCT TESTING (PT) (PENGUJIAN PRODUK) 52](#_Toc200439497)

[5.1. PENDAHULUAN 52](#_Toc200439498)

[5.2. DESKRIPSI PENGUJIAN 52](#_Toc200439499)

[5.2.1. BUTIR UJI 52](#_Toc200439500)

[5.2.1. TOOLS PENGUJIAN 56](#_Toc200439501)

[5.3. METODE PENGUJIAN 56](#_Toc200439502)

[5.3.1. Pengujian Fungsional 57](#_Toc200439503)

[5.3.2. Pengujian Non Fungsional 58](#_Toc200439504)

[BAB VI 60](#_Toc200439505)

[PRODUCT RELEASE (PR) (PELUNCURAN PRODUK) 60](#_Toc200439506)

[6.1. PENDAHULUAN 60](#_Toc200439507)

[6.2.DESKRIPSI 60](#_Toc200439508)

[6.2.1. DAYA GUNA PRODUK 60](#_Toc200439509)

[6.3 POSTER PRODUK 61](#_Toc200439510)

[DAFTAR PUSTAKA 63](#_Toc200439511)

[LAMPIRAN 64](#_Toc200439512)

[Dokumentasi Pengumpulan Data 67](#_Toc200439513)

[Data Set Tambahan 71](#_Toc200439514)

**DAFTAR GAMBAR**

[Gambar 1 Siklus hidup pengembangan produk 8](#_Toc200398514)

[Gambar 2 Metodologi 17](#_Toc200398515)

[Gambar 3 Project Organization 18](#_Toc200398516)

[Gambar 4 Work Breakdown Structure (WBS) 19](#_Toc200398517)

[Gambar 5 Proses Bisnis Fungsi Login 23](#_Toc200398518)

[Gambar 6 Proses Bisnis Fungsi Register 23](#_Toc200398519)

[Gambar 7 Proses Bisnis Fungsi Mengirimkan Pertanyaan 23](#_Toc200398520)

[Gambar 8 Proses Bisnis Fungsi Menampilkan Dashboard Admin 24](#_Toc200398521)

[Gambar 9 Use Case Diagram 24](#_Toc200398522)

[Gambar 10 user characteristic 25](#_Toc200398523)

[Gambar 11 Proses Bisnis Fungsi Mengirimkan Pertanyaan 26](#_Toc200398524)

[Gambar 12 Sequence Diagram CyberFox 26](#_Toc200398525)

[Gambar 13 Conceptual Data Model (CDM) 27](#_Toc200398526)

[Gambar 14 WireFrame Halaman Login 27](#_Toc200398527)

[Gambar 15 WireFrame Halaman Login 27](#_Toc200398528)

[Gambar 16 High-Level Architecture (HLA) 28](#_Toc200398529)

[Gambar 17 System Design 31](#_Toc200398530)

[Gambar 18 System Design 32](#_Toc200398531)

[Gambar 19 Diagram Query Analysis & Retrieval 37](#_Toc200398532)

[Gambar 20 Diagram ERD 41](#_Toc200398533)

[Gambar 21 Login 45](#_Toc200398534)

[Gambar 22 Halaman Chatbot 45](#_Toc200398535)

[Gambar 23 Menu Riwayat Chat 46](#_Toc200398536)

[Gambar 24 ChatbotHandler 46](#_Toc200398537)

[Gambar 25 Query Processing 48](#_Toc200398538)

[Gambar 26 HandleChatbotInteraction, processChatbotRequestFull 49](#_Toc200398539)

[Gambar 27 HandleTextQuery 50](#_Toc200398540)

[Gambar 28 ProcessTextWithAI 51](#_Toc200398541)

[Gambar 29 Poster Produk 62](#_Toc200398542)

[Gambar 30 FItur Utama 62](#_Toc200398543)

**DAFTAR TABEL**

[Tabel 1 Ruang Lingkup Produk 10](#_Toc200398700)

[Tabel 2 Daftar Definisi dan Singkatan 12](#_Toc200398701)

[Tabel 3 Daftar Definisi dan Singkatan 12](#_Toc200398702)

[Tabel 4 Kebutuhan Fungsional 14](#_Toc200398703)

[Tabel 5 Kebutuhan NonFungsional 15](#_Toc200398704)

[Tabel 6 Environment Hardware dan Software 15](#_Toc200398705)

[Tabel 7 Environment Hardware dan Software 16](#_Toc200398706)

[Tabel 8 Tools Pengembangan 17](#_Toc200398707)

[Tabel 9 Budget yang diperlukan 19](#_Toc200398708)

[Tabel 10 Tools 20](#_Toc200398709)

[Tabel 11 Kebutuhan Teknis 33](#_Toc200398710)

[Tabel 12 1. sessions (Menyimpan sesi percakapan Chatbot) 39](#_Toc200398711)

[Tabel 13 1. messages ( Menyimpan pesan chatbot ) 39](#_Toc200398712)

[Tabel 14 3. intents ( Menyimpan intent chatbot ) 39](#_Toc200398713)

[Tabel 15 4. responses (Menyimpan respons chatbot) 40](#_Toc200398714)

[Tabel 16 5. logs (Menyimpan aktivitas sistem) 40](#_Toc200398715)

[Tabel 17 Komponen Yang Dimodifikasi 42](#_Toc200398716)

[Tabel 18 Lingkungan Pengembangan Terintegrasi (IDE) 44](#_Toc200398717)

[Tabel 19 Testing Fungsi Login 52](#_Toc200398718)

[Tabel 20 Testing Fungsi Register 53](#_Toc200398719)

[Tabel 21 Testing Fungsi Ajukan Pertanyaan 54](#_Toc200398720)

[Tabel 22 Testing Fungsi Melihat History 55](#_Toc200398721)

# BAB I

# PRODUCT REQUIREMENT SPECIFICATION

# (SPESIFIKASI KEBUTUHAN PRODUK)

## 1.1 PENDAHULUAN

Dokumen ini menjelaskan proses pengembangan produk CyberFox, sebuah chatbot edukatif bertema keamanan siber yang ditujukan untuk anak-anak dan remaja. Produk ini dikembangkan dengan mengikuti siklus hidup pengembangan produk, yang mencakup tahapan-tahapan sistematis untuk memastikan bahwa produk yang dihasilkan sesuai dengan kebutuhan pengguna dan siap digunakan.



Requirement



Analysis



System Design



Implementation



System Testing



Deployment /



Release



Evaluation and



Maintenance

Gambar 1 Siklus hidup pengembangan produk

#### 1. Analisis Kebutuhan

Mengidentifikasi dan mengumpulkan kebutuhan fungsional maupun non-fungsional berdasarkan kebutuhan pengguna sasaran, termasuk tujuan edukasi keamanan siber untuk anak dan remaja.

2. Perancangan Sistem

Merancang arsitektur sistem, komponen, antarmuka pengguna (UI), dan alur data agar produk memenuhi tujuan teknis dan edukatif yang diharapkan.

3. Pengujian Sistem

Melakukan verifikasi dan validasi sistem melalui pengujian fungsional, pengujian antarmuka pengguna (UI/UX), dan akurasi respons chatbot untuk memastikan sistem

bekerja dengan benar.

4. Implementasi (Deployment)

Merilis aplikasi agar dapat digunakan oleh pengguna sasaran, termasuk menyiapkan infrastruktur hosting, domain, dan memastikan aksesibilitas secara daring.

5. Evaluasi dan Pemeliharaan

Memantau performa sistem, mengumpulkan umpan balik dari pengguna, memperbaiki bug, memperbarui konten edukasi, serta meningkatkan fitur secara berkala.

### 1.1.1. Tujuan Penulisan Dokumen

Dokumen ini disusun untuk memberi panduan utama yang terstruktur dan sistematis dalam pengembangan sistem chatbot edukatif CyberFox. Tujuan utamanya adalah untuk menguraikan kebutuhan produk secara rinci, menjadi referensi utama ketika mengambil keputusan saat pengembangan.

### 1.1.2. Latar Belakang Produk

Penggunaan internet dan media sosial semakin luas di kalangan anak – anak dan remaja, membawa dampak positif namun membawa dampak negatif juga, anak – anak dan remaja rentan terhadapat kejahatan kejahatan dunia digital, seperti phising, penipuan online dan penyalahgunaan data pribadi. Untuk itu, CyberFox hadir sebagai chatbot edukatif berbasis Retrieval-Augmented Generation (RAG) yang memberi edukasi mengenai keamanan di dunia digital kepada anak-anak dan remaja.

### 1.1.3. Tujuan Produk

Tujuan dari pengembangan produk CyberFox ini adalah:

1. Menciptakan chatbot edukatif yang memberikan informasi mengenai keamanan siber secara interaktif dan mudah dipahami oleh anak-anak dan remaja.
2. Meningkatkan kesadaran dan pemahaman pengguna muda tentang ancaman digital serta cara melindungi akun, identitas, dan perangkat dari serangan siber.
3. Menyediakan platform yang berbasis Retrieval-Augmented Generation (RAG) untuk memberikan jawaban yang relevan, akurat, dan kontekstual sesuai dengan pertanyaan pengguna.
4. Memfasilitasi akses yang cepat dan mudah untuk edukasi keamanan siber kapan saja dan di mana saja.
5. Mendukung pengembangan literasi digital dan keamanan siber untuk generasi muda sebagai langkah preventif terhadap ancaman online.

#### 1.1.4. Ruang Lingkup Produk

Ruang lingkup pengembangan CyberFox mencakup pembuatan chatbot edukatif yang bertujuan untuk meningkatkan kesadaran dan pemahaman pengguna muda mengenai keamanan siber. Fitur utama dari produk ini meliputi:

1. Edukasi tentang Keamanan Akun: Memberikan informasi tentang cara melindungi akun pengguna dari ancaman siber, seperti phishing dan hacking.
2. Pengenalan Identitas Digital: Menyediakan panduan tentang bagaimana menjaga data pribadi di dunia digital, termasuk pengaturan privasi di media sosial.
3. Simulasi Serangan Siber: Menyajikan simulasi sederhana tentang jenis-jenis serangan yang bisa terjadi dan cara mencegahnya.
4. Interaksi dengan Chatbot: Menggunakan Coherre untuk membangun chatbot berbasis Retrieval-Augmented Generation (RAG) yang memberikan jawaban relevan dan kontekstual terkait pertanyaan pengguna.
5. Akses Edukasi Seiring Waktu: Pengguna dapat mengakses informasi kapan saja untuk meningkatkan pemahaman mereka mengenai topik-topik keamanan siber

Tabel 1 Ruang Lingkup Produk

|  |  |
| --- | --- |
| **Batasan Teknis** | **Batasan Non Teknis** |
| Pengembangan chatbot berbasis Coherre yang menggunakan model AI untuk pencarian informasi relevan dan generasi teks berdasarkan permintaan pengguna. | Produk ini ditujukan untuk pengguna muda, terutama anak-anak dan remaja, dengan tampilan yang ramah dan mudah dimengerti. |
| Penyimpanan data interaksi pengguna dan riwayat percakapan di PostgreSQL untuk pengelolaan data struktural. | Fokus pada edukasi yang menyenangkan dan interaktif, bukan pada implementasi fitur-fitur kompleks lainnya. |
| Penyimpanan dan pencarian vektor untuk kemampuan pencarian yang efisien menggunakan Pinecone, yang mendukung penyimpanan dan pengelolaan data dalam bentuk vektor untuk pencarian berbasis semantik. | Sistem tidak dirancang untuk menangani pengolahan data yang bersifat sensitif atau pribadi di luar konteks pembelajaran keamanan siber. |

**Pengguna Produk**:

• Anak-anak dan remaja yang tertarik untuk mempelajari lebih lanjut tentang keamanan siber.

### 1.1.5. Manfaat Produk

Manfaat yang diharapkan dari produk CyberFox ini meliputi:

1. Teknis: Memberikan edukasi tentang keamanan siber secara interaktif dan berbasis data yang relevan, meningkatkan kemampuan pengguna dalam melindungi akun, identitas, dan data pribadi mereka dari ancaman siber.
2. Lingkungan: Meningkatkan kesadaran tentang pentingnya keamanan digital yang berkelanjutan, dengan cara yang ramah bagi pengguna muda, sekaligus mengurangi potensi kerugian yang disebabkan oleh serangan siber.
3. Pengguna: Memberikan pengalaman yang mudah dan menyenangkan dalam mempelajari cara-cara melindungi diri dari ancaman siber, serta memperkuat pemahaman mereka mengenai pentingnya keamanan digital dalam kehidupan seharihari.

### 1.1.6. Definisi dan Singkatan

Tabel 2 Daftar Definisi dan Singkatan

|  |  |  |
| --- | --- | --- |
| **No** | **Definisi/Singkatan** | **Keterangan** |
| 1 | RAG | Retrieval-Augmented Generation – Metode AI yang menggabungkan kemampuan pencarian (retrieval) dengan model generatif (LLM) untuk memberikan jawaban berbasis informasi yang rele |
| 2 | API | Application Programming Interface – Antarmuka yang memungkinkan aplikasi atau layanan berbeda saling berkomunikasi dan bertukar data. |
| 3 | LangChain | Framework open-source untuk membangun aplikasi AI berbasis LLM yang terhubung dengan sumber data eksternal (seperti API, database, dokumen). |
| 4 | LLM | Large Language Model – Model AI berskala besar yang dilatih untuk memahami dan menghasilkan teks alami, seperti GPT-4 |
| 5 | Retrieval | Proses pencarian dan pengambilan informasi yang relevan dari basis data atau dokumen untuk mendukung jawaban model. |
| 6 | PostgreSQL | Sistem manajemen basis data relasional open-source yang kuat, digunakan untuk menyimpan data pengguna dan log interaksi chatbot. |
| 7 | Pinecone | Layanan vector database untuk menyimpan dan mencari embedding (representasi vektor) dari data teks, sering digunakan dalam sistem RAG untuk pencarian semantik cepat. |

Tabel 3 Daftar Definisi dan Singkatan

|  |  |  |
| --- | --- | --- |
| **No** | **Definisi/Singkatan** | **Keterangan** |
| 1 | Sw | Software: perangkat lunak yang akan dikembangkan oleh tim |
| 2 | Framework | struktur yang disediakan untuk mengembangkan aplikasi atau solusi perangkat lunak |

### 1.1.7. Referensi

Referensi yang digunakan dalam pengembangan CyberFox meliputi penelitian, teknologi, dan solusi yang telah ada sebelumnya. Berikut beberapa referensi utama:

1. Abba, S., & Garba, A. M. (2020). An IoT-Based Smart Framework for a Human Heartbeat Rate Monitoring and Control System.
2. Afif, A., Nubli, A., Addani, F., & Nugrahaeni, C. (2020). Aplikasi Pelayanan

Kantin Pada Kantin Upn “Veteran” Jakarta. Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA) Jakarta-Indonesia.

1. Berryman, C., Ferguson, C. J., & Negy, C. (2018). Social Media Use and Mental Health among Young Adults. Cyberpsychology, Behavior, and Social Networking, 21(12), 711–717.
2. Henderson, M., Snyder, A., & Beale, N. (2020). Digital Parenting: Challenges and Opportunities in Monitoring Children's Online Activities. Journal of Cybersecurity Research, 5(2), 45–60.

## 1.2. DESKRIPSI UMUM PRODUK

###### **1.2.1. Permasalahan dan Persoalan**

1. **Permasalahan**

Rendahnya literasi anak anak dan remaja menyebabkan mereka rentan terhadap penipuan online seperti phising, pencurian data pribadi, dan konten konten negatif yang tidak sesuai. Di sisi lain, materi edukasi tentang keamanan digital sulit dipahami karena disajikan dalam buku buku ilmiah yang memiliki bahasa teknis dan kaku.

1. **Persoalan**

Anak – anak dan remaja sering kali belum memiliki kesadaran serta pengetahuan yang memadai untuk mengenail dan menghindari ancaman siber. Salah satu penyebabnya adalah anak – anak dan remaja hanya mampu masuk dunia digital tanpa memiliki literasi atau pengalaman edukasi yang cukup dalam dunia digital.

1. **Dampak**

Anak – anak dan remaja rentan terhadap penipuan di dunia digital, atau mengalami gangguan mental akibat Cyberbullying. Hal ini menekankan pentingnya sebuah solusi yang mampu menyampaikan edukasi keamanan digital dengan cara yang menyenangkan dan mudah dipahami, tanpa harus membaca buku buku atau artikel ilmiah.

###### 1.2.2. Produk yang menjadi Inspirasi

Salah satu produk yang menjadi inspirasi dalam pengembangan CyberFox adalah repositori

GitHub “RAG\_chatabot\_with\_Langchain” oleh AlaGrine. Produk ini menerapkan pendekatan RetrievalAugmented Generation (RAG) yang dikombinasikan dengan LangChain sebagai kerangka kerja utama, serta mendukung berbagai model bahasa besar (LLM) seperti GPT-4, Gemini-pro, dan lainnya. Sistem ini memungkinkan pengguna mengunggah berbagai jenis dokumen (pdf, txt, csv, docx) dan berinteraksi dengan kontennya melalui antarmuka chatbot berbasis Streamlit. Kelebihan utama dari sistem ini adalah fleksibilitas dalam memilih model LLM dan kemudahan integrasi dengan sumber data berbasis dokumen, namun belum disesuaikan secara spesifik untuk kebutuhan edukasi keamanan digital bagi anak dan remaja. Oleh karena itu, CyberFox dikembangkan dengan menyesuaikan konten dan antarmuka agar lebih ramah pengguna serta fokus pada pembelajaran interaktif dan aman seputar keamanan siber.

###### 1.2.3. Produk yang akan dibangun

Produk yang akan dibangun adalah CyberFox, sebuah chatbot edukatif berbasis teknologi Retrieval-Augmented Generation (RAG). Dirancang sebagai platform edukasi untuk anak – anak dan remaja.

Beberapa fitur utama yang akan diimplementasikan antara lain:

1. Antarmuka chatbot yang ramah anak dengan tampilan menarik dan mudah digunakan.
2. Sistem RAG yang memungkinkan chatbot menjawab pertanyaan berdasarkan dokumen atau materi edukasi yang disediakan.
3. Sistem pencatatan interaksi untuk analisis pemahaman pengguna.
4. Penyimpanan data menggunakan PostgreSQLdan pencarian cepat berbasis vektor menggunakanPinecone**.**

###### 1.2.4. Konteks

Sistem CyberFox merupakan chatbor edukatif berbasis web yang dirancang untuk memberi edukasi mengenai keamanan kiber kepada anak – anak dan remaja melalui chatbot berbasis *Large Language Model* (LLM) dan *Retrieval-Augmented Generation* (RAG). Sistem ini terdiri dari beberapa komponen utama, yaitu antarmuka chatbot ramah anak, backend integrasi LLM menggunakan LangChain, modul RAG untuk pencarian kontekstual dari database edukasi, serta penyimpanan data menggunakan PostgreSQL dan Pinecone. Stakeholder yang terlibat mencakup anak – anak pelajar SD sampai SMA, administator.

### 1.2.5. Deskripsi Kebutuhan Produk

#### 1.2.5.1 Kebutuhan Fungsional:

Tabel 4 Kebutuhan Fungsional

|  |  |  |
| --- | --- | --- |
| **No** | **Fitur** | **Deskripsi** |
| 1 | Modul Chatbot Edukasi | Menyediakan percakapan edukatif tentang keamanan siber menggunakan teknologi LLM. |
| 2 | Modul RAG (Retrieval-  Augmented Generation) | Mengambil informasi dari sumber referensi yang telah disiapkan (dokumen keamanan digital) untuk memperkaya jawaban chatbot. |
| 3 | Modul Admin Panel | Mengelola data pengguna dan aktivitas sesi pengguna |
| 4 | Modul Monitoring &  Logging | Merekam aktivitas interaksi pengguna untuk keperluan evaluasi dan keamanan |

#### 1.2.5.2 Kebutuhan NonFungsional

Tabel 5 Kebutuhan NonFungsional

|  |  |  |
| --- | --- | --- |
| **No** | **Aspek** | **Kebutuhan** |
| 1 | Reliability | Sistem harus memiliki tingkat ketersediaan tinggi (uptime minimal  99%) agar dapat diakses kapan pun |
| 2 | Performance | Respon chatbot harus diberikan dalam waktu kurang dari 3 detik setelah input pengguna |
| 3 | Security | Seluruh data pengguna, terutama anak-anak, harus dienkripsi dan dilindungi dengan kebijakan privasi ketat |
| 4 | Usability | Antarmuka harus ramah anak dengan navigasi sederhana dan visual yang menarik |
| 5 | Scalability | Sistem dirancang agar dapat menangani pertumbuhan jumlah pengguna tanpa penurunan performa |
| 6 | Maintainablity | Sistem modular untuk memudahkan pembaruan konten dan pengembangan fitur tambahan |

#### 1.2.6. Environment Hardware dan Software

Tabel 6 Environment Hardware dan Software

|  |  |  |
| --- | --- | --- |
| **No** | **Hardware** | **Spesifikasi atau Keterangan** |
| 1 | Laptop/PC Developer | Minimal Intel i7, RAM 8 GB, SSD 512 |
| 2 | Jaringan | Akses internet, untuk komunikasi dengan Coherre |

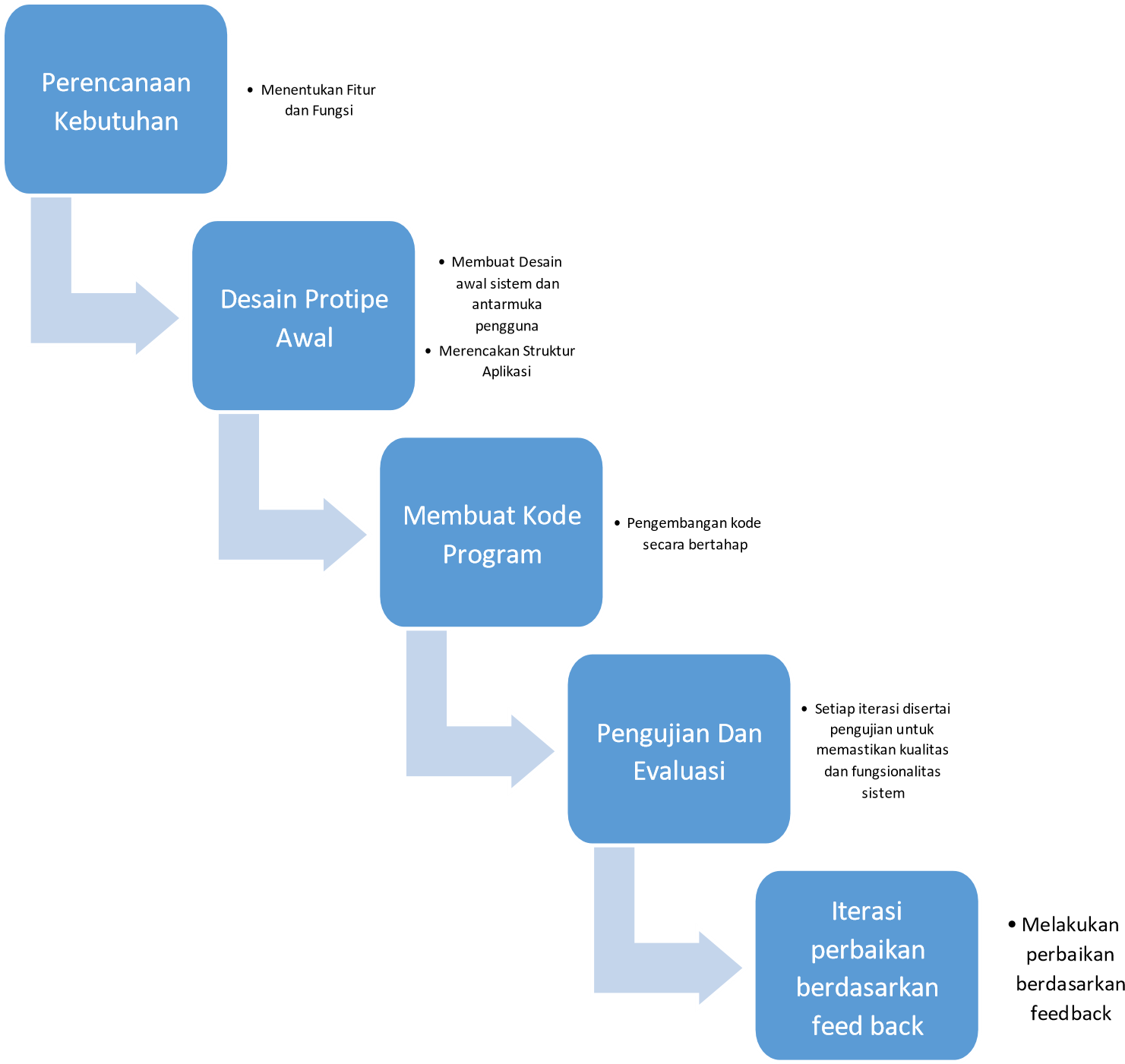
Tabel 7 Environment Hardware dan Software

|  |  |  |
| --- | --- | --- |
| **No** | **Software** | **Spesifikasi atau Keterangan** |
| 1 | Node.js | Backend untuk REST API dan interaksi dengan Frontend |
| 2 | Max (Jika menggunakan) | Untuk pengolahan data atau analisis tambahan sesuai kebutuhan |
| 3 | TypeScript | Untuk pengembangan aplikasi frontend dengan keunggulan tipe statis |
| 4 | JavaScript | Digunakan di frontend dan backend untuk scripting |
| 5 | Tailwind CSS | Styling responsif dan estetis untuk antarmuka pengguna |
| 6 | LangChain Framework | Untuk orkestrasi RAG dan pengelolaan interaksi dengan  LLM |
| 7 | PineCone Vector DB | Untuk penyimpanan dan pencarian embedding dokumen edukasi |
| 8 | PostgreSQL | Penyimpanan data pengguna dan metadata percakapan |
| 9 | SQL | Digunakan untuk pengolahan dan manajemen data dalam database PostgreSQL |

### 1.2.7. Metodologi dan Tools Pengembangan

#### 1.2.7.1. Metodologi

Metodologi yang akan digunakan dalam pengembangan produk ini adalah Agile, yang dipilih karena kemampuannya untuk mendukung proses pengembangan sistem secara iteratif dan adaptif. Dalam pendekatan ini, proyek dibagi menjadi beberapa siklus pendek yang disebut iterasi, memungkinkan pengembangan produk yang lebih fleksibel dan dapat disesuaikan dengan kebutuhan pengguna yang berubah.



Gambar 2 Metodologi

#### 1.2.7.2. Tools Pengembangan

Tools dan perangkat lunak yang digunakan untuk mendukung tahapan perancangan, pengkodean dan pengujian dapat dilihat pada tabel berikut.

Tabel 8 Tools Pengembangan

|  |  |  |
| --- | --- | --- |
| No | Tools | Deskripsi |
| 1 | Node.js | Platform runtime JavaScript yang digunakan untuk menjalankan backend dan mengelola dependensi proyek |
| 2 | TypeScript dan JavaScript | Bahasa pemrograman utama dalam pengembangan frontend dan backend |
| 3 | Tailwind CSS | Framework CSS untuk mempercepat proses styling antarmuka pengguna secara efisien dan konsisten |
| 4 | LangChain Framework | Digunakan untuk membangun fitur chatbot berbasis Large Language Model (LLM) dan integrasi dengan sumber data eksternal |
| 5 | SQL | Bahasa query untuk pengelolaan database |

# BAB II

# PROJECT PLANNING (PP) (PERENCANAAN PENGEMBANGAN PRODUK)

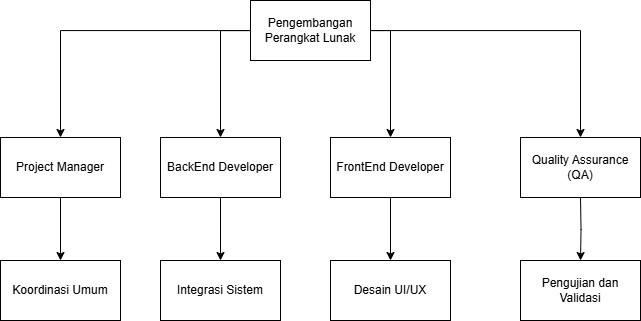
## 2.1. PENDAHULUAN

Perencanaan pengembangan produk merupakan tahap penting yang bertujuan untuk memastikan proses pembangunan sistem berjalan secara terstuktur, efisien, dan sesuai dengan kebutuhan pengguna akhir. Proyek ini dirancang sebagai solusi terhadap permasalahan keterbatasan sistem chatbot dalam memberikan layanan berbasis data yang relevan dan terverifikasi. Dengan menggabungkan teknologi pemrosesan bahasa alami (NLP) menggunakan LangChain serta basis data yang terstruktur, sistem ini diharapkan mampu menghadirkan chatbot yang tidak hanya responsif, tetapi juga mampu memberikan jawaban yang didukung oleh sumber data internal yang dapat diandalkan.

## 2.2.DESKRIPSI PROYEK

Proyek ini bertujuan mengembangkan CyberFox, chatbot berbasis Retrieval-Augmented Generation (RAG) yang mengintegrasikan framework LangChain. Sasaran pengguna dari proyek ini adalah anak – anak sampai SMA yang rentan terkena penipuan dan terkena paparan konten negatif pada dunia digital, dan mereka membutuhkan akses cepat terhadap informasi yang sering ditanyakan tanpa harus menelusuri dokumen secara manual.

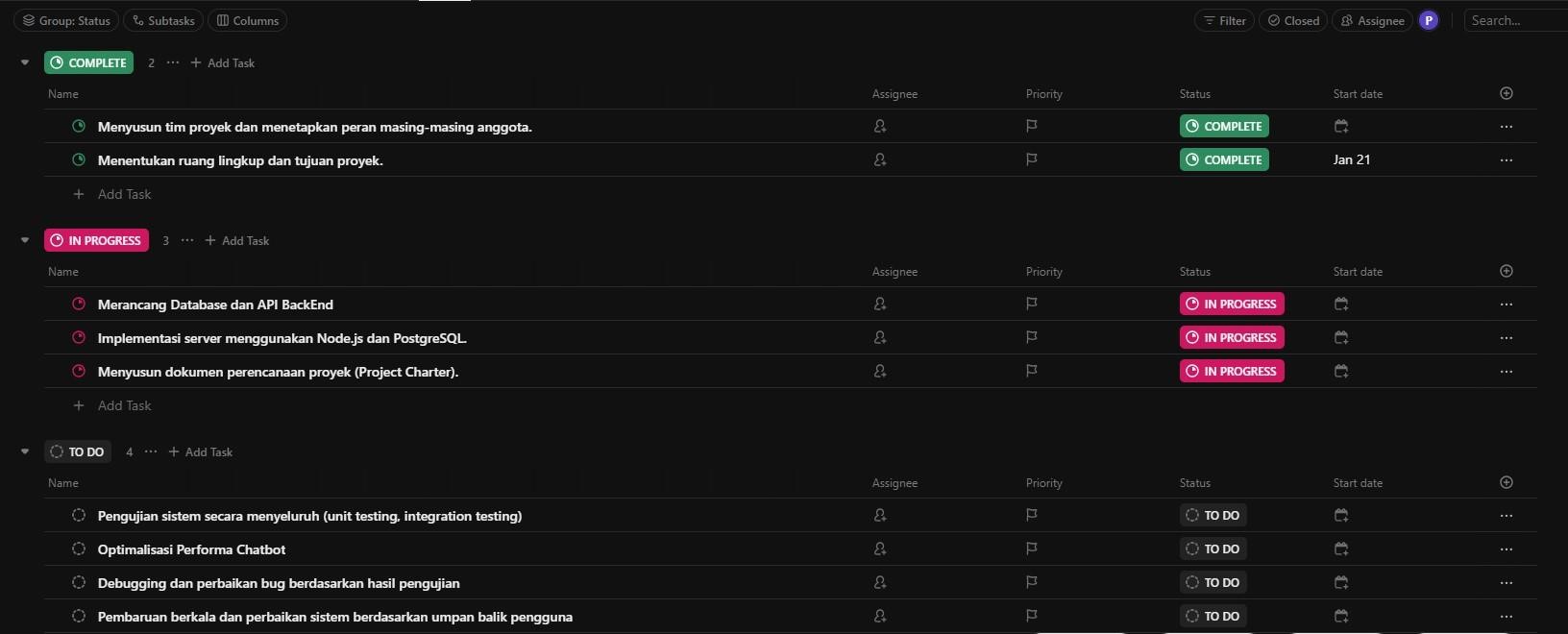
### 2.2.1. Project Organization



Gambar 3 Project Organization

Struktur organisasi proyek ini dibentuk secara kolaboratif, dengan Project Leader sebagai orang yang memberi koordinasi dan yang mengawasi keseluruhan pengembangan. Project Leader bertanggung jawab atas perencanaan, pemantauan, serta pengambilan Keputusan dan menjembatani komunikasi antar anggota tim.

2.2.2. Work Breakdown Structure (WBS**)**



Gambar 4 Work Breakdown Structure (WBS)

### 2.2.3. Budget

Bagian ini menjelaskan alokasi anggaran untuk proyek secara keseluruhan, termasuk perincian biaya yang dibutuhkan pada setiap fase proyek dan berbagai komponen yang akan mengeluarkan biaya. Budget yang tepat sangat penting untuk memastikan bahwa proyek dapat dilaksanakan sesuai dengan rencana dan tidak melebihi anggaran yang telah disepakati.

Tabel 9 Budget yang diperlukan

|  |  |  |  |
| --- | --- | --- | --- |
| **Biaya pengembangan Proyek Akhir**  **Jumlah**  **Satuan** | | | **Total** |
| **A. Biaya selama tahapan pengembangan perangkat lunak** |  |  |  |
| **1. Requirement Gathering** | 1 | Rp 150.000 | Rp150.000 |
| **2. Analisis** | 1 | Rp 0 | Rp 0 |
| **3. Desain** | 1 | Rp 0 | Rp 0 |
| **4. Implementasi** | 1 | Rp 0 | Rp 0 |
| **5. Testing** | 1 | Rp 0 | Rp 0 |
| **6. Maintenance** | 1 | Rp 0 | Rp 0 |
| **Total** |  |  | Rp 150.000 |
| **B. Biaya untuk pengembang perangkat lunak** |  |  |  |
| **1. Project Manager** | 2 | Rp 0 | Rp0 |
| **2. System analyst** | 1 | Rp 0 | Rp 0 |
| **3. Programmer** | 1 | Rp 0 | Rp 0 |
| **Total** |  |  | Rp 150.000 |

### 2.2.4. Tools

Berikut merupakan tools yang digunakan dalam pelaksanaan proyek. Pemilihan alat yang tepat sangat penting untuk memastikan kelancaran pengembangan,pengujian, manajemen proyek.

Tabel 10 Tools

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Hardware** | **Software** | **Tool managemen proyek** | | **Alat bantu untuk kolaborasi tim** | **Tools untuk simulasi, desain, pengujian** | **Alasan pemilihan tools** |
| 1. | Laptop | Node.js,  TypeScript,  JavaScript | Click  Trello | Up, | Github | Figma | Laptop digunakan untuk menuliskan kode dan running. Node.js dipilih untuk backend karena performa yang cepat.  TypeScript dan  JavaScript digunakan untuk meningkatakan stuktur kode. ClickUp digunakan untuk memantau dan mengelola tugas proyek. Github untuk kolaborasi dan komunikasi tim. Postman, Figma untuk pengujian dan desaain UI/UX. |
| 2 | Server | SQL,  LangChain  Framework | - |  | Github | Figma | Server digunakan untuk pengujian dan penyimpanan data. SQL dipilih untuk manajemen data relasional. LangChain digunakan untuk aplikasi berbasis  AI. |

### 2.2.5. Resiko dan Hambatan

1. **Keterlambatan Proses dan Performa Sistem** Penggunaan teknologi seperti pemrosesan teks dan pencocokan model besar bisa menyebabkan waktu eksekusi yang lama, terutama jika volume data yang harus diproses sangat besar. Untuk mengatasi hal ini, solusi yang dapat diterapkan termasuk pengoptimalan algoritma dan penggunaan teknik caching untuk menyimpan hasil sementara.
2. **Ketepatan Hasil Pemrosesan Model**

Menggunakan model berbasis pembelajaran mesin dalam sistem bisa menimbulkan hasil yang kurang akurat, terutama dalam kasus-kasus yang melibatkan ambiguitas atau konteks yang lebih rumit. Oleh karena itu, penting untuk menerapkan mekanisme validasi tambahan atau filter untuk memastikan jawaban yang diberikan lebih tepat dan relevan.

1. **Risiko Keamanan Data Pengguna**

Dalam sistem yang mengumpulkan dan memproses data pengguna, sangat penting untuk menjaga kerahasiaan data pribadi dan interaksi percakapan. Kebocoran informasi sensitif harus dihindari dengan menggunakan enkripsi data saat transit dan penyimpanan, serta implementasi kontrol akses yang ketat untuk memastikan hanya pihak yang berwenang yang dapat mengakses informasi tersebut.

1. **Keterbatasan Akses Internet**

Sistem berbasis web yang bergantung pada konektivitas internet rentan terhadap gangguan jaringan atau koneksi yang lambat, yang dapat mengurangi pengalaman pengguna atau bahkan menyebabkan ketidakmampuan mengakses fitur utama. Untuk mitigasi, solusi berbasis server cadangan atau pengoptimalan komunikasi jaringan dapat diterapkan untuk meminimalkan dampak dari masalah ini.

# BAB III

# PRODUCT DESIGN (PD) (DESAIN PENGEMBANGAN PRODUK)

## 3.1.PENDAHULUAN

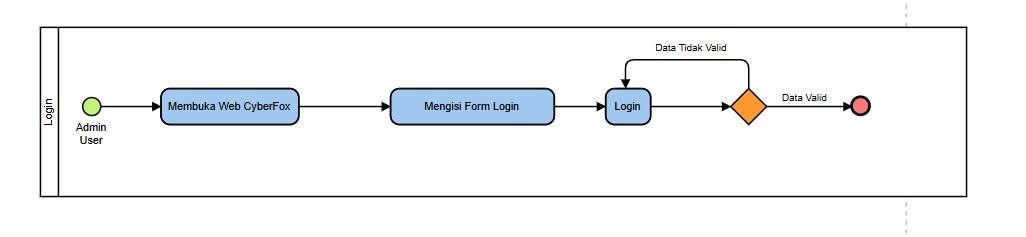
Desain produk merupakan tahap penting yang menjembatani antara kebutuhan pengguna (user requirement) dan implementasi teknis sistem. Pada tahap ini, seluruh masukan dari pengguna dianalisis dan diterjemahkan ke dalam bentuk rancangan yang dapat dipahami oleh tim pengembang. Tujuan utama dari perancangan produk ini adalah untuk menghasilkan desain sistem yang fungsional, efisien, dan sesuai dengan kebutuhan yang telah diidentifikasi sebelumnya. Desain yang baik akan membantu mempercepat proses pengembangan serta memastikan bahwa solusi yang dibangun mampu menyelesaikan permasalahan pengguna secara efektif.

Pendekatan desain yang digunakan dalam proyek ini menekankan pada prinsip usercentered design, yaitu dengan menempatkan kebutuhan dan kenyamanan pengguna sebagai prioritas utama. Hal ini mencakup pemilihan antarmuka yang intuitif, navigasi yang mudah dipahami, serta struktur sistem yang memudahkan pengguna dalam menjalankan fungsi-fungsi utama. Tidak hanya fokus pada pengguna akhir, perancangan juga mempertimbangkan aspek pemeliharaan oleh pengelola sistem di masa depan agar sistem mudah diperbarui dan dikelola tanpa kompleksitas yang berlebihan.

Dengan desain produk yang matang dan terstruktur, diharapkan implementasi sistem dapat berjalan dengan lebih terarah dan efisien. Risiko kesalahan dalam proses pengembangan pun dapat diminimalisir karena adanya acuan desain yang jelas dan terdokumentasi dengan baik. Selain itu, desain yang baik juga memberikan fondasi yang kuat untuk pengujian dan evaluasi sistem, sehingga setiap fitur yang diimplementasikan dapat divalidasi kesesuaiannya terhadap kebutuhan pengguna secara menyeluruh.

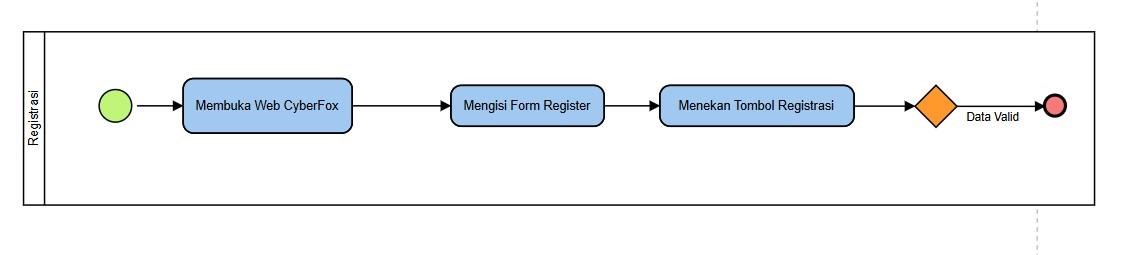
## 3.2. DESKRIPSI PRODUK DESIGN

### 3.2.1. Proses Bisnis Fungsi Login



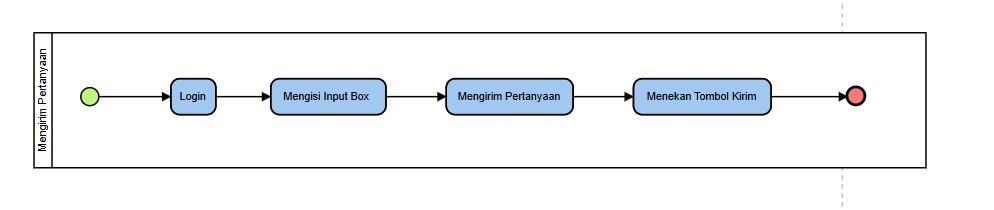
Gambar 5 Proses Bisnis Fungsi Login

### 3.2.2. Proses Bisnis Fungsi Register



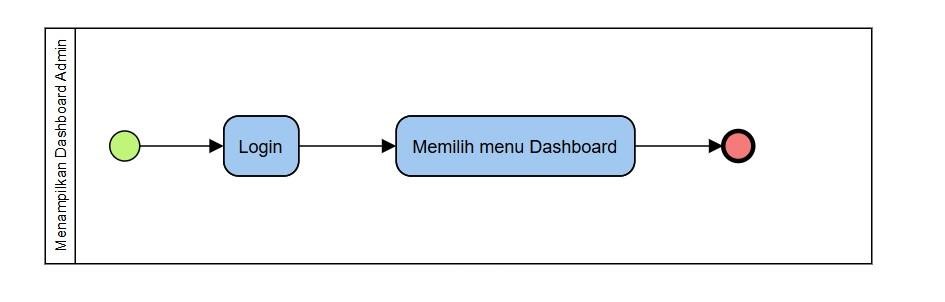
Gambar 6 Proses Bisnis Fungsi Register

### 3.2.3. Proses Bisnis Fungsi Mengirimkan Pertanyaan



Gambar 7 Proses Bisnis Fungsi Mengirimkan Pertanyaan

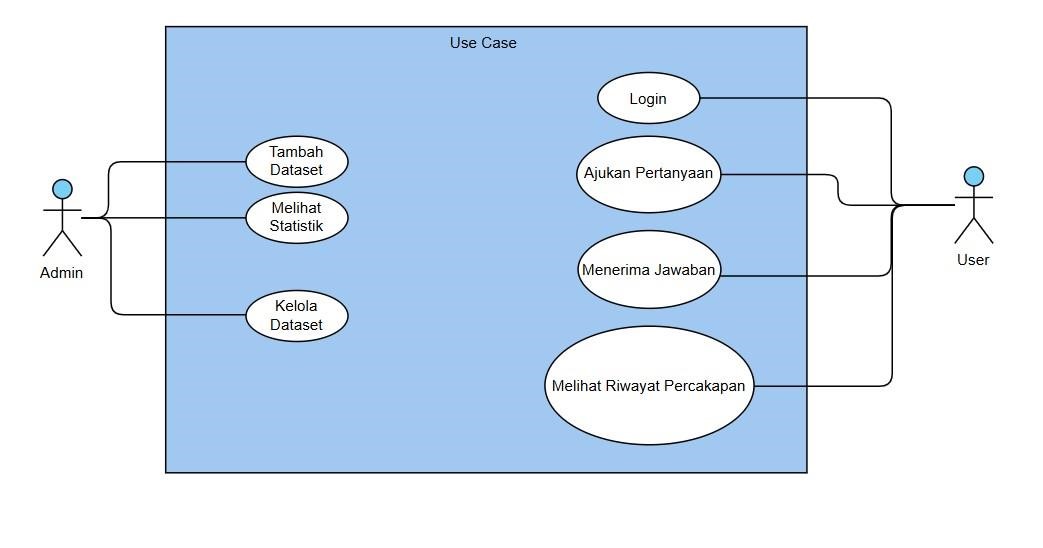
### 3.2.4. Proses Bisnis Fungsi Menampilkan Dashboard Admin



Gambar 8 Proses Bisnis Fungsi Menampilkan Dashboard Admin

### 

### 3.2.5. Use Case Diagram



Gambar 9 Use Case Diagram

### 3.2.6. User Characteristic

Karakteristik user terdiri dari Admin, User, Developer dapat dilihat pada tabel berikut.

Gambar 10 user characteristic

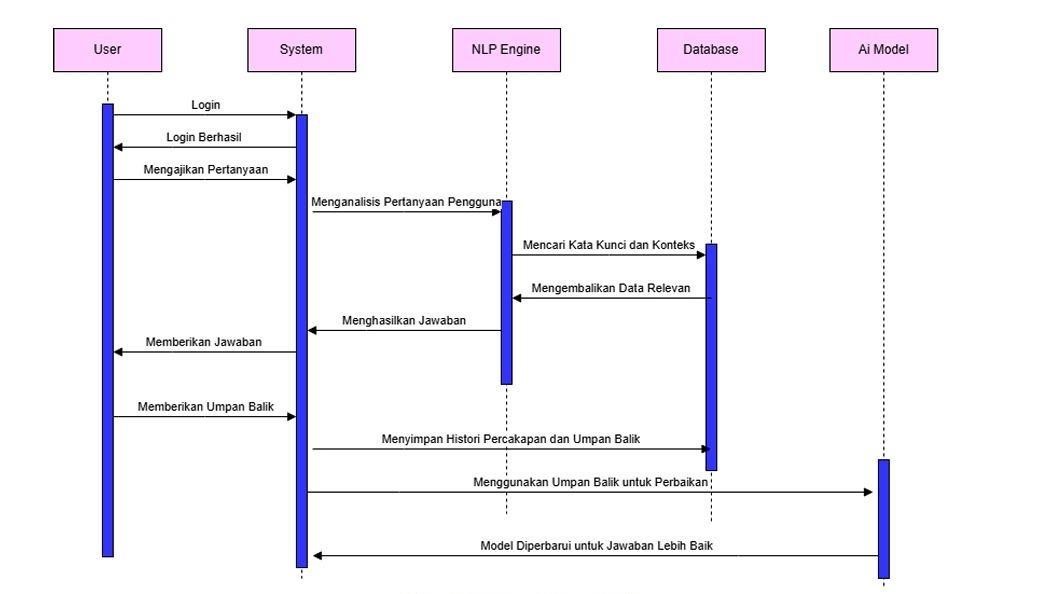
|  |  |  |
| --- | --- | --- |
| **User Group / Role** | **Kepentingan Akses** | **Hak Akses** |
| Admin Sistem | Memantau dan mengelola  keseluruhan sistem | * Akses penuh ke backend * Kelola pengguna * Hapus/edit data * Lihat laporan sistem |
| User/Pengguna Umum | Mengakses fitur utama untuk mendapatkan layanan  informasi atau interaksi | * Akses ke fitur frontend * Input data/form * Lihat hasil atau tanggapan |
| Developer | Mengembangkan, memperbaiki, dan mengelola sistem teknis | * Akses ke kode sumber * Debugging & maintenance * Pengujian fitur baru * Penambahan Dataset |

### 3.2.7. Sequence Diagram

Sequence diagram adalah diagram yang digunakan untuk menggambarkan interaksi antar objek dalam sistem dengan adanya urutan skenario atau langkah-langkah. Pada bagian ini akan dilampirkan sequence diagram yang akan menjelaskan setiap aliran aktivitas fungsi-fungsi yang ada dalam pengembangan chatbot CyberFox.

### 3.2.8. Sequence Diagram System

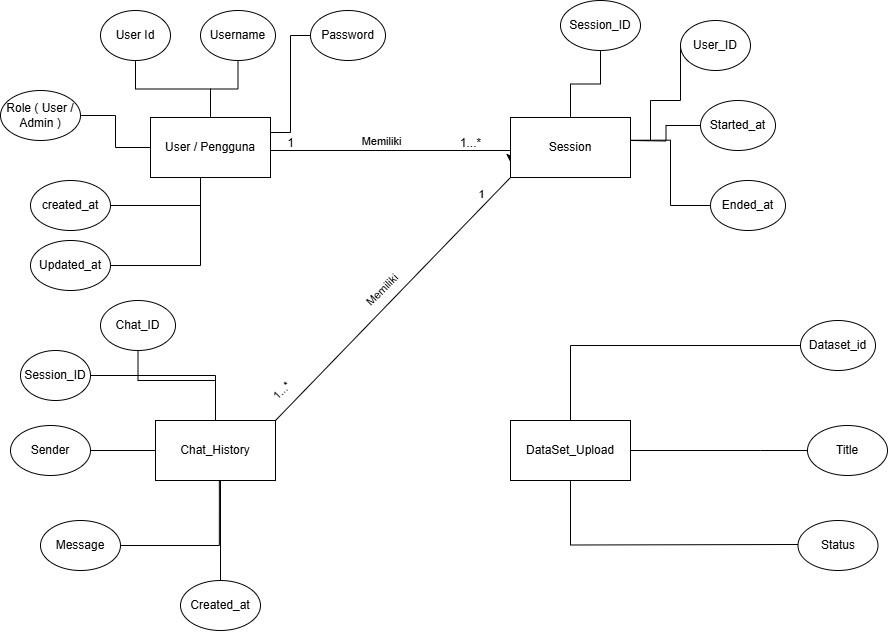
Proses login dimulai ketika pengguna mengisi formulir login dengan username dan password. Sistem frontend mengirimkan permintaan otentikasi ke backend server. Backend kemudian memvalidasi kredensial pengguna dengan mencocokkannya ke data dalam basis data. Jika kredensial valid, server mengirimkan token atau session ID sebagai bukti otentikasi berhasil, lalu mengarahkan pengguna ke halaman dashboard. Jika tidak valid, pengguna akan menerima pesan kesalahan dan diminta mengulangi login.



Gambar 11 Proses Bisnis Fungsi Mengirimkan Pertanyaan

### 3.2.9. Entity Relationship Diagram (ERD)

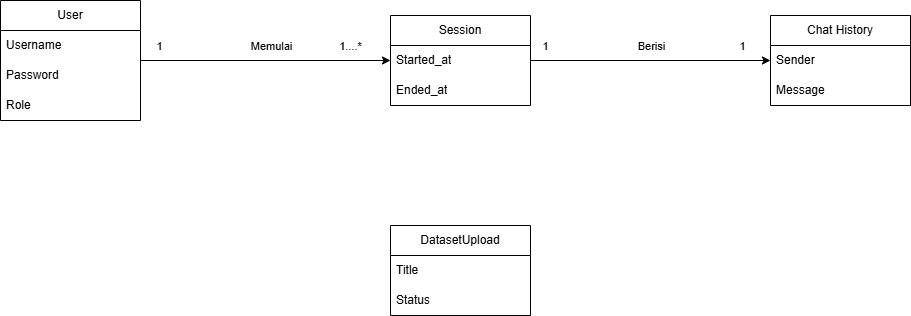
Entity Relationship Diagram (ERD) menggambarkan struktur relasional antara entitas dalam sistem yang dikembangkan. Diagram ini membantu dalam merancang database dengan memperlihatkan hubungan antar tabel, kunci primer, dan kunci asing, serta bagaimana data saling terhubung. Sistem ini terdiri atas empat entitas utama, yaitu: users, session, chat\_history, dan dataset\_upload.



Gambar 12 Sequence Diagram CyberFox

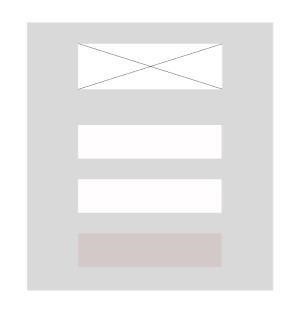
### 3.2.10 Conceptual Data Model (CDM)

Gambar berikut menggambarkan model data konseptual dari sistem CyberFox. Model ini terdiri dari empat entitas utama, yaitu User, Session, Chat History, dan Dataset, yang saling berelasi berdasarkan peran dan aktivitas dalam sistem.



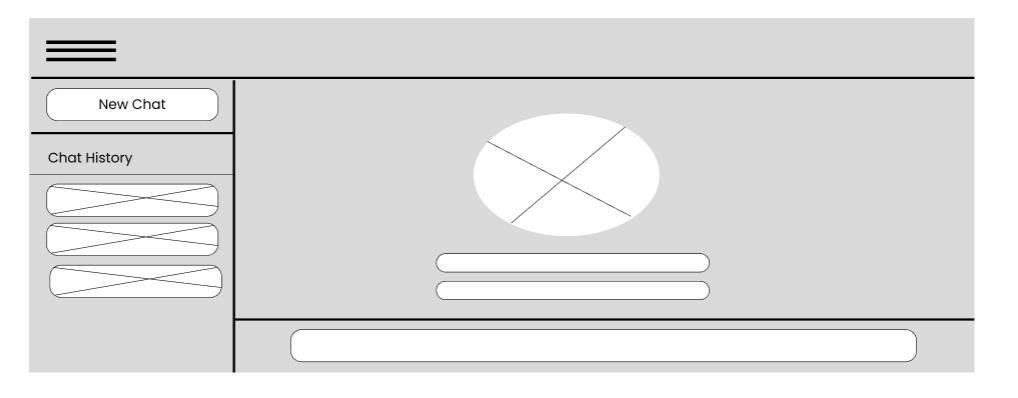
Gambar 13 Conceptual Data Model (CDM)

### 3.2.11 WireFrame Halaman Login



Gambar 14 WireFrame Halaman Login

### 3.2.12. Wireframe Halaman Chatbot

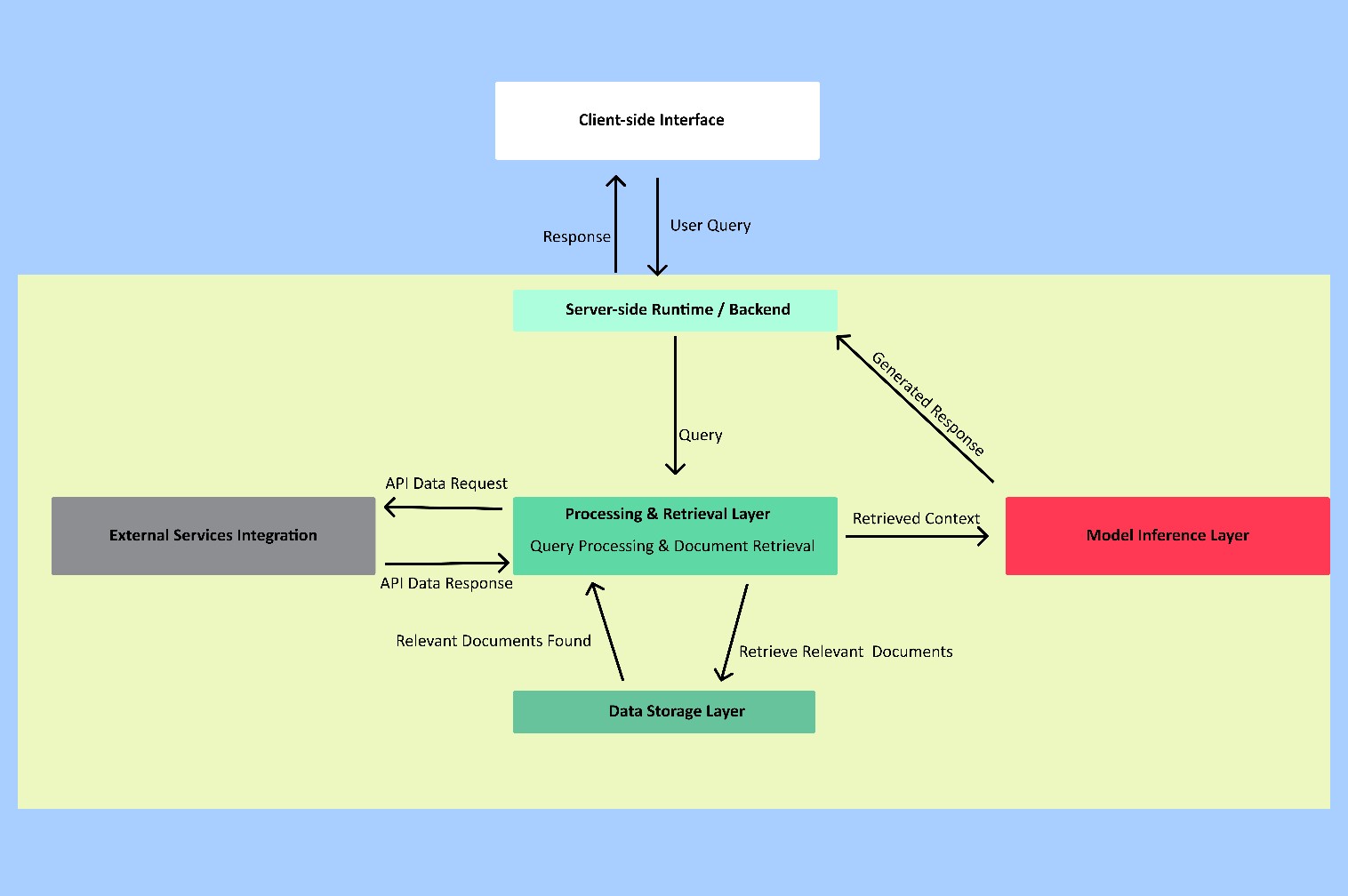


Gambar 15 WireFrame Halaman Login

### 3.2.13. High-Level Architecture (HLA)

Full Desain dapat Dilihat pada link berikut :

[https://www.figma.com/design/ANIfjtRT3EIbgm7bBwcLNG/Cyber-Guardian?nodeid=01](https://www.figma.com/design/ANIfjtRT3EIbgm7bBwcLNG/Cyber-Guardian?node-id=0)&t=OxeyFk0gJnRRouDv-1



Gambar 16 High-Level Architecture (HLA)

1. **User Query Handling (Client-Side Interface - React Vite)** 
   1. Pengguna memasukkan pertanyaan melalui antarmuka frontend yang dibangun menggunakan React Vite.
   2. Query ini kemudian dikirim ke server-side runtime (backend) untuk diproses lebih lanjut.
   3. Setelah respons dihasilkan oleh sistem, frontend akan menampilkannya kembali kepada pengguna.
2. **Query Routing (Backend - Node.js)** 
   1. **Backend** bertindak sebagai perantara yang meneruskan query dari pengguna ke Processing & Retrieval Layer.
   2. Setelah query diterima, backend mengirimkan permintaan analisis query ke Processing & Retrieval Layer.
   3. Setelah respons akhir dari Model Inference Layer dikembalikan, backend mengirimkan hasilnya kembali ke frontend untuk ditampilkan kepada pengguna.
3. **Query Analysis & Retrieval (Processing & Retrieval - LangChain)** 
   1. Query yang diterima akan dianalisis dan diubah menjadi vector embedding menggunakan model embedding yang didukung oleh LangChain (misalnya OpenAI, HuggingFace, dll).
   2. Setelah embedding query dibuat, sistem melakukan pencarian kesamaan vektor (vector similarity search) menggunakan Pinecone untuk menemukan dokumen yang paling relevan.
   3. Metadata dari dokumen hasil pencarian dapat diambil dari PostgreSQL, sementara isi semantik berasal dari hasil pencarian vektor di Pinecone.
   4. Jika diperlukan, sistem dapat menggunakan LangChain tools atau agents untuk mengambil informasi tambahan dari layanan eksternal (API, tools) guna memperkaya konteks jawaban.
   5. Setelah dokumen dan konteks yang relevan dikumpulkan, semuanya dikirim ke Model Inference Layer (misalnya GPT-4) untuk digunakan dalam proses pembuatan jawaban yang kontekstual dan akurat.
4. **Response Generation (Model Inference - OpenAI GPT-4)** 
   1. Model OpenAI GPT-4 menerima query pengguna dan konteks dari dokumen yang telah ditemukan.
   2. Jika ada tambahan informasi dari External Services, data tersebut juga dikombinasikan dalam proses ini.
   3. Model menghasilkan respons berdasarkan semua input yang diberikan.
   4. Respons akhir dikirim kembali ke backend untuk diteruskan ke frontend pengguna.

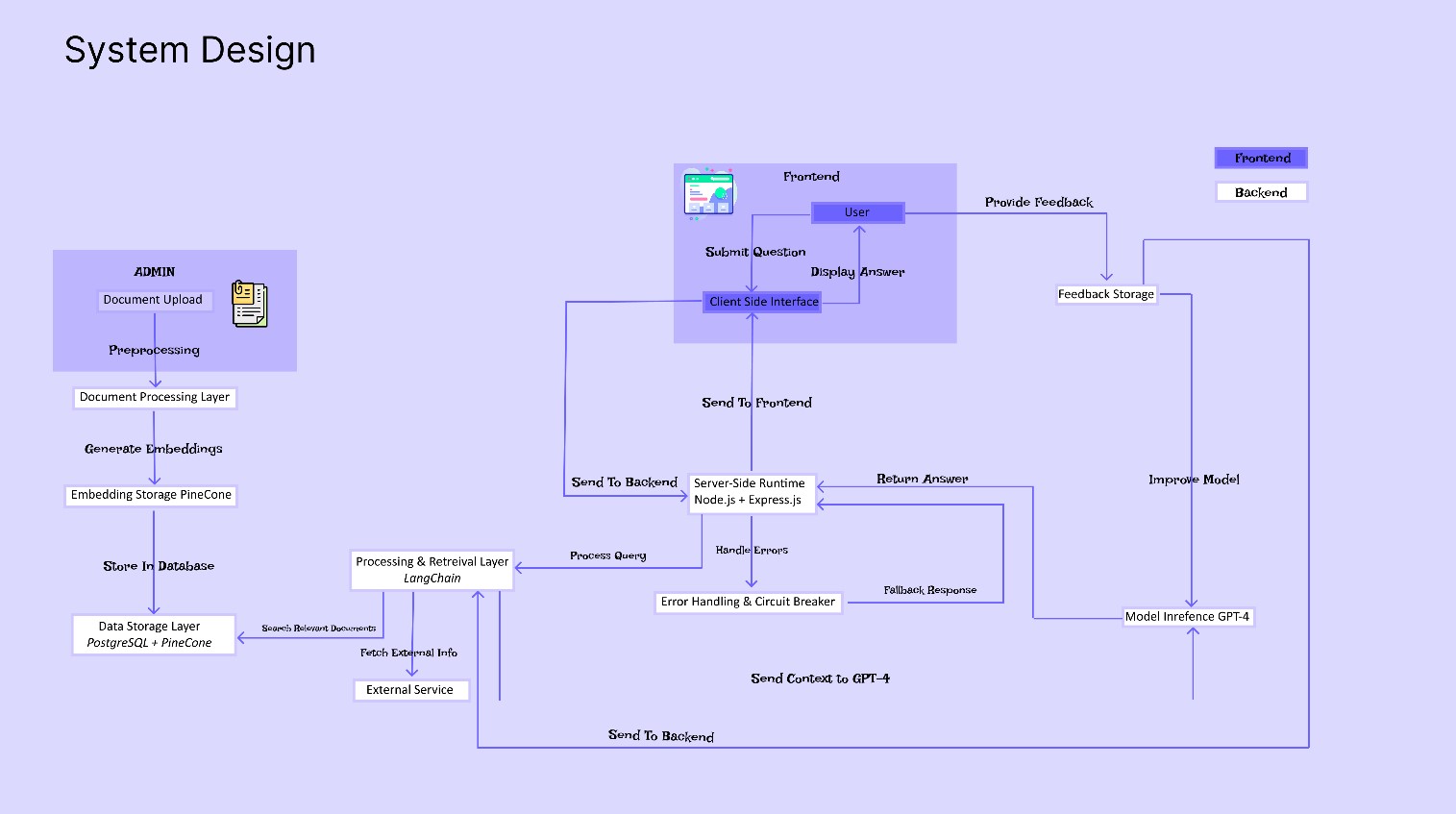
1. **Vector Storage (Data Storage - PostgreSQL + Pinecone)** 
   1. Data Storage Layer menggunakan Pinecone sebagai tempat penyimpanan embedding dokumen dalam bentuk vektor.
   2. Setiap kali ada query dari pengguna, sistem melakukan pencarian berbasis vector similarity search di Pinecone untuk menemukan dokumen yang paling relevan secara semantik.
   3. Setelah dokumen relevan ditemukan, hasil pencarian dikirimkan kembali ke Processing & Retrieval Layer untuk digunakan dalam proses pembuatan respons oleh model LLM.
2. **External Data (Opsional - API/Tools)** 
   1. Jika informasi tambahan dari sumber eksternal diperlukan, Processing & Retrieval Layer akan membuat permintaan API ke layanan pihak ketiga seperti database eksternal atau alat AI lainnya.
   2. Data yang diperoleh akan dikombinasikan dengan dokumen yang telah ditemukan untuk memperkaya jawaban yang dihasilkan oleh model.

1. **Document Processing (Document Ingestion - Preprocessing & Storage)**

Sistem memiliki proses terpisah untuk memasukkan dokumen baru ke dalam Data Storage Layer.

* 1. Dokumen yang dimasukkan akan melalui tahap preprocessing, seperti:
     1. Splitting text (memecah dokumen menjadi bagian kecil)
     2. Embedding generation (mengubah teks menjadi vektor menggunakan model embedding dari Deepset.ai)
  2. Setelah proses ini selesai, embedding dokumen akan disimpan dalam PostgreSQL + PgVector, sehingga siap digunakan dalam pencarian saat ada query dari pengguna.

###### 3.2.14. System Design



Gambar 17 System Design

CyberGuardian adalah sistem edukatif berbasis AI yang dirancang untuk membantu anak-anak memahami keamanan siber secara interaktif dan mudah dipahami. Pengguna memasukkan pertanyaan melalui antarmuka React Vite, yang kemudian dikirim ke backend berbasis Node.js + Express.js untuk diproses lebih lanjut.

Pertanyaan pengguna dapat dimodifikasi terlebih dahulu oleh Standalone Question Generator, lalu dikonversi menjadi embeddings. Proses pencarian dokumen relevan dilakukan menggunakan

LangChain, yang memanfaatkan vector similarity search dengan Pinecone sebagai vector store dan PostgreSQL sebagai penyimpan metadata dokumen.

Setelah dokumen yang relevan ditemukan, Context Builder menyusun informasi penting dari hasil pencarian tersebut. Informasi ini kemudian dikirim ke model GPT-4 untuk menghasilkan jawaban yang kontekstual, sesuai dengan kebutuhan anak-anak.

Jika terjadi kegagalan dalam pemrosesan, sistem akan memanfaatkan Error Handling & Circuit Breaker untuk mengaktifkan respons fallback agar pengalaman pengguna tetap lancar. Selain itu, LangChain juga dapat mengambil informasi tambahan dari layanan eksternal (External Services Integration) untuk memperkaya konteks jawaban.

Jawaban yang telah dihasilkan akan dikirimkan kembali ke antarmuka pengguna melalui React Vite, memastikan pengalaman belajar yang cepat dan responsif.

Untuk mendukung peningkatan performa, CyberGuardian dilengkapi dengan mekanisme Feedback Storage. Umpan balik dari pengguna dikumpulkan dan dianalisis untuk meningkatkan akurasi pencarian dan pemahaman model terhadap pertanyaan di masa mendatang.

Sistem juga mendukung proses unggah dokumen baru oleh admin. Dokumen tersebut diproses melalui Document Processing Layer, diubah menjadi embeddings, dan disimpan ke dalam Pinecone serta PostgreSQL, sehingga terus memperkaya basis pengetahuan sistem.

Dengan arsitektur yang fleksibel dan modern ini, CyberGuardian tidak hanya memberikan jawaban yang informatif tetapi juga adaptif, memastikan anak-anak mendapatkan edukasi keamanan siber yang aman, menyenangkan, dan terus berkembang.

**Pemetaan HLA → System Design**

Gambar 18 System Design

|  |  |  |  |
| --- | --- | --- | --- |
| **HLA Kompone** | **n** | **System Design Komponen** | **Penjelasan** |
| Client-side Interface |  | Client-Side Interface (React Vite) | Tempat user berinteraksi: submit  query, melihat jawaban, dan memberikan feedback. |
| Server-side  Runtime  Backend | / | Server-Side Runtime (Node.js + Express.js) | Menerima permintaan dari frontend dan mengoordinasikan semua proses backend. |
| Processing &  Retrieval Layer | | Processing & Retrieval Layer  (LangChain) | Bertanggung jawab memproses query user, mengambil dokumen dari storage atau external services. |
| Model Inference Layer | | Model Inference (GPT-4) | GPT-4 melakukan inferensi berdasarkan konteks yang sudah diambil. |
| Data Storage  Layer | | Data Storage Layer (PostgreSQL + PineCone) | Tempat penyimpanan dokumen dan hasil embedding dari dokumen. |

**Kebutuhan Teknis :**

Tabel 11 Kebutuhan Teknis

|  |  |  |
| --- | --- | --- |
| **Komponen** | **Fungsi** | **Teknologi yang digunakan** |
| Client-Side  Interface | Tempat pengguna memasukkan pertanyaan | React Vite, HTML, CSS, JavaScript |
| Backend  Processing | Meneruskan query pengguna  ke proses retrieval | Node.js (Express.js, Nest.js) |
| Processing &  Retrieval | Menganalisis query, membuat embedding, dan mencari  dokumen relevan | Deepset.ai (Haystack), OpenAI Embeddings |
| Model Inference  Layer | Menghasilkan jawaban  berbasis konteks dokumen | OpenAI GPT-4 |
| Data Storage Laye | Menyimpan embedding  dokumen dan metadata | PostgreSQL + PineCone |
| Document  Ingestion Layer | Memproses dokumen baru dan menyimpannya dalam storage | Node.js, LangChain, OpenAI Embeddings |
| External Services  (Opsional) | Mengambil data dari sumber  eksternal jika diperlukan | API Eksternal (misalnya Wikipedia,  WolframAlpha, atau layanan data lainnya) |

**OpenAI API**

* **Fungsi:**
  1. Membuat embeddings untuk mengubah teks menjadi representasi vektor angka.
  2. Menjalankan model LLM (Large Language Model) untuk menghasilkan respons berbasis konteks.
* **Cara Kerja:**
  1. Dokumen diubah menjadi embeddings dan disimpan di PostgreSQL dengan PgVector.
  2. Pertanyaan pengguna diubah menjadi embeddings dan dibandingkan dengan data di database menggunakan vector similarity search.
  3. Model GPT-4 memberikan jawaban berdasarkan hasil pencarian vektor.
* **Alasan Pemilihan:**
  1. Akurasi tinggi dibandingkan model lain.
  2. Tidak memerlukan pelatihan tambahan, langsung siap digunakan.
  3. Mudah diintegrasikan dengan JavaScript dan Node.js.

**LangChain**

* **Fungsi:**
  1. Mengubah pertanyaan pengguna menjadi *vector embeddings* menggunakan model seperti OpenAI, HuggingFace, atau Cohere.
  2. Melakukan pencarian dokumen relevan menggunakan teknik Retrieval-Augmented Generation (RAG).
  3. Mengatur alur kerja (pipeline) antara retriever, LLM, dan output secara modular.
* **Cara Kerja:**
  1. Query dari pengguna diubah menjadi embeddings.
  2. Embeddings dibandingkan dengan embeddings dokumen di vector database (misalnya pgvector, Chroma, Pinecone, dll).
  3. Dokumen relevan di-*retrieve* dan dikombinasikan ke dalam *context* yang dikirim ke LLM (misalnya GPT-4).
  4. LangChain *chain* akan menggabungkan semua proses ini dan mengembalikan jawaban ke pengguna.
* **Alasan Pemilihan:**
  1. Lebih fleksibel dibandingkan LangChain karena dapat digunakan dengan berbagai model embeddings dan vector database.
  2. Open-source dan mudah dikustomisasi sesuai kebutuhan.
  3. Lebih modular dan fleksibel dibandingkan Haystack, dengan banyak *components* yang bisa diganti-ganti sesuai kebutuhan (retriever, LLM, prompt, memory, tools, agent).
  4. Mendukung banyak *vector store*, *LLM providers*, dan *data sources*.
  5. Komunitas aktif dan dokumentasi lengkap.
  6. Mendukung integrasi cepat dengan frontend/React maupun backend/Node.js menggunakan LangChain.js.

**PostgreSQL dengan Pinecone**

* **Fungsi:**
  1. Mengelola dan menyimpan metadata dokumen (seperti judul, penulis, tanggal, topik) di PostgreSQL.
  2. Menyimpan embeddings dokumen dan melakukan pencarian berbasis vektor menggunakan Pinecone.
* **Cara Kerja:**
  1. Dokumen yang dimasukkan ke dalam sistem diproses menjadi embeddings menggunakan model embedding (seperti OpenAI, HuggingFace, dll).
  2. Embeddings dikirim dan disimpan di Pinecone sebagai vektor untuk keperluan pencarian semantik.
  3. Ketika pengguna mengajukan pertanyaan, sistem mengubah pertanyaan menjadi embeddings dan mengirimkannya ke Pinecone untuk menemukan dokumen paling relevan berdasarkan vector similarity search.
  4. Metadata dari dokumen relevan diambil dari PostgreSQL untuk memperkaya hasil pencarian.
* **Alasan Pemilihan:**
  1. Pinecone dirancang khusus untuk pencarian vektor dalam skala besar, dengan performa tinggi dan latensi rendah.
  2. Memberikan fleksibilitas dalam skenario multi-tenant dan real-time search.
  3. Pemisahan antara penyimpanan embeddings (di Pinecone) dan metadata terstruktur (di PostgreSQL) membuat sistem lebih efisien dan mudah diatur.
  4. Mendukung integrasi langsung dengan LangChain dan model LLM seperti GPT, cocok untuk aplikasi Retrieval-Augmented Generation (RAG).

**React Vite**

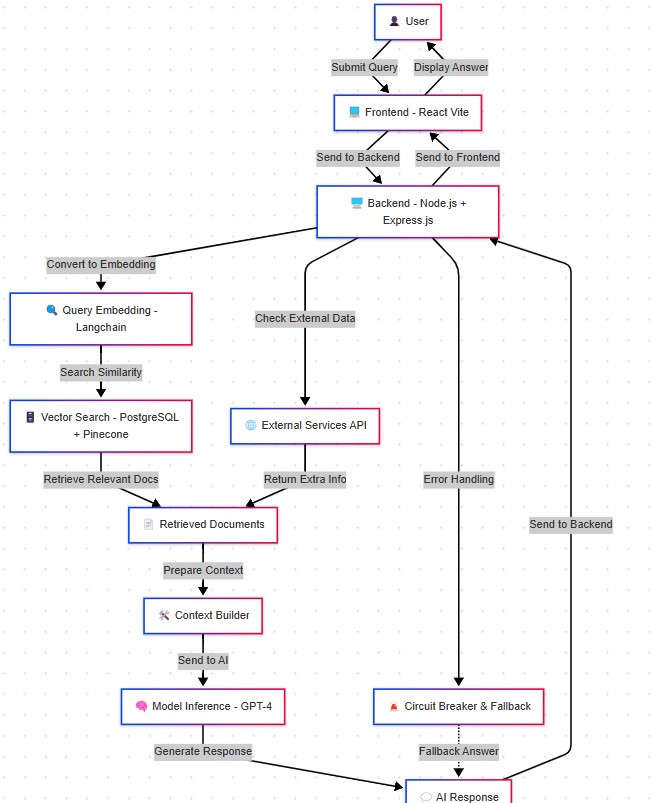
* **Fungsi:**
  1. Menyediakan antarmuka pengguna untuk mengajukan pertanyaan dan melihat jawaban chatbot.
* **Cara Kerja:**
  1. Pengguna memasukkan pertanyaan ke dalam aplikasi.
  2. Pertanyaan dikirim ke backend melalui API.
  3. Jawaban dari model inference layer ditampilkan kepada pengguna dalam format yang mudah dibaca.
* **Alasan Pemilihan:**
  1. Lebih cepat dan ringan dibandingkan React tradisional.
  2. Waktu build lebih singkat dengan performa lebih baik.
  3. Mendukung hot module replacement untuk pengembangan yang lebih cepat.

**Node.js**

* **Fungsi:**
  1. Menjalankan backend untuk menangani permintaan dari client dan mengelola komunikasi dengan layanan eksternal.
* **Cara Kerja:**
  1. Server menerima pertanyaan dari client.
  2. Query diteruskan ke processing dan retrieval layer.
  3. Hasil dari model inference layer dikirim kembali ke client melalui API.

* **Alasan Pemilihan:**
  1. Cepat dan efisien dalam menangani permintaan asynchronous.
  2. Ekosistem besar dengan banyak pustaka pendukung.
  3. Mudah diintegrasikan dengan berbagai layanan cloud dan database.

**Query Analysis & Retrieval (Processing & Retrieval - Langchain)**



Gambar 19 Diagram Query Analysis & Retrieval

**Penjelasan :**

**Query Analysis & Retrieval (Processing & Retrieval - LangChain)**

* 1. Query yang diterima dari pengguna akan dianalisis dan dikonversi menjadi vector embeddings menggunakan model embedding (misalnya OpenAI, HuggingFace, atau lainnya) melalui pipeline LangChain.
  2. Setelah embedding query dibuat, sistem menggunakan Pinecone untuk melakukan pencarian kesamaan vektor (vector similarity search) guna menemukan dokumen yang paling relevan secara semantik.
  3. Metadata dari dokumen relevan tersebut akan diambil dari PostgreSQL, untuk memberikan konteks tambahan yang bersifat terstruktur (seperti sumber, tanggal, penulis).
  4. Jika diperlukan, sistem dapat melakukan panggilan ke External Services (seperti API atau tools khusus) menggunakan LangChain Tools atau LangChain Agents untuk memperkaya konteks jawaban.
  5. Setelah informasi yang relevan dikumpulkan, dokumen dan data tambahan tersebut akan dikirim ke Model Inference Layer (misalnya GPT-4) untuk menghasilkan jawaban akhir yang kontekstual dan akurat.

### 3.2.15 Database Schema

**Database Schema – CyberFox**

1. **sessions (Menyimpan sesi percakapan Chatbot)**

Tabel 12 1. sessions (Menyimpan sesi percakapan Chatbot)

|  |  |  |
| --- | --- | --- |
| Nama Kolom | Tipe Data | Keterangan |
| id | UUID (PK) | ID unik sesi |
| session\_token | VARCHAR (UNIQUE) | Token unik sesi |
| created\_at | TIMESTAMP | Waktu pembuatan sesi |

1. **messages ( Menyimpan pesan chatbot )**

Tabel 13 1. messages ( Menyimpan pesan chatbot )

|  |  |  |
| --- | --- | --- |
| Nama Kolom | Tipe Data | Keterangan |
| id | UUID (PK) | ID unik pesan |
| session\_id | UUID (FK -> sessions.id) | ID sesi percakapan |
| sender | ENUM("user", "bot") | Pengirim pesan |
| message | TEXT | Isi pesan |
| created\_at | TIMESTAMP | Waktu pesan dikirim |

1. **intents ( Menyimpan intent chatbot )**

Tabel 14 3. intents ( Menyimpan intent chatbot )

|  |  |  |
| --- | --- | --- |
| Nama Kolom | Tipe Data | Keterangan |
| id | UUID (PK) | ID unik intent |
| name | VARCHAR (UNIQUE) | Nama intent |
| description | TEXT | Deskripsi intent |

1. **responses (Menyimpan respons chatbot)**

Tabel 15 4. responses (Menyimpan respons chatbot)

|  |  |  |
| --- | --- | --- |
| Nama Kolom | Tipe Data | Keterangan |
| id | UUID (PK) | ID unik respons |
| intent\_id | UUID (FK -> intents.id) | ID intent yang terkait |
| response\_text | TEXT | Teks respons chatbot |

1. **logs (Menyimpan aktivitas sistem)**

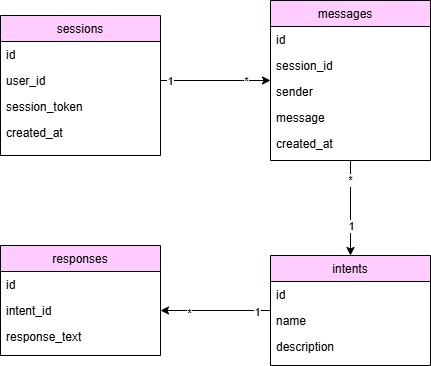
Tabel 16 5. logs (Menyimpan aktivitas sistem)

|  |  |  |
| --- | --- | --- |
| Nama Kolom | Tipe Data | Keterangan |
| id | UUID (PK) | ID unik log |
| action | TEXT | Aksi yang dilakukan |
| timestamp | TIMESTAMP | Waktu kejadian |

**Catatan:**

* 1. **PK (Primary Key)**: Kunci utama, memastikan setiap nilai unik.
  2. **FK (Foreign Key)**: Kunci asing, menunjukkan relasi antar tabel.
  3. **ENUM** digunakan untuk memastikan data hanya memiliki nilai yang valid.
  4. **logs** bersifat independen dan tidak terhubung langsung ke tabel lain.

**Diagram ERD**



Gambar 20 Diagram ERD

**Relasi Antar Tabel**

* 1. **sessions** ↔ **messages** (One-to-Many): Setiap sesi memiliki banyak pesan.
  2. **messages** ↔ **intents** (Many-to-One): Setiap pesan dapat dikenali sebagai satu intent.
  3. **intents** ↔ **responses** (One-to-Many): Satu intent dapat memiliki beberapa respons.

**Proses Penyimpanan Data**

- Alur Kerja

* + - Pengguna mengirim pesan ke chatbot melalui frontend (React

Vite).

* + - Server menerima pesan, lalu menyimpannya ke dalam database dengan status sender = 'user'.
    - Chatbot memproses pesan menggunakan Dialogflow dan menghasilkan balasan.
    - Balasan chatbot disimpan dalam database dengan status sender

= 'bot'.

* + - Chatbot mengirimkan respons ke pengguna melalui frontend.

## 3.2 Modifikasi RAG Menggunakan Langchain untuk Proyek CyberFox

### 3.2.1 Tujuan Modifikasi

Tujuan utama dari modifikasi ini adalah:

* Menyesuaikan pipeline RAG dengan infrastruktur layanan mikro (microservices) CyberFox.
* Memungkinkan pengambilan informasi dari berbagai sumber (dokumen, API, database).
* Mendukung pengalaman interaktif berbasis konteks menggunakan chatbot.
* Menambahkan kontrol terhadap hasil generation untuk konteks edukasi dan keamanan.

###### 3.2.2 Komponen Yang Dimodifikasi

Tabel 17 Komponen Yang Dimodifikasi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Komponen | Deskripsi | |  | | --- | |  |  |  | | --- | | **Modifikasi** | |
| Retriever | Pengambil dokumen relevan dari vektor | Menggunakan FAISS lokal yang diisi dari dokumen internal CyberFox |
| Prompt Template | Template pertanyaan & jawaban | Disesuaikan dengan gaya percakapan edukatif |
| Memory | Menyimpan konteks percakapan | Ditambahkan memory buffer untuk pengalaman chatbot |
| Chain | Pipeline Langchain | Menggunakan ConversationalRetrievalChain yang dimodifikasi |

###### 

# BAB IV

**PRODUCT IMPLEMENTATION (PI) (IMPLEMENTASI**

# PENGEMBANGAN PRODUK)

## 4.1.PENDAHULUAN

Proses implementasi CyberFox mengacu pada rancangan yang telah dijelaskan dalam dokumen desain pengembangan produk. Tujuan dari implementasi ini adalah merealisasikan desain yang telah dirancang ke dalam bentuk system nyata yang dapat dijalankan dan diuji. Implementasi dilakukan secara bertahap dan terstuktur agar setiap bagian dari system dapat berfungsi sesuai dengan kebutuhan yang telah diidentifikasi.

## 4.2.DESKRIPSI

Implementasi produk Cyberfox dilakukan dengan mengikuti prinsip modularitas, skalabilitas dan maintainabilitas, agar sistem mudah dikembangkan dan dikelola. Setiap bagian dari sistem diimplementasikan berdasarkan desain yang telah dibuat.

### 4.2.1. Prinsip Implementasi

Selamat tahap implementasi, proyek CyberFox menerapkan sejumlah prinsip utama guna memastikan proses pengembangan berlangsung secara terstruktur.

1. Pendekatan Metodologis

Pengembangan dilakukan dengan metode Agile Iteratif, di mana fitur utama dibangun dalam siklus sprint singkat. Setiap iterasi memungkinkan evaluasi dan peningkatan berkelanjutan, sehingga kesalahan dapat diperbaiki lebih awal sebelum dilanjutkan ke tahap berikutnya.

1. Fokus pada Modularitas dan Efisiensi

Sistem dirancang menggunakan pendekatan microservices agar setiap komponen (seperti autentikasi, pengelolaan dataset, layanan chatbot, media service) dapat dikembangkan dan dikelola secara terpisah. Hal ini mempercepat proses debugging, deployment, dan integrasi.

1. Penerapan Standar Keamanan

Pengguna diidentifikasi melalui sistem otentikasi berbasis token JWT. Setiap permintaan dikirim melalui protokol aman (HTTPS), dan data sensitif disimpan menggunakan fitur keamanan dari database yang digunakan, seperti enkripsi sisi server di PostgreSQL.

1. Stabilitas dan Ketahanan Sistem

Sistem dirancang untuk tetap dapat berjalan bahkan ketika salah satu service mengalami gangguan. Proses validasi input dan penanganan kesalahan (error handling) disiapkan untuk memastikan sistem tetap tangguh terhadap input tak terduga atau kegagalan eksternal, termasuk jika layanan eksternal seperti Coherre tidak responsif.

1. Standar Pengembangan dan Dokumentasi
   1. Penulisan kode backend mengikuti standar modern JavaScript dan TypeScript, dengan pendekatan modular untuk kemudahan pemeliharaan.
   2. Arsitektur proyek dibangun berdasarkan pemisahan tanggung jawab (separation of concerns), dengan struktur folder yang mendukung keterbacaan dan konsistensi.
   3. Penggunaan Git untuk kontrol versi, disertai strategi branching seperti main, dev, dan feature/\*, serta proses code review melalui pull request.

### 4.2.2. Lingkungan Pengembangan Terintegrasi (IDE)

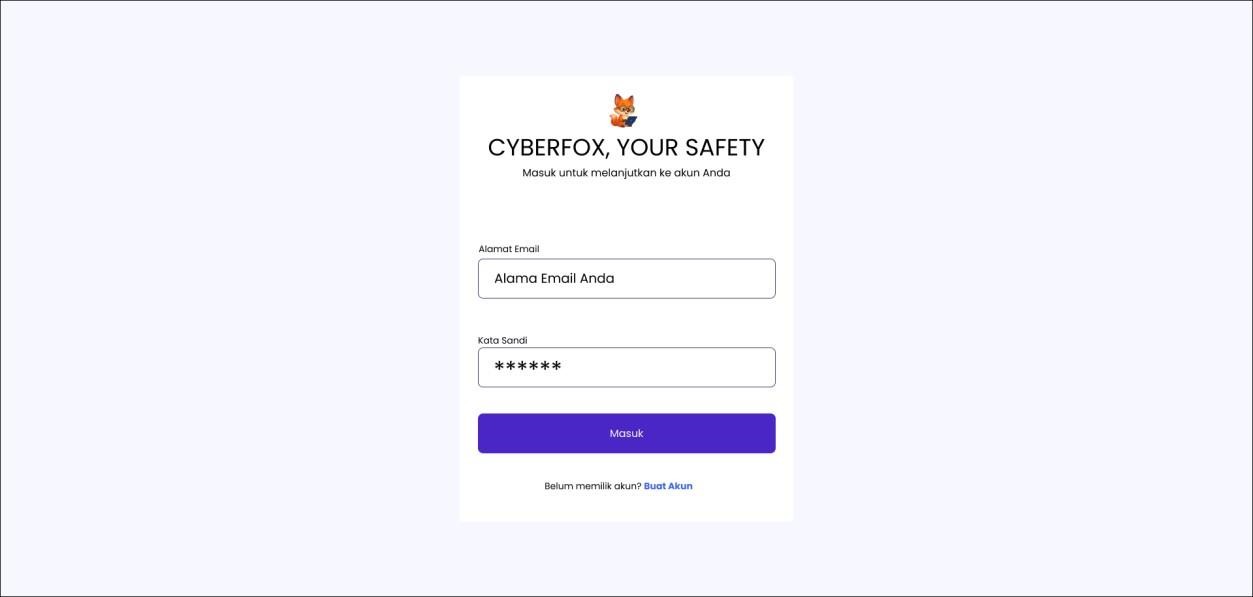
Tabel 18 Lingkungan Pengembangan Terintegrasi (IDE)

|  |  |  |  |
| --- | --- | --- | --- |
| **IDE / Editor / Alat** | **Versi** | **Alasan Penggunaan** | **Fitur yang**  **Dimanfaatkan** |
| Visual Studio Code | v1.89.0 | Rringan, fleksiblek mendukung banyak ekstensi  untuk JS, TypeScript dan  Node.js | Auto-completion, Git integration,  debugging, terminal  built-in |
| Figma | Web-based | Desain UI/UX antarmuka pengguna yang mudah  digunakan dan kolaboratif | Prototyping, layout grid, inspect tools, kolaborasi tim |
| Pinecone DB | v2.0 | Penyimpanan vektor untuk pencarian semantik yang cepat dan skalabel | Vector database untuk AI search, indexing, dan retrieval |
| PostgreSQL | v13.x | Database untuk menyimpan data | SQL query, relasi antar tabel, integrasi dengan backend |

### 4.2.3 Hasil Implementasi

#### 4.2.3.1 Hasil

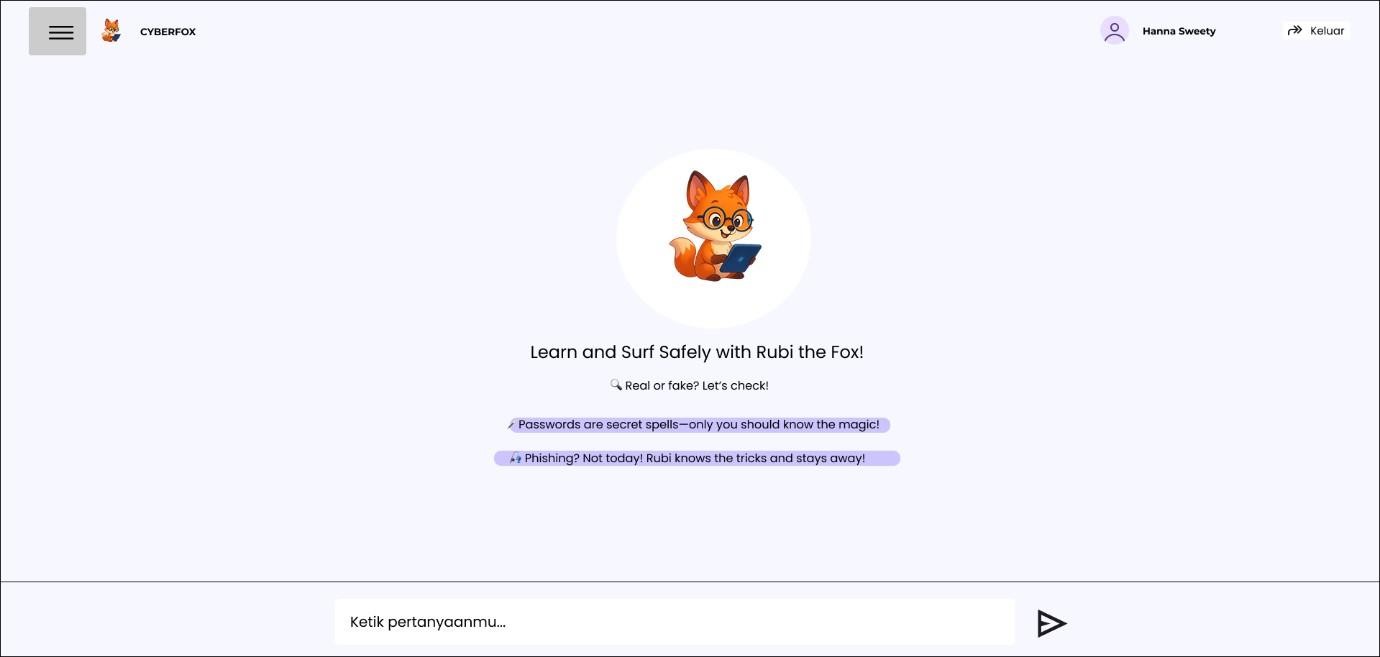
Berikut merupakan halaman untuk pengguna mengakses layanan CyberForx. Halaman ini berfungsi untuk mengautentikasi identitas pengguna sebelum mereka dapat menggunakan fitur – fitur utama.



Gambar 21 Login

#### Halaman Chatbot

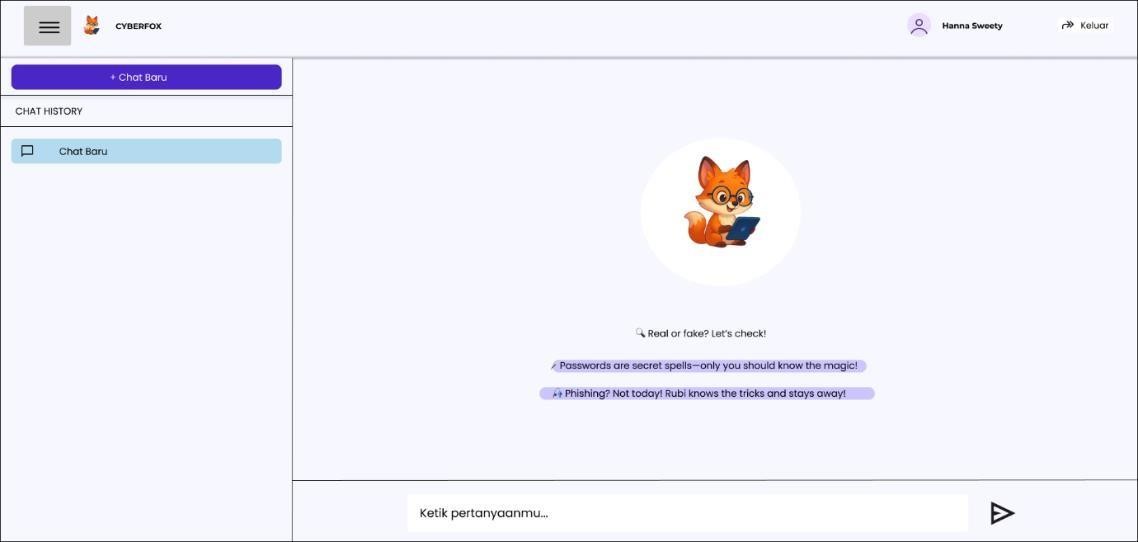
Halaman ini merupakan inti dari layanan CyberFox, yang dirancang sebagai antarmuka interaktif bagi pengguna untuk berkomunikasi secara langsung dengan CyberFox, asisten virtual yang memberikan edukasi dan bantuan terkait keamanan siber.



Gambar 22 Halaman Chatbot

#### Menu Riwayat Chat

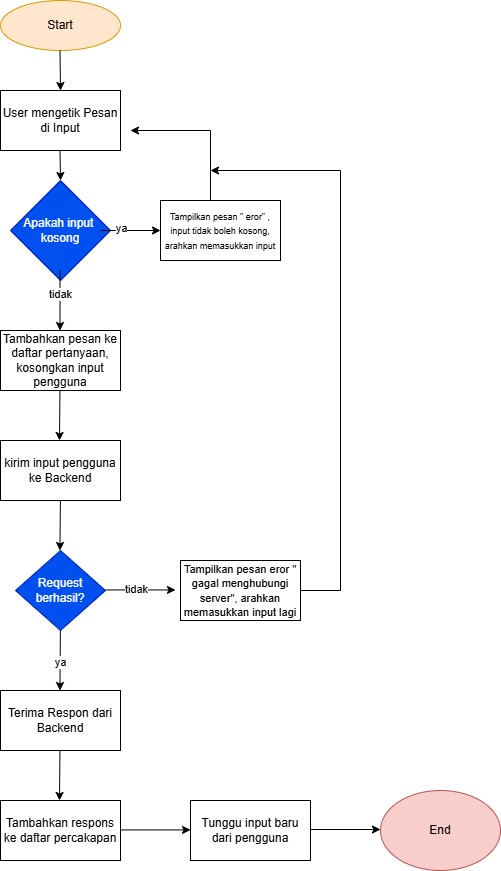
Gambar ini menampilkan antarmuka menu Riwayat Chat yang merupakan bagian dari fitur utama aplikasi CyberFox. Tampilan dirancang dengan pendekatan user-friendly dan minimalis, sehingga memudahkan pengguna untuk melihat kembali percakapan yang pernah dilakukan dengan chatbot.



Gambar 23 Menu Riwayat Chat

#### 4.2.4. Main Function (Fungsi Utama Sistem)

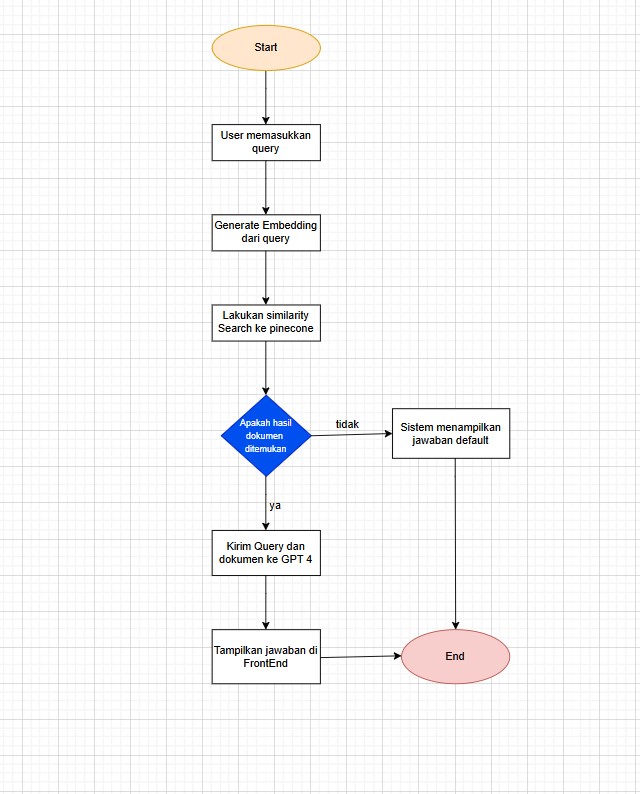
**ChatbotHandler**



Gambar 24 ChatbotHandler

Flowchart ini dimulai ketika pengguna mengetikkan pesan pada kolom input. Sistem kemudian memverifikasi apakah input tersebut kosong. Jika kosong, sistem akan menampilkan pesan kesalahan dan meminta pengguna untuk memasukkan input yang valid. Jika tidak kosong, pesan ditambahkan ke daftar percakapan dan kolom input dikosongkan. Selanjutnya, sistem mengirimkan pesan tersebut ke backend untuk diproses. Jika terjadi kegagalan dalam menghubungi backend, sistem akan menampilkan pesan kesalahan dan meminta pengguna untuk mencoba kembali. Namun, jika permintaan berhasil, sistem akan menerima respons dari backend, menambahkannya ke dalam percakapan, dan siap menunggu input selanjutnya dari pengguna. Alur ini memastikan interaksi berlangsung secara efisien, dengan penanganan kesalahan yang jelas dan pengalaman pengguna yang optimal.

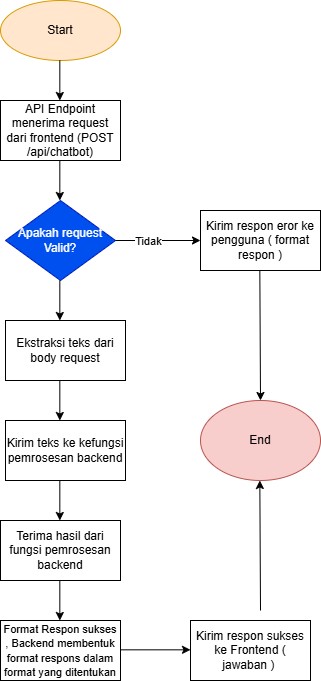
Query Processing



Gambar 25 Query Processing

Alur ini menjelaskan proses kerja sistem ketika pengguna mengirimkan sebuah *query*. Pertama, sistem menerima input dari pengguna, kemudian mengubah *query* tersebut menjadi bentuk *embedding*. Selanjutnya, dilakukan pencocokan kemiripan (*similarity search*) terhadap basis data vektor yang tersimpan menggunakan *PgVector*. Jika ditemukan dokumen yang relevan, sistem akan mengirimkan dokumen beserta *query* ke model GPT-4 untuk menghasilkan jawaban yang lebih tepat. Jawaban tersebut kemudian ditampilkan di antarmuka pengguna (*frontend*). Namun, jika tidak ditemukan dokumen yang sesuai, sistem akan menampilkan jawaban default. Proses ini dirancang untuk mengoptimalkan relevansi respons berdasarkan pengetahuan yang tersedia dalam basis data.

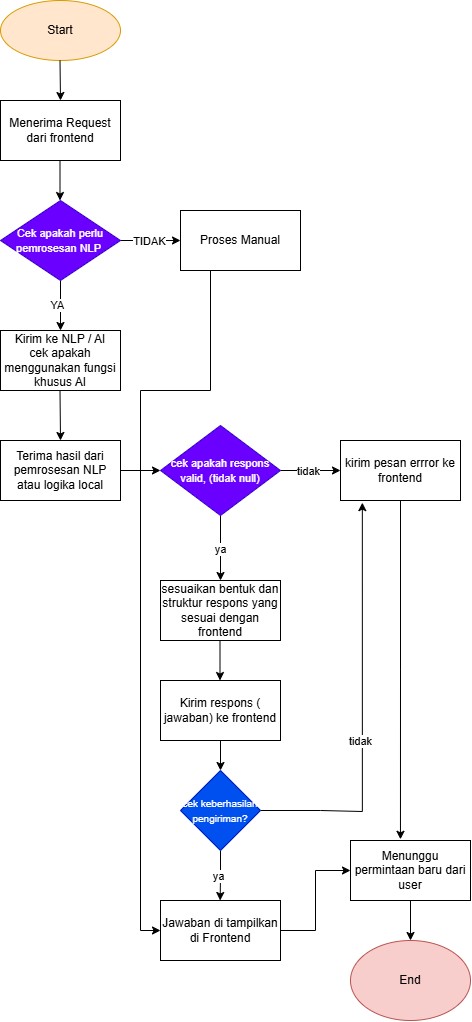
**HandleChatbotInteraction, processChatbotRequestFull**



Gambar 26 HandleChatbotInteraction, processChatbotRequestFull

Flowchart ini menjelaskan alur pemrosesan permintaan dari frontend ke backend melalui API endpoint. Proses dimulai saat sistem menerima request dari frontend melalui metode POST pada endpoint /api/chatbot. Sistem kemudian memvalidasi request tersebut. Jika tidak valid, sistem langsung mengirimkan respon error kepada pengguna dalam format yang telah ditentukan. Jika request valid, sistem mengekstrak teks dari body request dan meneruskannya ke fungsi pemrosesan di backend. Setelah diproses, hasilnya diformat sesuai struktur respon yang telah ditentukan, lalu dikirim kembali ke frontend sebagai jawaban akhir. Alur ini memastikan bahwa setiap interaksi pengguna diproses secara efisien dan sesuai standar komunikasi data yang telah ditetapkan.

**HandleTextQuery**

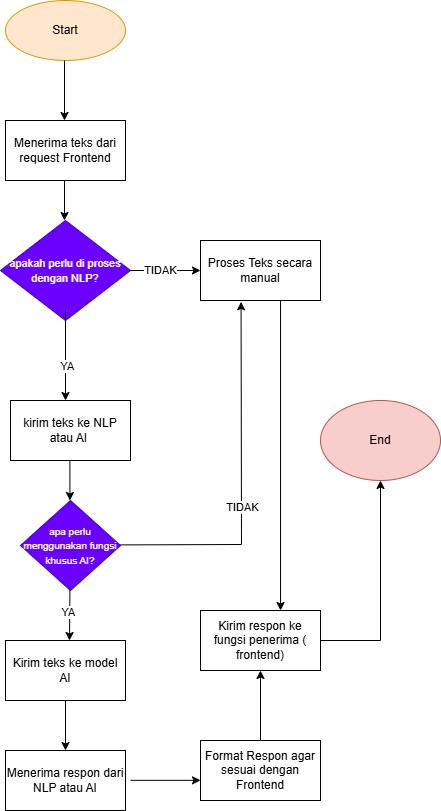


Gambar 27 HandleTextQuery

Flowchart ini menggambarkan alur pengolahan permintaan dari frontend yang dapat melibatkan pemrosesan berbasis NLP atau AI. Proses dimulai saat sistem menerima request dari frontend. Selanjutnya, sistem memeriksa apakah permintaan tersebut memerlukan pemrosesan NLP. Jika tidak, proses akan dilakukan secara manual. Jika diperlukan, permintaan dikirim ke modul NLP atau AI untuk diproses lebih lanjut. Setelah hasil diperoleh, sistem memverifikasi validitas respons. Jika tidak valid, sistem akan mengirimkan pesan kesalahan ke frontend. Bila valid, sistem akan menyesuaikan struktur respons agar sesuai dengan format frontend, kemudian mengirimkannya kembali ke frontend. Setelah itu, sistem memeriksa keberhasilan pengiriman.

Jika berhasil, jawaban akan ditampilkan ke pengguna. Jika tidak, sistem akan menunggu permintaan baru dari pengguna.

**ProcessTextWithAI**



Gambar 28 ProcessTextWithAI

Flowchart ini menjelaskan alur pemrosesan teks yang diterima dari frontend. Setelah sistem menerima input teks dari pengguna melalui frontend, sistem terlebih dahulu memeriksa apakah teks tersebut perlu diproses dengan Natural Language Processing (NLP). Jika tidak, teks akan diproses secara manual. Jika diperlukan, teks dikirim ke modul NLP atau AI. Selanjutnya, sistem mengevaluasi apakah pemrosesan tersebut memerlukan fungsi AI khusus. Jika ya, maka teks dikirim ke model AI untuk mendapatkan hasil yang relevan. Respons yang diterima kemudian diformat agar sesuai dengan kebutuhan frontend, dan dikirim kembali ke frontend untuk ditampilkan. Bila proses tidak memerlukan AI, maka hasil dari NLP langsung diformat dan dikirim ke frontend.

# BAB V

# PRODUCT TESTING (PT) (PENGUJIAN PRODUK)

## 5.1. PENDAHULUAN

Pengujian produk CyberFox dilakukan berdasarkan acuan dari Bab 3 (Product Design) dan Bab 4 (Product Implementation) yang telah disusun pada tahap sebelumnya. Tahapan ini bertujuan untuk memastikan bahwa semua fitur dan komponen yang dikembangkan telah memenuhi standar kualitas serta berjalan sesuai dengan kebutuhan dan tujuan awal pengembangan. Setiap pengujian difokuskan pada fungsi utama sistem, seperti deteksi cyberbullying, pemberian edukasi keamanan siber, serta interaksi chatbot dengan pengguna.

Metode pengujian yang digunakan mencakup black-box testing untuk mengevaluasi fungsionalitas sistem tanpa memperhatikan struktur internal kode, dan usability testing untuk menilai sejauh mana sistem mudah digunakan serta diterima oleh pengguna akhir. Pengujian ini juga dirancang untuk mengidentifikasi bug, inkonsistensi, atau kekurangan lain yang mungkin muncul selama proses interaksi. Dengan tahapan ini, pengembang dapat memastikan bahwa CyberFox telah siap untuk digunakan secara optimal dalam lingkungan nyata.

## 5.2. DESKRIPSI PENGUJIAN

Pengujian CyberFox mencakup serangkaian aktivitas yang dirancang untuk mengevaluasi kualitas, keandalan, dan fungsionalitas sistem sebelum diterapkan secara penuh. Pengujian ini menjadi langkah penting untuk menilai apakah seluruh fitur yang dikembangkan mampu bekerja secara optimal dalam berbagai kondisi penggunaan, baik secara teknis maupun dari sisi pengalaman pengguna.

Setiap pengujian dilakukan untuk memastikan bahwa komponen dalam sistem berjalan sesuai dengan spesifikasi yang telah ditetapkan pada tahap perancangan dan implementasi. Hal ini meliputi verifikasi terhadap alur kerja sistem, respons terhadap masukan pengguna, serta ketahanan sistem terhadap skenario penggunaan yang kompleks. Dengan demikian, pengujian berfungsi sebagai alat kontrol kualitas sebelum CyberFox diluncurkan ke publik.

### 5.2.1. BUTIR UJI

#### 5.2.1.1. Testing Fungsi Login

Tabel 19 Testing Fungsi Login

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nama Butir Uji** | | B-01 | | |
| **Tujuan** | | Memastikan bahwa pengguna dapat login ke dalam sistem dengan kredensial yang benar | | |
| **Deskripsi** | | Pengujian ini mengevaluasi apakah sistem dapat memverifikasi username dan password serta memberikan akses ke halaman utama | | |
| **Kondisi Awal** | | Pengguna berada pada halaman login dan memiliki akun aktif | | |
| **Tanggal**  **Pengujian** | | 26 Mei | | |
| **Penguji** | | 1. Gramaldy 2. Arga | | |
| **Skenario Pengujian** | | | | |
| 1. Pengguna memasukkan username dan password yang validPengguna memberikan pesan yang valid 2. Menekan Tombol Login 3. Memverifikasi data dan masuk ke halaman utama | | | | |
| **Kriteria Evaluasi Hasil** | | | | |
| Login berhasil jika sistem menerima kredensial, membuka halaman utama, dan menyimpan sesi login. | | | | |
| **Kasus dan Hasil Pengujian** | | | | |
| **Data Masukan** | **Yang diharapkan** | | **Pengamatan** | **Kesimpulan** |
| Username &  Password Valid | Sistem  Menerima | | Sesuai diharapkan | [ X ] diterima |

#### 5.2.1.2. Testing Fungsi Register

Tabel 20 Testing Fungsi Register

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nama Butir Uji** | | B-02 | | |
| **Tujuan** | | Memastikan pengguna dapat mendaftar akun baru | | |
| **Deskripsi** | | Pengujian dilakukan untuk memverifikasi apakah pengguna baru dapat mengisi form registrasi dan menyimpan data ke sistem | | |
| **Kondisi Awal** | | Pengguna belum memiliki akun dan berada pada halaman register | | |
| **Tanggal**  **Pengujian** | | 26 Mei 2025 | | |
| **Penguji** | | 1. Idven 2. Samuel | | |
| **Skenario Pengujian** | | | | |
| 1. Pengguna mengisi seluruh form dengan data valid 2. Menekan Tombol “Register” 3. Sistem menyimpan data dan menampilkan notifikasi berhasil | | | | |
| **Kriteria Evaluasi Hasil** | | | | |
| Registrasi dianggap berhasil jika data tersimpan dan sistem mengarahkan pengguna ke halaman login | | | | |
| **Kasus dan Hasil Pengujian** | | | | |
| **Data Masukan** | **Yang diharapkan** | | **Pengamatan** | **Kesimpulan** |
| Data Registrasi  Valid | Sistem menyimpan dan menampilkan pesan sukses | | Sesuai diharapkan | [ X ] diterima |

#### 5.2.1.3. Testing Fungsi Ajukan Pertanyaan

Tabel 21 Testing Fungsi Ajukan Pertanyaan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nama Butir Uji** | | B-03 | | |
| **Tujuan** | | Memastikan pengguna dapat mengirim pertanyaan ke chatbot | | |
| **Deskripsi** | | Pengujian dilakukan untuk melihat apakah pertanyaan ditangani dan dijawab oleh sistem menggunakan Coherre | | |
| **Kondisi Awal** | | Pengguna telah login dan berada di halaman chatbot | | |
| **Tanggal**  **Pengujian** | | 26 Mei 2025 | | |
| **Penguji** | | 1. Idven 2. Samuel | | |
| **Skenario Pengujian** | | | | |
| 1. Pengguna mengetik pertanyaan pada kolom pesan 2. Menekan Tombol Send 3. Sistem mengirim pertanyaan dan menampilkan jawaban | | | | |
| **Kriteria Evaluasi Hasil** | | | | |
| Fungsi dianggap berhasil jika sistem mengirim dan menampilkan jawaban yang relevan | | | | |
| **Kasus dan Hasil Pengujian** | | | | |
| **Data Masukan** | **Yang diharapkan** | | **Pengamatan** | **Kesimpulan** |
| Pertanyaan mengenai Cyber  Security | Sistem memberi respon yang  relevan | | Sesuai diharapkan | [ X ] diterima |

#### 5.2.1.4. Testing Fungsi Melihat History

Tabel 22 Testing Fungsi Melihat History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nama Butir Uji** | | B-04 | | |
| **Tujuan** | | Memastikan pengguna dapat melihat riwayat chat | | |
| **Deskripsi** | | Pengujian dilakukan untuk memastikan bahwa riwayat percakapan tersimpan dan dapat ditampilkan kembali | | |
| **Kondisi Awal** | | Pengguna telah melakukan beberapa sesi chat sebelumnya | | |
| **Tanggal**  **Pengujian** | | 26 Mei 2025 | |  |
| **Penguji** | | 1. Gramaldy 2. Idven | |  |
| **Skenario Pengujia** **n** | | | |  |
| 1. Pengguna mengkilk salah satu bagian history 2. Sistem Menampilkan bagian history yang dipilih | | | |  |
| **Kriteria Evaluasi Hasil** | | | |  |
| Fungsi dianggap berhasil jika history tampil lengkap tanpa error | | | |  |
| **Kasus dan Hasil Pengujian** | | | |  |
| **Data Masukan** | **Yang diharapkan** | | **Pengamatan** | **Kesimpulan** |
| Sesi Chat Sebelumnya | Sistem menampilkan  data chat | | Sesuai diharapkan | [ X ] diterima |

#### 5.2.1.5. Testing Fungsi

Tabel 23 Testing Fungsi Melihat History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nama Butir Uji** | | B-04 | | |
| **Tujuan** | | Memastikan pengguna dapat melihat riwayat chat | | |
| **Deskripsi** | | Pengujian dilakukan untuk memastikan bahwa riwayat percakapan tersimpan dan dapat ditampilkan kembali | | |
| **Kondisi Awal** | | Pengguna telah melakukan beberapa sesi chat sebelumnya | | |
| **Tanggal**  **Pengujian** | | 26 Mei 2025 | |  |
| **Penguji** | | 1. Gramaldy 2. Idven | |  |
| **Skenario Pengujia** **n** | | | |  |
| 1. Pengguna mengkilk salah satu bagian history 2. Sistem Menampilkan bagian history yang dipilih | | | |  |
| **Kriteria Evaluasi Hasil** | | | |  |
| Fungsi dianggap berhasil jika history tampil lengkap tanpa error | | | |  |
| **Kasus dan Hasil Pengujian** | | | |  |
| **Data Masukan** | **Yang diharapkan** | | **Pengamatan** | **Kesimpulan** |
| Sesi Chat Sebelumnya | Sistem menampilkan  data chat | | Sesuai diharapkan | [ X ] diterima |

### 5.2.1. TOOLS PENGUJIAN

Untuk memastikan bahwa sistem CyberFox berjalan dengan baik dan sesuai kebutuhan pengguna, beberapa tools digunakan selama proses pengujian baik dari sisi frontend, backend, maupun integrasi eksternal. Tools yang dipilih mendukung proses pengujian secara akurat, efisien, dan terdokumentasi dengan baik.

1. Postman
   1. Peran: Menguji endpoint API seperti login, register, pengiriman pesan, serta komunikasi dengan Supabase dan OpenAI API.
   2. Alasan Pemilihan: Postman memungkinkan pengujian REST API secara cepat dan mudah dengan dokumentasi otomatis dan fitur scripting untuk validasi respons.
2. Google Chrome Developer Tools
   1. Peran: Mengevaluasi performa aplikasi, debug JavaScript, dan mengamati komunikasi API serta pemuatan aset secara real-time.
   2. Alasan Pemilihan: Alat standar untuk pengujian frontend berbasis web, terutama untuk menangani error, time response, dan akses DOM.

## 5.3. METODE PENGUJIAN

Metode pengujian dalam proyek CyberFox dirancang untuk memastikan bahwa setiap komponen — baik dari sisi frontend, backend, maupun integrasi dengan API eksternal — berjalan dengan baik dan sesuai dengan kebutuhan pengguna. Pendekatan pengujian dilakukan secara bertahap dengan kombinasi pengujian manual dan pengujian berbasis skenario agar mencakup seluruh fungsionalitas utama sistem.

1. **Pengujian Fungsional (Functional Testing)** 
   1. Pendekatan: Dilakukan secara manual terhadap setiap fitur utama seperti login, register, interaksi chatbot, dan riwayat pesan.
   2. Tujuan: Memastikan bahwa fitur bekerja sebagaimana mestinya sesuai dengan spesifikasi pada dokumen desain dan implementasi.
2. **Pengujian Integrasi (Integration Testing)** 
   1. Pendekatan: Menguji hubungan antara modul frontend (React) dengan backend dan layanan eksternal seperti Supabase dan OpenAI API.
   2. Tujuan: Memastikan bahwa data dapat dikirim dan diterima dengan benar, dan komunikasi antar sistem berjalan lancar.
3. **Pengujian Respons dan Validasi Chatbot** 
   1. Pendekatan: Pengguna mencoba memberikan berbagai jenis pertanyaan untuk melihat bagaimana sistem merespons, khususnya dalam konteks edukasi keamanan siber.
   2. Tujuan: Mengevaluasi keakuratan, relevansi, dan kesopanan jawaban yang diberikan oleh chatbot.

### 5.3.1. Pengujian Fungsional

Pengujian fungsional pada CyberFox bertujuan untuk memastikan bahwa seluruh fitur utama dalam aplikasi bekerja sesuai dengan kebutuhan pengguna dan spesifikasi teknis. Fokus pengujian difokuskan pada interaksi pengguna dengan sistem, alur login, pengiriman pertanyaan, pengelolaan riwayat, serta integrasi dengan API eksternal.

1. **Fungsi Login dan Register**

1. Tujuan:

Memastikan pengguna dapat membuat akun dan masuk ke dalam sistem menggunakan kredensial yang valid.

• Skenario:

o Pengguna memasukkan email dan password yang valid → berhasil masuk ke sistem.

o Pengguna memasukkan email atau password yang salah → sistem menolak dan menampilkan pesan kesalahan.

1. Hasil yang Diharapkan:

Validasi input berhasil dilakukan, dan autentikasi berbasis token JWT berjalan sesuai alur keamanan.

1. Fungsi Chat (Ajukan Pertanyaan)

1. Tujuan:

Memastikan pengguna dapat mengajukan pertanyaan dan menerima balasan dari chatbot.

Skenario:

* + - * Pengguna mengetikkan pertanyaan seputar keamanan siber.
      * Sistem mengirimkan prompt ke API dan menampilkan balasan dari chatbot.

2. Hasil yang Diharapkan:

Respons cepat, informatif, dan relevan dengan konteks edukasi keamanan siber. 3. 4. Fungsi Riwayat (History)

1. Tujuan:

Memastikan sistem mencatat semua pertanyaan dan jawaban sebelumnya untuk setiap pengguna.

Skenario:

• Setelah sesi tanya-jawab, pengguna membuka halaman Riwayat Chat.

2. Hasil yang Diharapkan:

Riwayat percakapan ditampilkan secara berurutan berdasarkan waktu, lengkap dengan isi pertanyaan dan jawaban.

1. Fungsi Upload Dataset (Mode Maintenance)
   1. Tujuan:

Memastikan admin dapat mengunggah atau memperbarui dataset untuk keperluan pelatihan atau referensi offline chatbot.

Skenario:

o Admin login ke sistem dan mengunggah file .txt melalui mode maintenance.

* 1. Hasil yang Diharapkan:

File berhasil tersimpan di database Supabase tanpa terjadi error atau kegagalan pengunggahan.

1. Fungsi Logout dan Keamanan Sesi
   1. Tujuan:

Memastikan token sesi habis masa berlakunya setelah logout dan tidak dapat digunakan kembali.

Skenario:

* + - * Pengguna melakukan logout dari sistem.
      * Pengguna mencoba mengakses kembali dashboard tanpa login.
  1. Hasil yang Diharapkan:

Sistem menolak akses tidak sah dan mengarahkan pengguna ke halaman login.

### 5.3.2. Pengujian Non Fungsional

Pengujian non-fungsional bertujuan untuk mengevaluasi aspek-aspek yang tidak langsung terkait dengan fungsi utama CyberFox, namun sangat penting dalam menjamin kualitas keseluruhan sistem. Fokus pengujian mencakup kinerja, keamanan, dan keandalan layanan yang diberikan.

1. Pengujian Kinerja

Tujuan: Mengukur kecepatan respons aplikasi dalam memproses permintaan pengguna.

Metode:

1. Merekam waktu antara pengguna mengirim pertanyaan hingga jawaban ditampilkan.
2. Pengujian dilakukan pada jaringan normal dan kondisi jaringan lambat.

* Hasil yang Diharapkan:
* Waktu respons rata-rata di bawah 3 detik dalam kondisi normal.
* Sistem tetap responsif dalam kondisi koneksi lambat (< 7 detik).

# BAB VI

# PRODUCT RELEASE (PR) (PELUNCURAN PRODUK)

## 6.1. PENDAHULUAN

Peluncuran produk merupakan tahapan akhir dalam siklus pengembangan, yang menandai kesiapan sistem untuk digunakan oleh pengguna secara langsung. Pada tahap ini, seluruh hasil desain, implementasi, dan pengujian diuji dalam konteks nyata agar dapat memberikan gambaran menyeluruh terhadap performa sistem saat berinteraksi dengan pengguna sebenarnya. Peluncuran menjadi momentum penting untuk mengamati bagaimana sistem bekerja di luar lingkungan pengujian, serta untuk mengidentifikasi potensi perbaikan lanjutan pascaproduksi.

Tujuan utama dari peluncuran CyberFox adalah untuk memperkenalkan chatbot edukatif ini kepada khalayak sasaran, khususnya anak-anak dan pendidik, guna mendukung literasi keamanan internet sejak dini. Peluncuran dilakukan secara bertahap melalui strategi soft launch untuk menguji respons awal pengguna dan kesiapan sistem dalam skala terbatas, sebelum menuju ke full launch yang lebih luas. Pendekatan ini memungkinkan pengembang untuk mengumpulkan masukan berharga, melakukan penyesuaian teknis, serta memastikan infrastruktur pendukung siap menghadapi distribusi secara masif

## 6.2.DESKRIPSI

Peluncuran produk CyberFox dilakukan dengan strategi yang terencana guna memastikan jangkauan efektif kepada target pengguna, yaitu anak-anak usia sekolah dasar hingga menengah pertama, serta para pendidik dan orang tua sebagai pendamping literasi digital. Strategi ini mencakup identifikasi kanal distribusi yang tepat, seperti platform pembelajaran digital, media sosial edukatif, dan kerja sama dengan institusi pendidikan untuk memperluas eksposur chatbot kepada pengguna yang relevan.

Selain itu, peluncuran juga dilengkapi dengan materi pendukung seperti panduan penggunaan, video tutorial, dan sesi sosialisasi langsung agar pengguna dapat memahami manfaat dan cara kerja CyberFox secara menyeluruh. Melalui pendekatan ini, diharapkan adopsi teknologi dapat berlangsung lebih cepat, serta membangun kepercayaan dan keterlibatan aktif dari komunitas pendidikan dalam memanfaatkan CyberFox sebagai alat bantu pembelajaran keamanan digital yang interaktif dan menyenangkan.

### 6.2.1. DAYA GUNA PRODUK

Produk CyberFox dirancang untuk memberikan kemudahan akses edukasi mengenai keamanan siber kepada pengguna, khususnya remaja dan pelajar, melalui pendekatan interaktif berbasis chatbot. Dengan memanfaatkan teknologi percakapan otomatis, CyberFox mampu menyampaikan materi edukatif secara lebih menarik dan mudah dipahami, bahkan oleh pengguna yang belum terbiasa dengan istilah-istilah teknis dalam dunia keamanan digital. Pendekatan ini bertujuan untuk menciptakan pengalaman belajar yang lebih personal dan responsif terhadap kebutuhan pengguna.

Selain itu, produk ini memiliki sejumlah fitur unggulan yang memberikan nilai tambah dan membedakannya dari solusi lain yang tersedia di pasar. Beberapa di antaranya termasuk sistem pendeteksi kata kasar atau konten negatif, modul pembelajaran bertahap sesuai tingkat usia, serta fitur simulasi kasus yang mengajak pengguna untuk memahami ancaman siber melalui pengalaman interaktif. Fitur-fitur tersebut dirancang untuk mendorong kesadaran dan pemahaman mendalam mengenai bahaya di dunia digital, serta membekali pengguna dengan langkah-langkah perlindungan yang tepat.

## 

## 6.3 POSTER PRODUK

Poster untuk CyberFox dirancang untuk menarik perhatian audiens target, yaitu remaja dan pelajar, dengan desain yang segar, modern, dan ramah. Pemilihan warna-warna cerah, ilustrasi yang komunikatif, serta tipografi yang mudah dibaca menjadi elemen utama dalam menciptakan kesan visual yang menarik dan tidak membosankan. Desain ini bertujuan untuk mencerminkan semangat positif dan edukatif dari produk, sekaligus membangun kedekatan emosional dengan pengguna muda.

Elemen-elemen visual yang digunakan juga berfokus pada estetika yang mudah diakses dan menyenangkan, seperti ikon-ikon bertema digital, karakter chatbot yang bersahabat, dan layout yang tidak padat namun informatif. Selain sebagai media promosi, poster ini juga berfungsi sebagai alat edukasi visual yang memperkenalkan konsep dasar keamanan siber secara ringkas. Dengan pendekatan ini, diharapkan pesan inti CyberFox dapat tersampaikan dengan efektif dan mengundang minat audiens untuk mencoba produk secara langsung.

**Hal yang dapat disertakan:**

1. Gambar Produk :



Gambar 29 Poster Produk

1. Fitur Utama:



Gambar 30 FItur Utama

# DAFTAR PUSTAKA

Alami, A., & Mansour, H. (2020). *The impact of AI-driven chatbots in education: A review of research and applications*. Journal of Educational Technology, 18(4), 112-125.

Aspris, E., & Li, S. (2019). *Enhancing digital literacy through chatbot platforms in schools*. Journal of Digital Education, 25(3), 78-92.

Kaspersky. (2021). *Children and cybersecurity: Protecting young digital users*. Retrieved from https://www.kaspersky.com/children-cybersecurity

Smith, R., & Johnson, P. (2018). *Developing secure and interactive educational tools using AI chatbots*. Proceedings of the International Conference on Educational Technology, 34(2), 53-

62.

Wang, Z., Zhang, C., & Liu, H. (2020). *Integrating AI chatbots into educational systems: Benefits and challenges*. International Journal of Artificial Intelligence in Education, 22(1), 10-

25.

Zhang, Y., & Chen, Y. (2021). *AI and cybersecurity education for children: The role of interactive platforms*. Journal of Cybersecurity Education, 29(1), 30-42.

World Economic Forum. (2021). *The future of cybersecurity education for children in the digital age*. Retrieved from <https://www.weforum.org/future-cybersecurity-education>

# LAMPIRAN

* **Keamanan Akun & Identitas Digital**

**Ringkasan**

Keamanan akun dan identitas digital adalah aspek penting dalam menjaga privasi saat menggunakan layanan online. Banyak serangan siber terjadi akibat lemahnya perlindungan akun, seperti penggunaan kata sandi yang buruk atau tidak adanya autentikasi tambahan.

**Poin Edukasi Penting**

* 1. Gunakan kata sandi yang kuat dan unik untuk setiap akun.
  2. Aktifkan autentikasi dua faktor (2FA).
  3. Jangan gunakan informasi pribadi sebagai kata sandi.
  4. Gunakan password manager untuk menyimpan kata sandi secara aman.
  5. Waspadai email atau pesan mencurigakan yang meminta informasi login.

**Contoh Kasus**

Seorang pengguna memakai kata sandi yang sama untuk semua akun. Saat satu layanan mengalami kebocoran data, peretas menggunakan kata sandi tersebut untuk membobol akun email utama.

**Tips Pencegahan**

* + 1. Gunakan kombinasi huruf besar, kecil, angka, dan simbol.
    2. Jangan simpan kata sandi di browser tanpa enkripsi.
    3. Hindari Wi-Fi publik tanpa VPN saat login.
    4. Ganti kata sandi secara berkala.

**Sumber Referensi**  : tekno.sindonews.com

* **Keamanan Perangkat & Proteksi Digital**

**Ringkasan**

Keamanan perangkat adalah kunci utama menjaga data dan sistem informasi. Perangkat yang tidak diperbarui atau tidak dilindungi rentan menjadi target serangan siber.

**Poin Edukasi Penting**

* 1. Perbarui sistem operasi dan aplikasi secara rutin.
  2. Gunakan antivirus dan anti-malware terpercaya.
  3. Aktifkan firewall.
  4. Hindari menginstal aplikasi dari sumber tidak terpercaya.
  5. Evaluasi izin aplikasi sebelum menginstal.

**Contoh Kasus**

Pengguna tidak memperbarui sistem operasi laptopnya. Akibatnya, malware memanfaatkan celah keamanan dan mencuri data login bank miliknya.

**Tips Pencegahan**

* + 1. Aktifkan pembaruan otomatis.
    2. Gunakan koneksi internet aman.
    3. Periksa izin akses aplikasi.
    4. Lakukan pemindaian antivirus secara berkala.

**Sumber Referensi** : tekno.sindownews.com

* **Paparan Konten Negatif & Kesehatan Mental Digital**

**Ringkasan**

Konten negatif seperti kekerasan, hoaks, dan ujaran kebencian dapat berdampak buruk secara emosional dan mental. Ini juga bisa menjadi pintu masuk serangan sosial-engineering atau phishing.

**Poin Edukasi Penting**

* 1. Paparan berlebih dapat menyebabkan stres dan kelelahan mental.
  2. Konten palsu digunakan untuk manipulasi atau penyebaran malware.
  3. Penipuan daring sering menargetkan orang yang rentan secara psikologis.

**Contoh Kasus**

Seorang remaja mengikuti akun penuh ujaran kebencian dan hoaks. Ia menjadi gelisah setiap membuka media sosial, dan akhirnya tertipu oleh tautan phishing berkedok “berita penting.”

**Tips Pencegahan**

* 1. Kurasi akun/media yang diikuti.
  2. Lakukan detoks media sosial secara berkala.
  3. Gunakan fitur "report" dan "block".
  4. Verifikasi kebenaran informasi sebelum menyebarkannya.
  5. Jaga kesehatan mental sebagai bagian dari keamanan digital.

**Sumber Referensi** : https://www.detik.com

* **Waspadai Phishing: Ciri-Ciri & Cara Mengeceknya**  **Ringkasan**

Phishing adalah upaya penipuan yang menyamar sebagai entitas terpercaya untuk mencuri data pribadi, biasanya lewat email, SMS, atau link palsu.

**Poin Edukasi Penting**

* 1. Link phishing sering meniru situs resmi (contoh: go0gle.com).
  2. Pesan phishing bersifat mendesak atau menakut-nakuti.
  3. Bisa terjadi di media sosial, email, bahkan SMS.

**Contoh Kasus**

Seseorang menerima email dari “Bank XYZ” yang menyatakan akunnya akan diblokir. Karena panik, ia mengklik link dan mengisi data pribadi di situs palsu. Akibatnya, akun dan dananya dicuri.

**Tips Pencegahan**

* 1. Periksa ejaan URL dan domain dengan teliti.
  2. Jangan klik link mencurigakan tanpa verifikasi.
  3. Aktifkan autentikasi dua faktor.
  4. Gunakan antivirus dengan proteksi web.
  5. Laporkan dan hapus email phishing.

**Sumber Referensi**  : <https://www.msn.com/>

# Dokumentasi Pengumpulan Data

Observasi dilakukan dengan metode pengumpulan data melalui kuesioner yang diberikan kepada anak-anak. Kuesioner berisi pertanyaan terbuka terkait dengan dua topik utama: Keamanan Siber dan Cyberbullying. Hasilnya dianalisis untuk memahami pola pemikiran anak-anak terhadap kedua isu tersebut.

**Pertanyaan Anak-Anak tentang Keamanan cyber :**

Beberapa pertanyaan yang diajukan oleh anak-anak terkait dengan keamanan siber adalah:

1. Mengapa tidak boleh mengklik iklan sembarangan di internet?
2. Mengapa tidak boleh membagikan alamat rumah atau sekolah di media sosial?
3. Mengapa tidak boleh memberikan password kepada teman?
4. Apa itu hacker, dan mengapa harus takut pada hacker?
5. Mengapa tidak boleh sembarangan mengunduh aplikasi atau game?
6. Mengapa tidak boleh percaya semua berita yang dibaca di internet?

**Anak SD Mutiara :**

* 1. Mengapa kita harus berhati-hati saat menggunakan internet?
  2. Mengapa kita tidak boleh membagikan informasi pribadi kepada orang asing di internet?
  3. Apa saja contoh informasi pribadi yang tidak boleh dibagikan di internet?
  4. Apa yang harus dilakukan sebelum mendownload aplikasi atau game di HP atau komputer?
  5. Mengapa kita tidak boleh asal membagikan foto atau video pribadi di internet?

**Anak SMP N 2 Balige:**

1. Mengapa kita harus menggunakan kata sandi yang kuat dan unik untuk setiap akun?
2. Mengapa kita harus berhati-hati saat menerima permintaan pertemanan dari orang yang tidak dikenal?
3. Apa saja tanda-tanda bahwa seseorang sedang mencoba menipu kita di internet?
4. Mengapa kita tidak boleh membagikan lokasi kita secara real-time di media sosial?
5. Apa saja informasi pribadi yang sebaiknya tidak dibagikan kepada orang lain di dunia maya?
6. Bagaimana cara membuat kata sandi yang kuat dan sulit ditebak?
7. Apa dampak dari menyebarkan berita hoaks atau informasi palsu di internet?
8. Apa yang harus dilakukan jika kita tidak sengaja menyebarkan informasi yang salah di media sosial?

**Anak SMA BTB:**

1. Apa perbedaan antara cyber security dan cyber crime?
2. Bagaimana cara kita sebagai pengguna bisa ikut serta dalam meningkatkan kesadaran tentang cyber security**?**
3. Bagaimana perkembangan Internet of Things (IoT) bisa meningkatkan risiko serangan siber?
4. Bagaimana cara menghindari penipuan online di media sosial atau marketplace?
5. Apa bahaya dari membagikan terlalu banyak informasi pribadi di media sosial?
6. Mengapa kita harus berhati-hati saat menggunakan Wi-Fi publik?
7. Bagaimana cara mengetahui apakah sebuah situs web itu aman atau berbahaya?
8. Bagaimana cara mengamankan akun media sosial agar tidak mudah diretas?
9. Apa dampak serangan siber terhadap individu dan perusahaan?

**Pertanyaan Anak-Anak tentang Cyberbullying :**

Selain keamanan siber, anak-anak juga mengajukan berbagai pertanyaan terkait cyberbullying, antara lain:

1. Mengapa korban cyberbullying bisa merasa sangat sedih?
2. Apakah bercanda di internet bisa dianggap cyberbullying?
3. Apakah menyebarkan rumor atau gosip palsu termasuk cyberbullying?
4. Apakah mengecualikan seseorang dari grup online juga termasuk cyberbullying?
5. Bagaimana jika seseorang menyebarkan rahasia atau foto orang lain tanpa izin?
6. Apakah cyberbullying dapat mempengaruhi prestasi akademik?
7. Apakah memberikan "like" pada komentar ejekan juga termasuk cyberbullying?
8. Apa yang harus dilakukan jika melihat teman dibully di internet?
9. Bagaimana cara memblokir pelaku cyberbullying?
10. Jika melaporkan cyberbullying ke platform media sosial, apakah akun pelaku akan langsung dihapus?

**Anak Smp N 2 balige :**

1. Apakah media sosial seperti Instagram, TikTok, atau WhatsApp aman dari cyber bullying?
2. Bagaimana cara mengatur privasi akun media sosial agar lebih aman?
3. Apakah sekolah bisa menghukum siswa yang melakukan cyber bullying?
4. Apa hukuman bagi seseorang yang melakukan cyber bullying?
5. Apakah ada cara untuk melaporkan pelaku cyber bullying?
6. Bagaimana cara mengatur privasi akun media sosial agar lebih aman?
7. Apa yang harus saya lakukan jika akun saya diretas dan digunakan untuk cyber bullying?
8. Jika saya membalas cyber bullying, apakah saya juga dianggap bersalah?

**Remaja SMA BTB :**

**Tingkat 1**

1. Mengapa banyak orang merasa lebih berani melakukan cyber bullying dibandingkan bullying langsung?
2. Bagaimana cyber bullying bisa berdampak pada kesehatan mental seseorang?
3. Apa perbedaan antara kritik dan cyber bullying?

**Tingkat 2 :**

1. Bagaimana cyber bullying dapat berdampak pada kehidupan sosial dan akademik seseorang?
2. Mengapa banyak orang yang menjadi korban cyber bullying tetap diam dan tidak melaporkannya?
3. Apakah ada batasan antara "dark humor" dan cyber bullying? Bagaimana cara membedakannya?

**Tingkat 3 :**

1. Jika seseorang menyebarkan screenshot percakapan pribadi tanpa izin, apakah itu termasuk cyber bullying atau pelanggaran privasi?
2. Apakah ada tanggung jawab bagi platform media sosial jika terjadi cyber bullying di dalam platform mereka?
3. Bagaimana cara membedakan kebebasan berpendapat dengan cyber bullying?
4. Bagaimana cara membangun mental yang kuat agar tidak mudah terpengaruh oleh cyber bullying?
5. Apakah menghindari media sosial sepenuhnya adalah solusi terbaik untuk menghindari cyber bullying? Mengapa?
6. Seberapa besar pengaruh media sosial dalam membentuk budaya cyber bullying di kalangan remaja?
7. Bagaimana psikologi seseorang yang menjadi pelaku cyber bullying? Apakah mereka juga korban dalam beberapa kasus?

# Data Set Tambahan

1. Apa yang sebaiknya kamu lakukan jika menerima pesan mencurigakan dari orang yang tidak dikenal?

Jawaban: Jangan dibalas, segera laporkan dan hapus pesannya.

1. Mengapa kita tidak boleh membagikan kata sandi kepada teman?

Jawaban: Karena kata sandi bersifat pribadi dan bisa disalahgunakan.

1. Apa itu virus komputer dan bagaimana cara menghindarinya?

Jawaban: Virus komputer adalah program berbahaya. Hindari dengan tidak mengklik tautan sembarangan dan selalu gunakan antivirus.

1. Apa fungsi dari fitur ‘privasi akun’ di media sosial?

Jawaban: Untuk membatasi siapa saja yang bisa melihat informasi pribadimu.

1. Mengapa penting untuk selalu logout dari akun setelah selesai digunakan, terutama di komputer umum?

Jawaban: Agar orang lain tidak bisa mengakses akunmu dan menyalahgunakannya.

1. Apa yang dimaksud dengan cyberbullying?

Jawaban: Tindakan mengganggu, menghina, atau menyakiti orang lain melalui internet.

1. Bagaimana cara melindungi data pribadi saat bermain game online?

Jawaban: Jangan membagikan data pribadi seperti nama lengkap, alamat, atau nomor telepon.

1. Apa yang harus dilakukan jika akun media sosial kamu diretas?

Jawaban: Segera ubah kata sandi, aktifkan verifikasi dua langkah, dan laporkan ke penyedia layanan.

1. Kenapa penting menggunakan kata sandi yang kuat dan unik?

Jawaban: Agar akun tidak mudah dibobol oleh orang yang tidak bertanggung jawab.

1. Apa itu ‘verifikasi dua langkah’ dan mengapa penting?

Jawaban: Fitur keamanan tambahan yang meminta kode saat login. Penting agar akun lebih aman.

1. Apa tanda-tanda situs web yang tidak aman untuk dikunjungi?

Jawaban: Tidak menggunakan HTTPS, banyak iklan mencurigakan, dan meminta informasi pribadi tanpa alasan jelas.

1. Mengapa tidak boleh mengunggah foto kartu pelajar atau identitas lainnya ke internet?

Jawaban: Karena bisa digunakan oleh orang lain untuk pencurian identitas.

1. Apa yang sebaiknya dilakukan jika melihat teman diintimidasi secara online?

Jawaban: Dukung teman tersebut, simpan bukti, dan laporkan ke pihak berwenang atau guru.

1. Apa itu hoax dan bagaimana cara mengenalinya?

Jawaban: Hoax adalah berita bohong. Ciri-cirinya: tidak ada sumber jelas, berisi provokasi, dan terlalu sensasional.

1. Apa dampaknya jika kamu membagikan informasi pribadi sembarangan di internet?

Jawaban: Bisa jadi korban penipuan, pencurian identitas, atau pelecehan online.

1. Bagaimana cara membuat kata sandi yang aman?

Jawaban: Gunakan kombinasi huruf besar, kecil, angka, dan simbol. Jangan gunakan tanggal lahir atau nama sendiri.

1. Apa itu malware dan bagaimana masuk ke komputer?

Jawaban: Malware adalah program jahat. Bisa masuk lewat file yang diunduh, tautan palsu, atau situs tidak aman.

1. Apa itu spam dan kenapa harus dihindari?

Jawaban: Pesan sampah yang seringkali berisi penipuan atau virus. Bisa mengganggu dan membahayakan.

1. Apa yang harus kamu lakukan jika melihat akun palsu di media sosial?

Jawaban: Laporkan ke platform tersebut agar dihapus atau diblokir.

1. Mengapa perlu memeriksa izin aplikasi sebelum menginstalnya?

Jawaban: Agar kamu tahu data apa yang diakses aplikasi dan bisa mencegah penyalahgunaan.

1. Apa itu jejak digital?

Jawaban: Semua data dan aktivitasmu yang terekam di internet.

1. Apa yang dimaksud dengan pencurian identitas?

Jawaban: Saat seseorang menggunakan data pribadimu untuk berpura-pura menjadi kamu.

1. Apa manfaat menggunakan VPN saat menggunakan Wi-Fi umum?

Jawaban: Melindungi data pribadi agar tidak mudah disadap orang lain.

1. Kenapa kita tidak boleh sembarangan klik link hadiah di internet?

Jawaban: Karena bisa jadi jebakan berisi virus atau penipuan.

1. Apa yang harus dilakukan jika kamu menerima ancaman secara online?

Jawaban: Simpan bukti, blokir pelaku, dan laporkan ke orang tua atau pihak berwajib.

1. Mengapa perlu mengatur batas waktu penggunaan gadget?

Jawaban: Agar tidak kecanduan, lebih fokus belajar, dan menjaga kesehatan mental.

1. Apa perbedaan antara teman online dan teman nyata?

Jawaban: Teman online belum tentu bisa dipercaya karena kamu tidak mengenalnya secara langsung.

1. Bagaimana cara tahu apakah aplikasi itu aman diunduh?

Jawaban: Lihat ulasan pengguna, jumlah unduhan, dan pastikan dari toko aplikasi resmi.

1. Apa itu phishing?

Jawaban: Upaya penipuan dengan menyamar sebagai pihak terpercaya untuk mencuri data pribadi.

1. Kenapa kita harus hati-hati saat berbagi cerita pribadi di internet?

Jawaban: Karena orang lain bisa menyalahgunakan informasi tersebut.

1. Apa itu konten negatif di internet?

Jawaban: Konten yang mengandung kekerasan, kebencian, pornografi, atau hal yang tidak pantas.

1. Kenapa kita perlu berpikir sebelum berkomentar di media sosial?

Jawaban: Karena komentar kita bisa menyakiti orang lain atau disalahartikan.

1. Apa bahaya bermain game online tanpa pengawasan?

Jawaban: Bisa terkena cyberbullying, kecanduan, atau diminta membayar hal yang tidak perlu.

1. Apa arti dari 'akun kamu dibajak'?

Jawaban: Akunmu diambil alih oleh orang lain tanpa izin.

1. Bagaimana cara mencegah akun dibajak?

Jawaban: Gunakan kata sandi kuat dan aktifkan verifikasi dua langkah.

1. Apa itu deepfake dan kenapa berbahaya?

Jawaban: Video palsu yang dimanipulasi agar terlihat nyata. Bisa digunakan untuk menipu atau merusak reputasi orang.

1. Apa yang harus dilakukan jika melihat video hoax tersebar di grup chat?

Jawaban: Jangan ikut sebar, periksa kebenarannya, dan beri tahu orang lain bahwa itu hoax.

1. Mengapa penting menjaga etika saat berdiskusi di forum online?

Jawaban: Agar suasana tetap positif dan tidak terjadi pertengkaran.

1. Apa saja yang tidak boleh dibagikan di internet?

Jawaban: Nomor KTP, alamat rumah, nomor rekening, foto identitas, dan informasi sensitif lainnya.

1. Apa yang dimaksud dengan grooming online?

Jawaban: Upaya orang dewasa mendekati anak atau remaja secara online untuk tujuan buruk.

1. Bagaimana cara mengenali email penipuan?

Jawaban: Biasanya menggunakan bahasa aneh, minta data pribadi, dan berasal dari alamat email tidak resmi.

1. Apa itu doxing?

Jawaban: Menyebarkan informasi pribadi seseorang di internet tanpa izin.

1. Apa yang dimaksud dengan cybercrime?

Jawaban: Kejahatan yang dilakukan menggunakan komputer atau internet.

1. Bagaimana cara menjaga reputasi digital yang baik?

Jawaban: Berperilaku positif, tidak menyebar hoax, dan menjaga konten yang dibagikan.

1. Apa bahaya membuka file dari pengirim tidak dikenal?

Jawaban: File tersebut bisa mengandung virus atau program jahat lainnya.

1. Mengapa tidak boleh percaya begitu saja pada informasi di media sosial?

Jawaban: Karena tidak semua informasi benar dan bisa saja menyesatkan.

1. Apa itu kebocoran data?

Jawaban: Saat data pribadi tersebar atau diakses orang lain tanpa izin.

1. Bagaimana cara aman menggunakan media sosial?

Jawaban: Jaga privasi, jangan bagikan data pribadi, dan berhati-hati saat berteman dengan orang baru.

1. Apa manfaat belajar tentang keamanan digital sejak usia muda?

Jawaban: Agar lebih bijak, aman, dan terhindar dari kejahatan digital.

1. Apa yang harus dilakukan jika kamu jadi korban penipuan online?

Jawaban: Laporkan ke orang tua, guru, dan pihak berwajib. Jangan diam saja.

1. Apa yang dimaksud dengan konten berbahaya di internet?

Jawaban: Konten yang bisa mempengaruhi pikiran atau perilaku negatif, seperti kekerasan, ujaran kebencian, atau pornografi.

1. Mengapa kita harus memperbarui aplikasi secara rutin?

Jawaban: Untuk memperbaiki bug dan meningkatkan keamanan dari serangan terbaru.

1. Bagaimana cara agar tidak mudah tertipu iklan palsu di internet?

Jawaban: Jangan langsung percaya, periksa sumbernya, dan hindari mengklik iklan mencurigakan.

1. Apa itu bot dalam dunia digital?

Jawaban: Program otomatis yang bisa digunakan untuk kebaikan atau kejahatan, seperti menyebarkan spam.

1. Apa yang dimaksud dengan ‘scam’?

Jawaban: Penipuan online yang biasanya bertujuan mencuri uang atau data pribadi.

1. Kenapa penting untuk membatasi siapa yang bisa melihat profil media sosialmu?

Jawaban: Agar informasi pribadi tidak dilihat atau disalahgunakan orang asing.

1. Apa yang harus kamu lakukan saat melihat komentar jahat di postingan orang lain?

Jawaban: Jangan ikut-ikutan, laporkan komentarnya, dan beri dukungan positif.

1. Apa itu ‘cookies’ di situs web dan apa bahayanya?

Jawaban: Data kecil yang menyimpan informasi pengguna. Bisa digunakan untuk melacak aktivitasmu.

1. Kenapa perlu berhati-hati saat bermain di ruang obrolan publik game online?

Jawaban: Karena siapa pun bisa ada di sana, termasuk orang yang berniat jahat.

1. Apa itu pengaturan privasi dan mengapa penting digunakan?

Jawaban: Fitur yang mengontrol siapa yang bisa melihat informasi kita, untuk menjaga keamanan akun.

1. Mengapa tidak boleh menyebar foto teman tanpa izin?

Jawaban: Karena itu termasuk pelanggaran privasi dan bisa membuat temanmu tidak nyaman.

1. Bagaimana kamu tahu aplikasi itu legal dan aman?

Jawaban: Diunduh dari toko resmi dan memiliki banyak ulasan positif.

1. Apa yang harus dilakukan jika kamu menemukan video tidak pantas beredar?

Jawaban: Jangan disebarkan, laporkan ke platform, dan beri tahu orang dewasa.

1. Mengapa kita perlu membaca syarat dan ketentuan saat mendaftar suatu layanan online?

Jawaban: Untuk tahu hak dan kewajiban kita serta bagaimana data kita digunakan.

1. Apa itu fake account dan bagaimana bahayanya?

Jawaban: Akun palsu yang menyamar menjadi orang lain. Bisa digunakan untuk menipu atau mencuri data.

1. Kenapa tidak boleh asal memasukkan informasi kartu kredit di situs tidak dikenal?

Jawaban: Karena bisa disalahgunakan untuk penipuan atau pencurian uang.

1. Apa itu cyberstalking?

Jawaban: Saat seseorang mengawasi aktivitas online kita secara berlebihan atau mengganggu.

1. Bagaimana kamu bisa tahu bahwa sebuah aplikasi minta akses berlebihan?

Jawaban: Jika minta izin yang tidak ada hubungannya dengan fungsi aplikasinya, seperti minta akses kamera untuk aplikasi catatan.

1. Mengapa tidak disarankan menerima permintaan pertemanan dari orang asing?

Jawaban: Karena kamu tidak tahu siapa mereka dan bisa berisiko.

1. Apa peran keluarga dalam menjaga keamanan digitalmu?

Jawaban: Memberi arahan, mendampingi saat online, dan membantu jika ada masalah.

1. Apa itu filter konten dan kenapa penting?

Jawaban: Fitur yang memblokir konten negatif agar kita tidak melihat hal yang tidak pantas.

1. Apa dampaknya jika kita menyebar berita yang belum pasti kebenarannya?

Jawaban: Bisa menyebabkan kepanikan, kesalahpahaman, atau menyebar kebohongan.

1. Bagaimana cara mendeteksi akun palsu di media sosial?

Jawaban: Ciri-cirinya seperti tidak punya banyak teman asli, fotonya aneh, atau isinya mencurigakan.

1. Apa yang dimaksud dengan ‘over-sharing’ di media sosial?

Jawaban: Membagikan terlalu banyak informasi pribadi yang seharusnya tidak dipublikasikan.

1. Kenapa kita harus mengatur waktu penggunaan gadget setiap hari?

Jawaban: Agar tidak kecanduan dan tetap punya waktu untuk belajar, istirahat, dan bersosialisasi.

1. Apa yang harus dilakukan jika kamu merasa terganggu oleh seseorang secara online?

Jawaban: Blokir orang tersebut dan laporkan ke platform atau orang dewasa.

1. enapa penting untuk tidak menyimpan foto sensitif di internet atau cloud?

Jawaban: Karena bisa diretas dan disebarkan tanpa izin.

1. Apa itu konten palsu yang diedit agar terlihat nyata?

Jawaban: Disebut sebagai konten manipulatif atau hoax visual, biasanya digunakan untuk menipu orang.

1. Bagaimana cara melaporkan konten yang tidak pantas di media sosial?

Jawaban: Gunakan tombol “laporkan” atau “report” yang disediakan di setiap postingan atau komentar.

1. Apa bahaya bermain internet tanpa pengawasan orang tua?

Jawaban: Bisa mengakses hal berbahaya, tertipu, atau berbicara dengan orang asing berbahaya.

1. Apa yang harus dilakukan jika ada orang asing yang memaksa minta foto pribadi?

Jawaban: Jangan diberi, blokir orangnya, dan segera laporkan ke orang dewasa.

1. Mengapa kita harus hati-hati dengan siapa yang kita izinkan mengikuti akun kita?

Jawaban: Karena bisa saja mereka punya niat buruk terhadap kita atau data kita.

1. Apa risiko menyimpan kata sandi di catatan ponsel tanpa pengamanan?

Jawaban: Jika ponsel hilang atau diretas, orang lain bisa mengakses semua akunmu.

1. Apa yang dimaksud dengan ‘konten yang memicu’ atau triggering content?

Jawaban: Konten yang bisa membuat orang merasa trauma, takut, atau tidak nyaman.

1. Kenapa tidak boleh menanggapi komentar kebencian dengan emosi?

Jawaban: Bisa memperburuk keadaan dan memancing lebih banyak konflik.

1. Bagaimana cara tahu sebuah giveaway online itu palsu?

Jawaban: Jika minta data pribadi, bayar duluan, atau terdengar terlalu bagus untuk jadi kenyataan.

1. Kenapa sebaiknya tidak sembarang klik link yang dikirim di grup?

Jawaban: Bisa jadi link tersebut berisi virus atau situs penipuan.

1. Apa itu dark web dan kenapa harus dihindari?

Jawaban: Bagian dari internet yang tidak bisa diakses biasa, sering digunakan untuk aktivitas ilegal.

1. Apa yang harus kamu lakukan sebelum posting sesuatu ke media sosial?

Jawaban: Pikirkan dampaknya, pastikan tidak melanggar privasi orang lain, dan tidak menyinggung.

1. Bagaimana cara menghindari kecanduan media sosial?

Jawaban: Atur waktu penggunaan, matikan notifikasi, dan fokus pada aktivitas offline.

1. Kenapa harus update sistem operasi secara rutin?

Jawaban: Agar perangkat lebih aman dan tidak mudah diserang virus.

1. Apa itu cyber grooming dan kenapa sangat berbahaya?

Jawaban: Saat orang dewasa membujuk anak muda online untuk tujuan buruk, seperti eksploitasi.

1. Apa itu rekam jejak digital negatif?

Jawaban: Catatan online yang bisa merugikan kita di masa depan, seperti komentar kasar atau konten tidak pantas.

1. Apa saja langkah awal saat membuat akun online yang aman?

Jawaban: Gunakan email aktif, kata sandi kuat, dan aktifkan fitur keamanan tambahan.

1. Bagaimana cara bijak menggunakan fitur story atau status?

Jawaban: Jangan posting hal pribadi, lokasi real-time, atau sesuatu yang bisa menimbulkan masalah.

1. Apa itu scammer dan bagaimana mereka menipu?

Jawaban: Penipu online yang menyamar dan menggunakan berbagai cara untuk mencuri uang atau data.

1. Apa yang bisa terjadi jika kita memakai Wi-Fi publik tanpa perlindungan?

Jawaban: Data pribadi bisa disadap oleh orang lain yang terhubung di jaringan itu.

1. Apa itu fake news dan apa bahayanya?

Jawaban: Berita palsu yang bisa menyesatkan, membentuk opini salah, atau menyebabkan konflik.

1. Bagaimana cara menjadi pengguna internet yang bertanggung jawab?

Jawaban: Gunakan dengan bijak, jangan menyebar kebencian, dan lindungi privasi.

1. Apa yang bisa kamu lakukan untuk membantu orang lain lebih aman di dunia digital?

Jawaban: Beri informasi yang benar, ajak mereka berhati-hati, dan laporkan hal mencurigakan bersama.

101. Apa itu phishing di media sosial?

Jawaban: Penipuan dengan menyamar sebagai akun resmi untuk mencuri data pribadi kita.

102. Mengapa tidak boleh membagikan OTP (kode sekali pakai)?

Jawaban: Karena bisa digunakan orang lain untuk masuk ke akunmu tanpa izin.

103. Bagaimana cara mengetahui kalau aplikasi itu mengandung virus?

Jawaban: Aplikasi tidak dari toko resmi, banyak izin aneh, dan bikin HP lemot atau eror.

104. Kenapa penting membedakan akun pribadi dan akun publik?

Jawaban: Agar informasi pribadi tidak mudah diakses semua orang.

105. Apa itu ‘digital footprint positif’?

Jawaban: Jejak online yang menunjukkan hal baik, seperti prestasi, karya, atau sikap sopan.

106. Apa tanda-tanda seseorang sedang mengalami cyberbullying?

Jawaban: Tiba-tiba murung, menarik diri, takut buka HP, atau sedih setelah online.

107. Apa tindakan yang harus diambil jika kamu melihat teman jadi korban perundungan online?

Jawaban: Dukung dia, jangan diam, bantu laporkan ke pihak berwenang.

108. Apa itu VPN dan kapan sebaiknya digunakan?

Jawaban: Alat untuk menyamarkan koneksi internet agar lebih aman, dipakai saat akses jaringan publik.

109. Mengapa kita tidak boleh asal ikut challenge di media sosial?

Jawaban: Karena beberapa challenge berbahaya atau menyebarkan konten negatif.

110. Bagaimana cara aman menyimpan kata sandi?

Jawaban: Gunakan pengelola kata sandi (password manager) dan jangan ditulis sembarangan.

111. Apa itu clickbait dan bagaimana cara menghindarinya?

Jawaban: Judul yang dibuat heboh untuk menarik klik, tapi isinya menyesatkan. Jangan langsung percaya dan baca sumbernya dulu.

112. Apa risiko terlalu sering menggunakan kamera online tanpa pengawasan?

Jawaban: Bisa direkam diam-diam atau disalahgunakan.

113. Apa manfaat mengikuti akun edukasi digital di media sosial?

Jawaban: Menambah pengetahuan tentang keamanan internet dan jadi lebih bijak online.

114. Kenapa harus log out dari akun saat selesai menggunakannya di perangkat umum?

Jawaban: Supaya orang lain tidak bisa mengakses akunmu.

115. Bagaimana cara menghadapi hoax yang menyangkut nama baik seseorang?

Jawaban: Jangan ikut sebar, bantu klarifikasi, dan laporkan ke platform.

116. Apa itu ‘2FA’ dan kenapa penting?

Jawaban: Verifikasi dua langkah, membuat akun lebih aman meski password bocor.

117. Apa yang harus diperhatikan sebelum install game atau aplikasi baru?

Jawaban: Cek izin aplikasi, rating, komentar, dan sumber unduhan.

118. Mengapa penting mengenali tanda-tanda kecanduan internet?

Jawaban: Supaya bisa mengontrol diri sebelum berdampak buruk pada kesehatan dan kehidupan sosial.

119. Apa yang dimaksud dengan etika digital?

Jawaban: Aturan dan sikap sopan yang harus diikuti saat beraktivitas di dunia digital.

120. Bagaimana peran teman sebaya dalam menjaga keamanan digital?

Jawaban: Saling mengingatkan, berbagi informasi aman, dan mendukung jika ada masalah online.

121. Apa bahaya menerima file dari orang asing di internet?

Jawaban: File tersebut bisa mengandung virus atau program berbahaya.

122. Mengapa harus berhati-hati dengan aplikasi yang meminta terlalu banyak izin?

Jawaban: Karena bisa menyalahgunakan data pribadi kita.

123. Apa itu spam dan kenapa harus dihindari?

Jawaban: Pesan berulang yang tidak penting dan bisa membawa virus atau penipuan.

124. Bagaimana cara melindungi akun dari pencurian?

Jawaban: Gunakan kata sandi kuat dan aktifkan verifikasi dua langkah.

125. Apa yang harus dilakukan jika akun media sosial diretas?

Jawaban: Segera ubah kata sandi, keluar dari semua perangkat, dan laporkan ke platform.

126. Kenapa tidak boleh membuka lampiran email dari pengirim tak dikenal?

Jawaban: Karena bisa berisi malware atau program jahat.

127. Apa itu cyberstalking?

Jawaban: Mengikuti seseorang secara terus-menerus di dunia maya hingga membuat korban tidak nyaman atau takut.

128. Apa itu digital detox dan manfaatnya?

Jawaban: Istirahat dari internet untuk menjaga kesehatan mental dan fisik.

129. Apa yang dimaksud dengan keamanan siber?

Jawaban: Upaya melindungi data dan aktivitas digital dari serangan atau pencurian.

130. Kenapa kita harus peduli dengan kebijakan privasi aplikasi?

Jawaban: Agar tahu data apa saja yang dikumpulkan dan bagaimana digunakan.

131. Apa yang dimaksud dengan identitas digital?

Jawaban: Segala informasi tentang diri kita yang ada di internet.

132. Bagaimana cara menghindari jebakan quiz palsu online?

Jawaban: Jangan ikut jika minta data pribadi atau terlihat mencurigakan.

133. Apa saja contoh data pribadi yang tidak boleh dibagikan sembarangan?

Jawaban: Nama lengkap, alamat rumah, nomor HP, dan akun media sosial.

134. Apa itu scam investasi digital?

Jawaban: Penipuan berkedok investasi yang menjanjikan keuntungan besar tapi tidak nyata.

135. Kenapa remaja rentan menjadi korban kejahatan siber?

Jawaban: Karena sering aktif online tapi belum sepenuhnya sadar risiko digital.

136. Bagaimana cara mengetahui kalau sebuah situs web aman?

Jawaban: Cek apakah alamatnya diawali dengan 'https://' dan ada ikon gembok.

137. Apa peran keluarga dalam menjaga keamanan digital anak muda?

Jawaban: Memberi bimbingan, pengawasan, dan dukungan saat ada masalah.

138. Kenapa kita harus membatasi informasi pribadi di bio akun publik?

Jawaban: Agar tidak dimanfaatkan oleh orang jahat.

139. Apa dampak negatif terlalu banyak mengonsumsi konten negatif online?

Jawaban: Bisa membuat stres, cemas, atau punya pandangan buruk terhadap diri sendiri dan orang lain.

140. Bagaimana cara menyampaikan kampanye keamanan digital ke teman sebaya?

Jawaban: Buat konten edukatif yang menarik, mudah dipahami, dan relevan dengan kehidupan mereka.

141. Apa itu doxing dan mengapa berbahaya?

Jawaban: Mengungkap data pribadi seseorang di internet tanpa izin yang bisa membahayakan korban.

142. Mengapa penting memperbarui perangkat lunak secara rutin?

Jawaban: Agar perangkat tetap aman dari celah keamanan yang lama.

143. Apa itu cyber grooming?

Jawaban: Proses pendekatan oleh pelaku jahat untuk membangun hubungan lalu memanipulasi korban secara online.

144. Bagaimana cara menghindari pencurian identitas digital?

Jawaban: Jangan bagikan data pribadi dan gunakan sistem keamanan yang kuat.

145. Apa itu konten palsu atau deepfake?

Jawaban: Video atau suara palsu yang dibuat menggunakan teknologi untuk menipu orang.

146. Apa tindakan bijak jika mendapat komentar jahat di media sosial?

Jawaban: Jangan balas dengan emosi, laporkan, dan blokir akunnya.

147. Kenapa kita harus selektif memilih teman di media sosial?

Jawaban: Karena tidak semua orang di internet memiliki niat baik.

148. Bagaimana cara mengetahui kalau sebuah informasi itu hoaks?

Jawaban: Cek di situs cek fakta, cari sumber terpercaya, dan lihat tanggalnya.

149. Apa dampak negatif oversharing di internet?

Jawaban: Data bisa disalahgunakan atau membuat kita jadi target penipuan.

150. Kenapa harus waspada dengan akun giveaway palsu?

Jawaban: Karena biasanya dibuat untuk mencuri data atau menipu pengguna.

151. Apa itu malware?

Jawaban: Program jahat yang bisa merusak sistem atau mencuri data dari perangkat kita.

152. Bagaimana cara menjaga keamanan saat menggunakan Wi-Fi publik?

Jawaban: Gunakan VPN, hindari login akun penting, dan matikan auto-connect.

153. Mengapa harus hati-hati dengan pop-up mencurigakan saat browsing?

Jawaban: Karena bisa berisi tautan berbahaya atau program jahat.

154. Apa itu fake account?

Jawaban: Akun palsu yang dibuat untuk menipu atau menyamar sebagai orang lain.

155. Apa yang harus dilakukan jika melihat penyebaran konten kekerasan online?

Jawaban: Laporkan ke platform dan jangan ikut menyebarkan.

156. Kenapa harus membaca review sebelum unduh aplikasi?

Jawaban: Untuk mengetahui apakah aplikasi itu aman dan terpercaya.

157. Apa manfaat membatasi screen time?

Jawaban: Agar hidup lebih seimbang dan tidak kecanduan gadget.

158. Apa itu bot dan bagaimana bisa berdampak di media sosial?

Jawaban: Akun otomatis yang bisa menyebar spam, hoaks, atau memanipulasi opini.

159. Bagaimana cara membangun citra digital yang baik?

Jawaban: Posting hal positif, sopan, dan tunjukkan karakter baik secara konsisten.

160. Mengapa penting mendiskusikan keamanan digital di sekolah?

Jawaban: Agar semua pelajar sadar risiko online dan tahu cara menghadapinya.

161. Apa itu ransomware?

Jawaban: Jenis malware yang mengunci data korban dan meminta tebusan agar bisa dibuka kembali.

162. Mengapa tidak boleh menyebarkan informasi pribadi teman tanpa izin?

Jawaban: Karena itu melanggar privasi dan bisa berbahaya bagi teman kita.

163. Apa yang dimaksud dengan kebocoran data?

Jawaban: Ketika informasi pribadi bocor dan bisa diakses oleh pihak yang tidak berwenang.

164. Bagaimana cara mengetahui aplikasi palsu di toko aplikasi?

Jawaban: Cek nama pengembang, ulasan negatif, dan jumlah unduhan yang tidak wajar.

165. Apa itu keamanan berlapis?

Jawaban: Menggunakan lebih dari satu cara perlindungan seperti password dan verifikasi dua langkah.

166. Kenapa jangan asal klik link dari pesan tidak dikenal?

Jawaban: Link bisa mengarah ke situs palsu atau memasang malware.

167. Apa manfaat belajar literasi digital sejak remaja?

Jawaban: Agar lebih bijak, aman, dan bertanggung jawab saat menggunakan internet.

168. Bagaimana cara menghindari kecanduan game online?

Jawaban: Atur waktu bermain, fokus ke kegiatan lain, dan minta dukungan keluarga.

169. Apa itu jejak digital negatif?

Jawaban: Informasi buruk yang kita tinggalkan di internet dan bisa merugikan kita di masa depan.

170. Kenapa harus hati-hati berbagi foto atau video pribadi?

Jawaban: Karena bisa disebar tanpa izin dan berdampak buruk pada diri kita.

171. Apa yang harus dilakukan jika mendapat pesan ancaman online?

Jawaban: Jangan panik, simpan bukti, dan segera laporkan ke orang dewasa atau pihak berwajib.

172. Apa itu spyware?

Jawaban: Perangkat lunak jahat yang diam-diam memantau aktivitas kita dan mencuri data.

173. Mengapa kita harus menjaga etika dalam grup chat?

Jawaban: Agar komunikasi tetap sehat, nyaman, dan tidak merugikan orang lain.

174. Apa itu akun palsu yang berpura-pura jadi selebriti?

Jawaban: Akun yang menyamar untuk menipu pengikut atau mendapatkan uang secara ilegal.

175. Bagaimana cara menghindari penipuan di toko online?

Jawaban: Cek ulasan toko, pastikan situsnya aman, dan jangan tergiur harga murah.

176. Apa itu rekam layar diam-diam dan bahayanya?

Jawaban: Merekam aktivitas orang tanpa izin yang bisa disalahgunakan untuk menyebarkan privasi.

177. Apa pentingnya mengenali hoaks seputar kesehatan di internet?

Jawaban: Agar tidak termakan informasi salah yang bisa membahayakan diri sendiri dan orang lain.

178. Kenapa tidak boleh menggunakan jaringan Wi-Fi tanpa izin?

Jawaban: Itu bisa melanggar hukum dan membahayakan keamanan perangkat kita.

179. Apa itu rekayasa sosial dalam kejahatan siber?

Jawaban: Manipulasi psikologis agar korban memberikan informasi penting secara sukarela.

180. Bagaimana cara membangun komunitas digital yang sehat?

Jawaban: Saling mendukung, menyebar kebaikan, dan tidak menyebarkan kebencian.

181. Apa itu phising?

Jawaban: Upaya penipuan untuk mencuri data pribadi dengan menyamar sebagai pihak terpercaya.

182. Kenapa penting membedakan akun asli dan akun palsu?

Jawaban: Agar tidak tertipu oleh penipuan atau informasi palsu.

183. Bagaimana cara membuat password yang kuat?

Jawaban: Gunakan kombinasi huruf besar, kecil, angka, dan simbol.

184. Apa itu cyberbullying?

Jawaban: Tindakan menyakiti orang lain melalui media digital seperti komentar jahat atau ejekan online.

185. Apa yang harus dilakukan jika jadi korban peretasan akun?

Jawaban: Segera ubah password, keluar dari semua perangkat, dan laporkan ke penyedia layanan.

186. Apa peran antivirus dalam keamanan digital?

Jawaban: Melindungi perangkat dari virus, malware, dan ancaman lainnya.

187. Kenapa penting memperbarui sistem dan aplikasi secara rutin?

Jawaban: Agar celah keamanan ditutup dan perangkat tetap aman.

188. Apa itu verifikasi dua langkah?

Jawaban: Fitur keamanan tambahan yang meminta kode selain password saat login.

189. Kenapa harus waspada terhadap giveaway palsu?

Jawaban: Karena bisa digunakan untuk mencuri data atau menipu uang.

190. Apa saja contoh perilaku berbahaya di internet?

Jawaban: Membuka situs ilegal, menyebar hoaks, atau membully orang lain.

191. Bagaimana cara menjaga identitas digital tetap aman?

Jawaban: Hindari membagikan data pribadi sembarangan dan aktifkan fitur keamanan.

192. Apa itu malware?

Jawaban: Perangkat lunak berbahaya yang bisa merusak atau mencuri data di perangkat kita.

193. Apa yang dimaksud dengan kebijakan privasi aplikasi?

Jawaban: Aturan tentang bagaimana aplikasi mengumpulkan dan menggunakan data pengguna.

194. Mengapa remaja mudah jadi sasaran penipuan online?

Jawaban: Karena belum semua memahami cara kerja keamanan digital.

195. Apa yang harus dilakukan sebelum mengunggah sesuatu ke media sosial?

Jawaban: Pikirkan dampaknya dan pastikan tidak membahayakan diri sendiri atau orang lain.

196. Apa itu DDoS?

Jawaban: Serangan yang membuat sebuah layanan online tidak bisa diakses dengan membanjiri trafik palsu.

197. Bagaimana cara melindungi akun media sosial?

Jawaban: Gunakan password kuat, verifikasi dua langkah, dan logout dari perangkat umum.

198. Apa itu spam?

Jawaban: Pesan yang tidak diinginkan dan biasanya berisi promosi atau penipuan.

199. Apa yang dimaksud dengan jejak digital positif?

Jawaban: Hal-hal baik yang kita tinggalkan di internet seperti prestasi atau karya.

200. Bagaimana peran keluarga dalam menjaga keamanan digital remaja?

Jawaban: Membimbing, memberi pengawasan, dan menjadi tempat curhat yang aman.