DOKUMEN SOFTWARE REQUIREMENTS SPECIFICATION (SRS)/SPESIFIKASI KEBUTUHAN PERANGKAT LUNAK (SKPL)

Nama Kelompok :

Mochammad Riky Hidayat	(2408561090)
Kadek Pasek Divandra Kusuma	(2408561069)
Made Mahatmika Adriananda Kusuma	(2408561045)
I Kadek Candra Gunawan	(2408561057)
I Gede Arya Kesha Narendra Subirman	(2408561048)

PROGRAM STUDI SARJANA INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS UDAYANA

JIMBARAN

2025

ABSTRAK

Phisfence adalah ekstensi browser yang berfungsi untuk mendeteksi dan mencegah pengguna mengakses situs phishing. Sistem ini bekerja secara preventif dengan menganalisis URL (alamat domain, elemen halaman (DOM)) serta pola berbahaya menggunakan rule-based detection dan machine learning (XGBoost). Ekstensi ini ditujukan untuk pengguna internet umum agar lebih aman dalam beraktivitas di dunia maya, terutama saat membuka tautan dari media sosial atau platform berbagi konten.

1. PENDAHULUAN

1.1 Kegunaan

Dokumen ini berfungsi sebagai panduan formal bagi pengembang, penguji, dan stakeholder dalam memahami kebutuhan sistem PhishFence. Dokumen ini disusun untuk mendefinisikan rincian kebutuhan perangkat lunak PhisFence, sebuah ekstensi google (browser extension) yang berfungsi untuk mendeteksi (secara realtime) dan mencegah pengguna mengakses situs web berbahaya atau phishing.

1.2 **Tujuan**

Menjelaskan kebutuhan perangkat lunak ekstensi browser PhishFence yang mendeteksi domain berbahaya dan halaman phishing melalui inspeksi struktur web dan pemodelan data.

1.3 Daftar Istilah

Istilah	Arti
Phishing	Upaya menipu pengguna agar memberikan data sensitif seperti password atau kartu kredit.
Frontend/Ekstensi	Bagian antarmuka yang berjalan di peramban pengguna.
URL	Alamat unik di internet yang digunakan untuk menemukan dan mengakses sumber

	daya seperti halaman web, gambar, video, atau file lainnya.
DOM (Document Object Model)	Struktur elemen dalam halaman web yang dapat dianalisis oleh script.
XGBoost	Algoritma machine learning yang digunakan untuk model klasifikasi URL.
Endpoint	Titik akses API untuk komunikasi antara ekstensi dan server.
Blocklist	Daftar domain atau URL yang diketahui berbahaya.
ML (Machine Learning)	Model pembelajaran mesin untuk deteksi pola phishing.

1.4 Rujukan

- IEEE Std 830-1998 – Recommended Practice for Software Requirements Specifications
- Dokumen teknis Manifest V3 – Google Chrome Extension API
- Dataset phising (kaggle), PhishTank dan OpenPhish (referensi domain berbahaya)

1.5 Sistematika

Dokumen ini disusun berdasarkan standar IEEE 830 untuk melakukan pendekatan analisis kebutuhan perangkat lunak yang meliputi deskripsi umum sistem, analisis kebutuhan fungsional dan nonfungsional, serta model interaksi data.

2. DESKRIPSI UMUM PERANGKAT LUNAK

Perangkat lunak PhishFence, sebuah ekstension (browser extension) yang mendeteksi dan memperingatkan pengguna/user terhadap situs phishing secara real-time. Phisfence terdiri dari 2 komponen yang saling berinteraksi yaitu :

- Ekstensi Browser (Client) : Berjalan di peramban pengguna (Chrome), berfungsi sebagai antarmuka untuk menerima input URL dan menampilkan peringatan.

- Server Backend (Server): Aplikasi berbasis Python (FastAPI) yang menjalankan model AI (XGBoost) untuk menganalisis karakteristik URL dan menentukan tingkat keamanannya. Sistem ini menggunakan basis data lokal (SQLite) untuk menyimpan riwayat pemindaian.

2.1 Perspektif Produk

Produk ini bernama PhishFence, yaitu plug-in atau ekstensi Google Chrome yang dikembangkan untuk mendeteksi situs web berbahaya, khususnya phishing. PhishFence berperan sebagai lapisan keamanan tambahan (plug-in) yang aktif memantau URL yang sedang diakses oleh pengguna, kemudian menganalisisnya dengan menggunakan model deteksi berbasis *machine learning* (XGBoost) serta database situs berbahaya terkini.

Ketika pengguna membuka sebuah tautan (misalnya dari pesan langsung di media sosial seperti Instagram atau WhatsApp), PhishFence akan secara otomatis memeriksa kredibilitas situs tersebut. Jika ditemukan indikasi phishing seperti panjang url aneh(abnormal url) , domain mencurigakan, pola halaman penipuan, atau tautan tiruan dari situs populer sistem akan menampilkan peringatan sebelum pengguna melanjutkan akses.

Dengan demikian, PhishFence tidak hanya berfungsi sebagai alat pendeteksi, tetapi juga sebagai sarana edukasi untuk meningkatkan kesadaran keamanan siber di kalangan pengguna internet.

2.2 Fungsi Produk

Fungsi utama dari PhishFence dirancang untuk memberikan perlindungan otomatis dan notifikasi interaktif kepada pengguna tanpa mengganggu aktivitas berselancar di internet. Fitur-fitur utama antara lain:

1. Analisis URL Otomatis
   Setiap kali pengguna mengunjungi situs baru, sistem akan memeriksa URL tersebut melalui algoritma XGBoost, model akan memprediksi apakah URL aman (Legitimate) atau berbahaya (Phising) berdasarkan 22 ekstraksi fitur URL.
2. Peringatan Dini (Early Warning System)
   Jika terdeteksi indikasi phishing, ekstensi akan menampilkan pop-up peringatan dengan tingkat risiko (rendah, sedang, tinggi) disertai rekomendasi untuk tidak melanjutkan akses.

3. Manajemen Whitelist

   PhisFence Memastikan domain populer dan terpercaya tidak salah dideteksi sebagai ancaman.

4. Integrasi Media Sosial

   PhishFence mampu mengenali tautan eksternal dari media sosial seperti Instagram, Facebook, atau Twitter yang sering digunakan sebagai sarana penyebaran phishing.

5. Pelaporan Situs (User Report System)

   Pengguna dapat melaporkan situs mencurigakan secara manual. Laporan ini akan dikirim ke server untuk divalidasi dan digunakan sebagai data pelatihan tambahan bagi sistem deteksi.

6. Dasbor Aktivitas & Riwayat Pemindaian

   Menyediakan tampilan riwayat situs yang pernah diperingatkan dan statistik situs phishing yang ditemukan.

2.3 Pemakai

PhishFence dirancang agar dapat digunakan oleh berbagai jenis pengguna, dari individu hingga institusi.

2.3.1 Administrator Sistem (System Administrator)

Pengguna dengan hak akses tertinggi yang mengelola konfigurasi ekstensi dan basis data situs phishing. (jika ingin di deploy ke server jadi sifatnya close-source)

Peran:

1. Mengelola daftar situs phishing & whitelist yang diverifikasi
2. Memperbarui model deteksi dan konfigurasi server
3. Memantau laporan pengguna dan statistik deteksi global.

Karakteristik Umum:

Melatih model, Mengelola Data Base, dan Menjaga Server Tetap Aktif

2.3.2 Pengguna Umum (End User)

Pengguna internet yang memasang ekstensi ini di peramban Chrome untuk melindungi diri dari ancaman phishing.

Peran:

1. Menginstal ekstensi dari Chrome Web Store.
2. Mendapatkan peringatan otomatis saat membuka situs mencurigakan.

3. Melaporkan situs yang dianggap berpotensi berbahaya.

Karakteristik Umum:

1. Tidak perlu latar belakang teknis.
2. Menginginkan perlindungan sederhana, otomatis, dan ringan tanpa konfigurasi kompleks.

2.4 Batasan-Batasan

1. PhishFence hanya berfungsi pada peramban Google Chrome (atau browser berbasis Chromium).
2. Sistem memerlukan koneksi internet aktif untuk melakukan pembaruan database situs phishing. (jika Phisfence dideploy ke server)
3. Sistem backend harus berjalan secara lokal (localhost) pada port 8000 agar ekstensi dapat berfungsi. (jika Phisfence berjalan di localhost)
4. Deteksi phising berbasis *machine learning* memiliki tingkat akurasi tinggi, tetapi tidak 100%. Potensi *false positive* (situs aman terdeteksi berbahaya) tetap ada, oleh karena itu kami disini menambahkan whitelist.
5. Ekstensi tidak memblokir situs secara permanen, tetapi hanya memberikan peringatan kepada pengguna.
6. Ekstensi tidak memantau aktivitas pribadi pengguna (seperti isi pesan, data akun, atau kata sandi).

2.5 Asumsi dan Ketergantungan

1. Sistem diasumsikan berjalan pada lingkungan browser dengan versi terbaru.
2. Pengguna telah menginstal Python dan dependensi yang diperlukan (urlib,pandas, dan numpy).
3. Server pusat yang menyimpan database situs phishing berjalan pada infrastruktur cloud dengan REST API untuk komunikasi ekstensi. (jika Phisfence di deploy)
4. Pengguna diasumsikan memiliki pemahaman dasar untuk menginstal ekstensi dari Chrome Web Store.
5. Pengembangan menggunakan metode Agile-Prototype Iteratif untuk fleksibilitas dan efisiensi.

3. DEFINISI KEBUTUHAN PERANGKAT LUNAK

3.1 Kebutuhan Antarmuka Eksternal

3.1.1 Antarmuka Pemakai

Tampilan utama berupa popup browser extension dan halaman peringatan (alert). Popup Ekstensi menampilkan:

- Tab Dashboard: Menampilkan statistik (Total Scan, Threats Blocked, Accuracy) dan daftar history yang menampilkan URL terakhir yang di-scan.
- Tab Cek URL: Input teks untuk memasukkan URL manual dan tombol "Check Now". Menampilkan hasil berupa kartu status (Aman/Waspada/Bahaya).
- Tab Fitur Proteksi : Menampilkan modul yang aktif dan nonaktif.
- Tab Pengaturan: Opsi untuk mengaktifkan/menonaktifkan modul proteksi.

Halaman Peringatan	:	Halaman HTML khusus yang memblokir akses pengguna ketika URL berbahaya terdeteksi, dengan opsi "Kembali ke Aman" atau "Lanjutkan (Tidak Disarankan)".

3.1.2 Antarmuka Perangkat Keras

Sistem Phisfence bisa bekerja pada perangkat keras speksifikasi minimalnya :

- Processor : i3-2120 (3.3Ghz)
- Memory RAM : 4GB
- Harddisk : Minimal 2 GB Tersedia
- Spesifikasi Recomended :
- Processor : i5-11400H (4.4 Ghz)
- Memory RAM : 8GB
- Harddisk : 10 GB Tersedia

3.1.3 Antarmuka Perangkat Lunak

Sistem Operasi : Windows, MacOS, atau Linux

Front-End (Browser Extension)

- Google Chrome Extension API (Manifest V3)
- HTML5
- CSS3
- JavaScript (ES6+)

Menggunakan HTTP/HTTPS untuk pembaruan data blocklist dan sinkronisasi laporan pengguna.

Back-End (Server)

- Python 3.x
- FastAPI
- Uvicorn
- SQLite

Artificial Intelligence & Data Processing

- XGBoost
- Scikit-Learn
- Pandas
- NumPy

3.1.4 Antarmuka Komunikasi

Komunikasi antar client dan server menggunakan REST API melalui HTTP, dengan format pertukaran datanya adalah JSON

3.2 Kebutuhan Fungsional

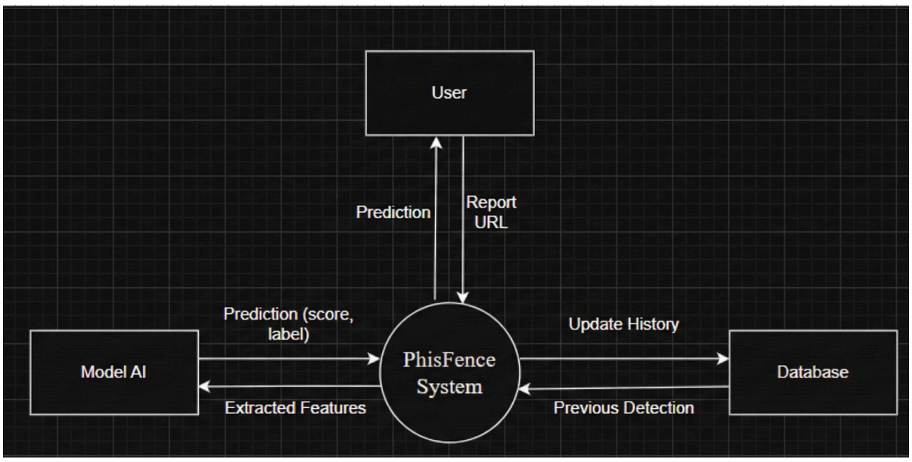
3.2.1 Deskripsi Kebutuhan Fungsional

ID	Nama Fungsi	Deskripsi	Input	Output
F-001	Predict URL	Memproses URL untuk menentukan apakah situs tersebut aman atau berbahaya menggunakan model XGBoost.	Link URL Website	Status Keamanan (Aman / Phishing) dan Skor Resiko
F-002	Get Stats	Menampilkan ringkasan aktivitas keamanan pengguna, seperti jumlah link yang discan dan ancaman yang digagalkan.	Permintaan Data Statistik	Jumlah Scan Hari Ini, Total Ancaman, dan Akurasi
F-003	Save History	Menyimpan setiap aktivitas	Data Hasil	Konfirmasi

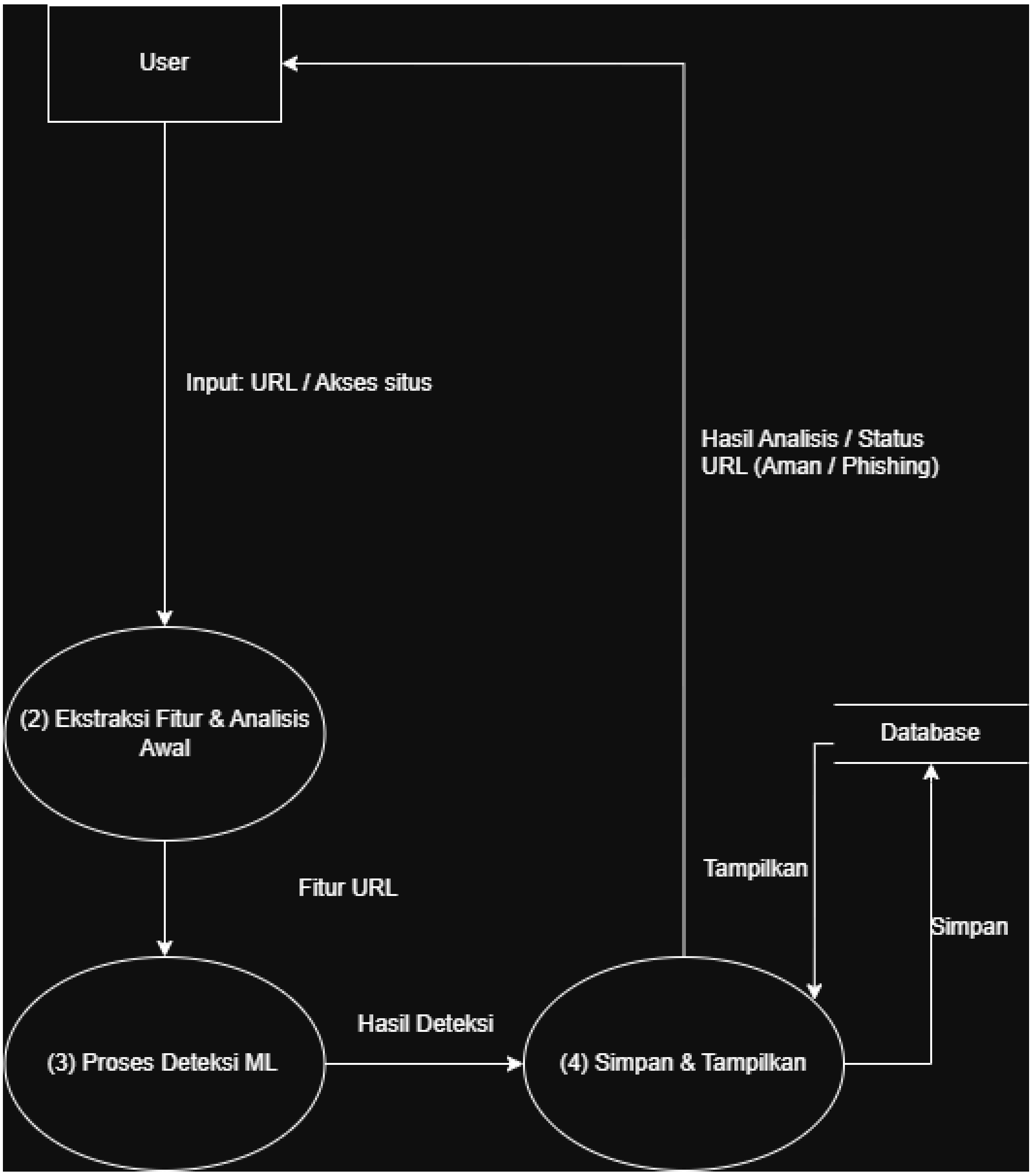
		pengecekan URL secara otomatis ke dalam catatan riwayat lokal.	Scan (URL & Status)	Penyimpanan Data
F-004	Get History	Mengambil dan menampilkan daftar situs-situs terakhir yang pernah diperiksa oleh pengguna.	Permintaan Data Riwayat	Daftar 10 Aktivitas Scan Terakhir
F-005	Delete History	Membersihkan seluruh catatan riwayat pengecekan URL dari penyimpanan untuk menjaga privasi pengguna.	Perintah Hapus	Pesan Konfirmasi Penghapusan
F-006	Whitelist Check	Memeriksa apakah situs yang dikunjungi termasuk dalam daftar situs terpercaya resmi (seperti Google, Facebook) untuk menghindari salah blokir.	Nama Domain Website	Status Terdaftar (Ya/Tidak) di Daftar Putih

3.2.2 Data Flow Diagram

3.2.2.1 Context Diagram



3.2.2.2 Data Flow Diagram (Level 1)



3.2.3 Data Dictionary

User Data Dictionary (local-storage)

Key	Tipe Data	Deskripsi
moduleStates	Object (JSON)	Menyimpan status On/Off fitur modular yang dipilih user.
moduleStates.toggle-realtime	Boolean	true jika perlindungan Real-time aktif, false jika mati.

moduleStates.toggle-blocking	Boolean	true jika fitur akses blokir aktif.

Backend

Nama Atribut	Tipe Data	Format	Deskripsi
id	INTEGER	PRIMARY KEY, AUTOINCREMENT	Penanda unik (Primary Key) untuk setiap baris data riwayat. dibuat otomatis.
url	TEXT	NOT NULL	Alamat website lengkap yang dipindai pengguna.
result	TEXT	-	Label hasil prediksi. Nilai: 'Legitimate' (Aman) atau 'Phishing' (Berbahaya).
probability	FLOAT	Range: 0.0 - 1.0	Skor kepercayaan model AI. Semakin mendekati 0 semakin phishing, diatas 0.5 & mendekati 1 semakin aman.
timestamp	DATETIME	YYYY-MM-DD HH:MM:SS	Waktu dan tanggal ketika proses scanning dilakukan.

Input Model AI UR

No	Nama Fitur	Tipe Data	Deskripsi Lengkap
1	URLLength	INTEGER	Jumlah total karakter dalam URL.
2	DomainLength	INTEGER	Jumlah karakter pada nama domain
3	TLDLength	INTEGER	Panjang Top-Level Domain

4	NoOfImage	INTEGER	Jumlah tag <img> dalam halaman.
5	NoOfJS	INTEGER	Jumlah file JavaScript eksternal yang dipanggil.
6	NoOfCSS	INTEGER	Jumlah file CSS yang dipanggil..
7	NoOfSelfRef	INTEGER	Jumlah link/anchor (<a>) yang mengarah ke halaman yang sama (Self-Referencing Links).
8	NoOfExternalRef	INTEGER	Jumlah link yang mengarah ke domain lain (keluar).
9	IsHTTPS	INTEGER (0/1)	Status protokol keamanan. 1 jika HTTPS, 0 jika HTTP biasa.
10	HasObfuscation	INTEGER (0/1)	1 jika URL menggunakan teknik pengaburan (misalnya @ atau hex code).
11	HasTitle	INTEGER (0/1)	1 jika halaman memiliki tag <title>.
12	HasDescription	INTEGER (0/1)	1 jika halaman memiliki meta description.
13	HasSubmitButton	INTEGER (0/1)	1 jika ada tombol <input type="submit"> atau <button>.
14	HasSocialNet	INTEGER (0/1)	1 jika ditemukan link menuju sosial media (FB, Twitter, dll).
15	HasFavicon	INTEGER (0/1)	1 jika website memuat ikon favicon.
16	HasCopyrightInfo	INTEGER (0/1)	1 jika ditemukan teks seperti "Copyright", "©", atau "All rights reserved".
17	popUpWindow	INTEGER (0/1)	1 jika halaman memicu popup window otomatis.

18	Iframe	INTEGER (0/1)	1 jika halaman menggunakan <iframe> .
19	Abnormal_URL	INTEGER (0/1)	1 jika hostname bagian dari URL tidak cocok dengan standar umum.
20	LetterToDigitRatio	FLOAT	Rasio jumlah huruf dibagi jumlah angka.
21	Redirect_0	INTEGER (0/1)	Variabel dummy untuk status redirect (Tidak ada redirect/Normal).
22	Redirect_1	INTEGER (0/1)	Variabel dummy untuk status redirect (Ada redirect mencurigakan).

3.2.4 Process Specification

Awalnya user akan menginputkan secara manual atau langsung membuka tab. Perbedaan yang ada di keduanya hanya di input nya saja jadi secara skenario dan pengambilan keputusan akan sama saja.

Setelah user membuka/menginputkan url, front end akan mengirim url itu ke server (backend) dan di backend url itu akan di ekstract fitur fiturnya. Setelah mengekstrak model akan memberikan hasil (probabilitas) & Legitimate/Phising.

Hasil dari backend akan dikirim ke frontend dan ditampilkan ke user, dari sini user bisa memilih apakah ingin lanjut (jika percaya) atau ingin kembali (jika takut).

3.3 Kebutuhan Performansi

Kami memastikan agar sistem bisa bekerja dengan cepat & akurat jadi kebutuhan performansi nya adalah waktu respon & akurasi. Kami mengharapkan ekstensi ini mampu menampilkan hasil analisis URL dalam waktu kurang dari 2 detik. Dan kami juga berharap agar model bisa memiliki akurasi diatas 90%.

3.4 Kebutuhan Lain

User harus menginstal ini dengan cara menload di Google Ekstension secara lokal, yaitu dengan mengaktifkan mode developer dan klik “load unpacked” di Chrome Developer Mode. Untuk backup data ekstensi (preferensi), user akan menyimpan data secara lokal menggunakan API di browser pengguna, jadi selagi tidak dihapus ekstensi nya maka settingan preferensi pengguna akan tetap aman (ini tidak berlaku jika user berpindah device).