Lampiran 1. Lembar Kesediaan Bimbingan

SURAT KESEPAKATAN BIMBINGAN SKRIPSI

Kami yang bertanda tangan dibawah ini:

Pihak Pertama

Nama	: Fajri Abdul Ghani
NIM	: 21090067
Program Studi	: Sarjana Terapan Teknik Informatika

Pihak Kedua

Nama	: M. Nishom, S.Kom., M.Kom.
Status	: Dosen
NIDN	: 0619048701
Jabatan Fungsional	: Lektor
Pangkat/Golongan	: Penata /III/C

Pada hari ini Jumat tanggal 07 Maret 2025 telah terjadi sebuah kesepakatan bahwa Pihak Kedua bersedia menjadi Pembimbing II Skripsi Pihak Pertama dengan syarat Pihak Pertama wajib melakukan bimbingan Skripsi minimal 8 kali kepada Pihak Kedua. Adapun waktu dan tempat pelaksanaan disepakati antar pihak.

Demikian kesepakatan ini dibuat dengan penuh kesadaran guna kelancaran penyelesaian Skripsi

Tegal, 07 Maret 2025

Pihak Pertama	Pihak Kedua
Fajri Abdul Ghani	M. Nishom, S.Kom., M.Kom.

Mengetahui
Ketua Program Studi Sarjana Terapan Teknik Informatika

Dyah Apriliani, S.T., M.Kom.
NIPY. 09.015.225

Lampiran 2. Surat Pernyataan Pengajuan HKI

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini, pemegang hak cipta:

1. Nama : Fajri Abdul Ghani
   Kewarganegaraan : Indonesia
   Alamat : Desa Pakijangan RT.001/003, Kecamatan Bulakamba, Kabupaten Brebes, Provinsi Jawa Tengah, 52253
2. Nama : Dega Surono Wibowo, S.T., M.Kom.
   Kewarganegaraan : Indonesia
   Alamat : Perumahan Sapphire Regency Blok H, No.1, RT.004, RW.001, Kelurahan Pulosari, Kecamatan Brebes, 52213
3. Nama : M. Nishom, S.Kom., M.Kom.
   Kewarganegaraan : Indonesia
   Alamat : Jl. Jepara, Perumahan Griya Putri Land Blok A6, RT 03/04, Margadana, Tegal, 52143

Dengan ini menyatakan bahwa:

1. Karya Cipta yang saya mohonkan:
   Berupa : Program Komputer
   Berjudul : Aplikasi Deteksi URL Phishing Berbasis Machine Learning Dengan Catboost Classifier
   - Tidak meniru dan tidak sama secara esensial dengan Karya Cipta milik pihak lain atau obyek kekayaan intelektual lainnya sebagaimana dimaksud dalam Pasal 68 ayat (2);
   - Bukan merupakan Ekspresi Budaya Tradisional sebagaimana dimaksud dalam Pasal 38;
   - Bukan merupakan Ciptaan yang tidak diketahui penciptanya sebagaimana dimaksud dalam Pasal 39;
   - Bukan merupakan hasil karya yang tidak dilindungi Hak Cipta sebagaimana dimaksud dalam Pasal 41 dan 42;
   - Bukan merupakan Ciptaan seni lukis yang berupa logo atau tanda pembeda yang digunakan sebagai merek dalam perdagangan barang/jasa atau digunakan sebagai lambang organisasi, badan usaha, atau badan hukum sebagaimana dimaksud dalam Pasal 65 dan;
   - Bukan merupakan Ciptaan yang melanggar norma agama, norma susila, ketertiban umum, pertahanan dan keamanan negara atau melanggar peraturan perundang-undangan sebagaimana dimaksud dalam Pasal 74 ayat (1) huruf d Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

2. Sebagai pemohon mempunyai kewajiban untuk menyimpan asli contoh ciptaan yang dimohonkan dan harus memberikan apabila dibutuhkan untuk kepentingan penyelesaian sengketa perdata maupun pidana sesuai dengan ketentuan perundang-undangan.

3. Karya Cipta yang saya mohonkan pada Angka 1 tersebut di atas tidak pernah dan tidak sedang dalam sengketa pidana dan/atau perdata di Pengadilan.

4. Dalam hal ketentuan sebagaimana dimaksud dalam Angka 1 dan Angka 3 tersebut di atas saya / kami langgar, maka saya / kami bersedia secara sukarela bahwa:
   a. permohonan karya cipta yang saya ajukan dianggap ditarik kembali; atau
   b. Karya Cipta yang telah terdaftar dalam Daftar Umum Ciptaan Direktorat Hak Cipta, Direktorat Jenderal Hak Kekayaan Intelektual, Kementerian Hukum Dan Hak Asasi Manusia R.I dihapuskan sesuai dengan ketentuan perundang-undangan yang berlaku.
   c. Dalam hal kepemilikan Hak Cipta yang dimohonkan secara elektronik sedang dalam berperkara dan/atau sedang dalam gugatan di Pengadilan maka status kepemilikan surat pencatatan elektronik tersebut ditangguhkan menunggu putusan Pengadilan yang berkekuatan hukum tetap.

Demikian Surat pernyataan ini saya/kami buat dengan sebenarnya dan untuk dipergunakan sebagimana mestinya.

Tegal, 26 Juni 2025

Fajri Abdul Ghani
Pemegang Hak Cipta*

Dega Surono Wibowo, S.T., M.Kom
Pemegang Hak Cipta*

M. Nishom, S.Kom., M.Kom.
Pemegang Hak Cipta*

Lampiran 3. Surat Pengalihan HKI

SURAT PENGALIHAN HAK CIPTA

Yang bertanda tangan di bawah ini :

1. Nama : Fajri Abdul Ghani
   Kewarganegaraan : Indonesia
   Alamat : Desa Pakijangan RT.001/003, Kecamatan Bulakamba, Kabupaten Brebes, Provinsi Jawa Tengah, 52253

2. Nama : Dega Surono Wibowo, S.T., M.Kom.
   Kewarganegaraan : Indonesia
   Alamat : Perumahan Sapphire Regency Blok H, No.1, RT.004, RW.001, Kelurahan Pulosari, Kecamatan Brebes, 52213

3. Nama : M. Nishom, S.Kom., M.Kom.
   Kewarganegaraan : Indonesia
   Alamat : Jl. Jepara, Perumahan Griya Putri Land Blok A6, RT 03/04, Margadana, Tegal, 52143

Adalah **Pihak I** selaku pencipta, dengan ini menyerahkan karya ciptaan saya kepada :

Nama : Pusat Penelitian dan Pengabdian Masyarakat (P3M)
Alamat : Jl. Mataram No. 9 Pesurungan Lor Tegal

Adalah **Pihak II** selaku Pemegang Hak Cipta berupa Program Komputer dengan judul**"Aplikasi Deteksi URL Phishing Berbasis Machine Learning Dengan Catboost Classifier"** untuk didaftarkan di Direktorat Hak Cipta dan Desain Industri, Direktorat Jenderal Kekayaan Intelektual, Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia.

Demikianlah surat pengalihan hak ini kami buat, agar dapat dipergunakan sebagaimana mestinya.

Tegal, 26 Juni 2025

Pemegang Hak Cipta
Kepala P3M

(Muhammad Fikri Hidayattullah, S.T., M.Kom.)

Pencipta

(Fajri Abdul Ghani)

(Dega Surono Wibowo, S.T., M.Kom.)

(M. Nishom, S.Kom., M.Kom.))

Lampiran 4. Syarat Pengajuan HKI

DAFTAR ISI

DAFTAR GAMBAR

PENDAHULUAN

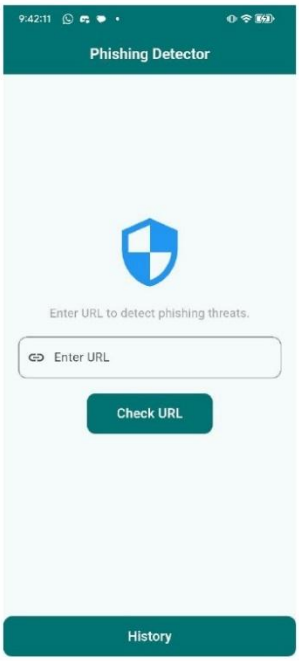
Selamat datang di SeClick - Phishing Detector, sebuah aplikasi yang dirancang untuk membantu Anda mendeteksi dan menghindari ancaman phishing dari tautan (URL) yang beredar secara daring. Dalam era digital yang semakin maju, serangan phishing menjadi salah satu ancaman serius yang dapat mencuri data pribadi, mengakses akun penting, dan menyebabkan kerugian besar bagi individu maupun organisasi.

SeClick hadir sebagai solusi praktis dan cepat bagi Anda yang ingin tetap aman saat menjelajahi internet, menerima pesan dari media sosial, email, atau aplikasi chatting lainnya. Melalui tampilan yang sederhana, Anda cukup memasukkan atau menyalin tautan ke dalam aplikasi ini, dan SeClick akan langsung menganalisis serta memberikan hasil berupa persentase kemungkinan apakah tautan tersebut aman atau berisiko.

Dirancang khusus untuk pengguna dari berbagai kalangan, SeClick memadukan teknologi pintar dengan kemudahan penggunaan. Aplikasi ini dilengkapi dengan fitur pemindaian otomatis dari clipboard maupun notifikasi, serta riwayat pemeriksaan yang bisa ditinjau kembali kapan saja. SeClick berkomitmen untuk menjadi asisten keamanan digital Anda yang responsif dan terpercaya, kapan pun Anda membutuhkannya. oleh pengguna umum, orang tua, tenaga kerja, maupun siswa/mahasiswa yang sering menerima tautan melalui media sosial atau aplikasi chat. Dengan antarmuka yang ramah dan proses deteksi cepat, Phishing Detector hadir sebagai solusi modern untuk meningkatkan kewaspadaan digital masyarakat terhadap ancaman siber berbasis tautan.

TAMPILAN AWAL

Saat Anda pertama kali menggunakan aplikasi Phishing Detector, Anda akan langsung diarahkan ke tampilan utama seperti yang ditunjukkan pada gambar berikut:



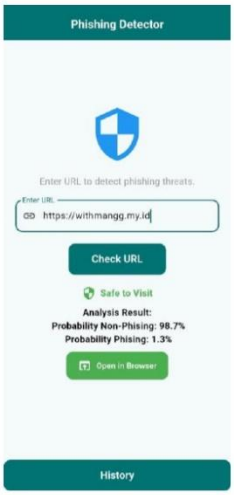
Gambar 1. Halaman Awal Aplikasi

Pada halaman ini, Anda akan melihat logo berbentuk perisai berwarna biru yang merepresentasikan keamanan dan perlindungan. Di bawah logo tersebut, terdapat kolom untuk memasukkan tautan (URL) yang ingin Anda periksa.

PENGGUNAAN APLIKASI

Untuk memulai proses deteksi phishing, pengguna dapat mengikuti langkah-langkah berikut pada halaman utama aplikasi:

1. Buka aplikasi **Phishing Detector**.
2. Pada halaman awal, Anda akan melihat kolom bertuliskan **"Enter URL"**.
3. Ketik atau tempel tautan (URL) yang ingin Anda analisis ke dalam kolom tersebut.
4. Tekan tombol **"Check URL"** untuk memulai proses pemeriksaan.
5. Tunggu beberapa saat hingga hasil analisis ditampilkan di layar.



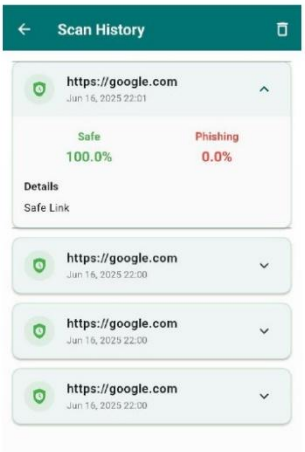
Gambar 2. Halaman Input URL

Hasil analisis akan ditampilkan dalam bentuk dua nilai persentase, yaitu **Probability Non-Phishing** yang menunjukkan seberapa besar kemungkinan URL tersebut aman, dan **Probability Phishing** yang menunjukkan seberapa besar kemungkinan URL tersebut mengandung ancaman phishing. Kedua nilai ini bertujuan untuk membantu pengguna dalam mengambil keputusan, apakah akan membuka atau menghindari tautan tersebut. Semakin tinggi nilai **Probability Phishing**, maka semakin besar pula potensi bahaya dari URL yang diperiksa.

HALAMAN SCAN HISTORY

Setiap URL yang telah diperiksa akan otomatis tersimpan di halaman Scan History. Halaman ini menampilkan daftar tautan beserta tanggal dan waktu analisis. Pengguna dapat mengetuk salah satu entri untuk melihat detail hasilnya, termasuk:

- Probability Non-Phishing: persentase kemungkinan URL aman.
- Probability Phishing: persentase kemungkinan URL berbahaya.
- Details: ringkasan seperti "Safe Link" atau "Potentially Dangerous Link".



Gambar 3. Halaman Scan History

Fitur ini sangat berguna bagi pengguna yang ingin melacak kembali link-link yang pernah diperiksa sebelumnya, baik untuk tujuan keamanan pribadi maupun untuk evaluasi lebih lanjut.

FITUR NOTIFIKASI DETEKSI

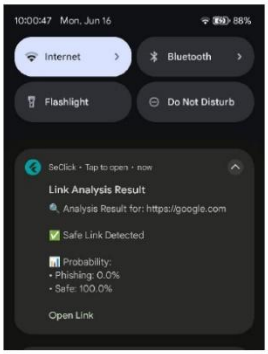
Aplikasi Phishing Detector dilengkapi dengan fitur notifikasi otomatis yang bekerja di latar belakang. Fitur ini memungkinkan aplikasi mendeteksi tautan mencurigakan secara real-time dari pesan yang masuk di berbagai aplikasi seperti WhatsApp, Telegram, atau media sosial lainnya.

Cara Kerja:

- Saat perangkat menerima pesan yang berisi URL (misalnya dari WhatsApp),
- Aplikasi secara otomatis akan mengekstrak tautan tersebut **tanpa perlu dibuka atau disentuh oleh pengguna**,
- Proses analisis berjalan di latar belakang,
- Hasil analisis akan langsung muncul dalam bentuk notifikasi.

Isi Notifikasi:

- **URL yang terdeteksi**
- **Status deteksi** (misalnya: ✅ Safe Link Detected atau ⚠️ Potential Phishing Detected)
- **Persentase**: menampilkan Probability Phishing dan Probability Non-Phishing
- **Tombol**: opsi "Open Link" jika pengguna tetap ingin membukanya



Gambar 4. Notifikasi Otomatis dari Hasil Deteksi

Dengan fitur ini, pengguna mendapatkan perlindungan ekstra tanpa harus membuka aplikasi. Proses ini berlangsung secara pasif dan efisien, memastikan setiap tautan yang masuk dapat segera dianalisis untuk mencegah potensi ancaman.

PEMECAH MASALAH

1. **Notifikasi Tidak Muncul**
    a. Periksa Izin Notifikasi: Pastikan aplikasi memiliki izin untuk menampilkan notifikasi di pengaturan perangkat.
    b. Periksa Mode Hemat Daya: Beberapa perangkat membatasi aktivitas aplikasi di latar belakang saat mode hemat baterai aktif. Nonaktifkan mode tersebut jika perlu.
2. **Tautan Tidak Terdeteksi Otomatis**
    a. Periksa Izin Akses Notifikasi: Pastikan izin untuk membaca notifikasi dari aplikasi lain (seperti WhatsApp atau Telegram) telah diberikan.
    b. Restart Aplikasi: Coba tutup dan buka kembali aplikasi agar layanan latar belakang aktif kembali.
3. **Aplikasi Tidak Menampilkan Hasil Analisis**
    a. Periksa Koneksi Internet: Pastikan perangkat Anda terhubung ke jaringan internet yang stabil.
    b. Ulangi Pemeriksaan URL: Coba masukkan ulang URL secara manual dan tekan "Check URL".
4. **Hasil Analisis Terlalu Lama Muncul**
    a. Server Lambat atau Sibuk: Tunggu beberapa saat dan coba kembali, bisa jadi server sedang memproses banyak permintaan.
    b. Perbarui Aplikasi: Gunakan versi terbaru dari aplikasi untuk performa yang lebih baik.

TEKNIKAL
BOOK

SECLICK

APLIKASI DETEKSI URL PHISHING

FAJRI ABDUL GHANI

DEGA SURONO WIBOWO, S.T., M.KOM.

M. NISHOM, S.KOM., M.KOM.

1. SOURCE CODE BACKEND (FLASK)

1.1 API Utama untuk Deteksi URL

Kode ini adalah inti dari sistem backend. Endpoint /predict menerima URL dari frontend, mengekstrak fiturnya, dan mengirim hasil klasifikasi kembali ke frontend.

```python
@api_v1_blueprint.route("/predict", methods=["POST"])
def predict():
    app.logging.info("Request prediction incoming...")
    data = request.get_json()
    url = data.get("url")
    result = detect_phishing(url)

    print(result)

    return jsonify(result)
```

- Menerima permintaan JSON berisi URL.
- Memanggil detect_phishing(url) dari detection_service.py.
- Mengembalikan hasil klasifikasi phishing.

1.2 Load Model dan Fitur Ekstraksi

Model CatBoost diload dari file .pkl, dan fungsi extract_features dipanggil untuk menghasilkan array fitur numerik dari URL.

📍 File: detection_service.py

```python
# Load model menggunakan pickle
with open(MODEL_PATH, "rb") as f:
    model = pickle.load(f)
```

Ekstraksi Fitur:

```python
obj = FeatureExtraction(url)
features = obj.getFeaturesList()  # Return 30+ fitur
```

2. SOURCE CODE FRONTEND (FLUTTER)

2.1 Halaman Utama (HomePage.dart)

Halaman ini merupakan **UI utama** dari aplikasi SECLICK yang memungkinkan pengguna:

- Memasukkan URL secara manual.

- Mendeteksi URL dari clipboard.
- Mendeteksi URL dari notifikasi.
- Melihat hasil klasifikasi secara langsung.
- Menyalin, membuka, atau menyimpan URL yang telah dianalisis.

1. Input URL dan Tombol "Check URL"

```
child: TextField(
  controller: _urlController,
  decoration: InputDecoration(
    labelText: "Enter URL",
    labelStyle: const TextStyle(fontFamily: 'Lato'),
    hintText: "https://example.com",
    border: OutlineInputBorder(
      borderRadius: BorderRadius.circular(12),
    ), // OutlineInputBorder
    prefixIcon: const Icon(Icons.link),
```

📌 TextField digunakan untuk menerima URL dari pengguna

```
ElevatedButton(
  onPressed: _isLoading ? null : _checkURL,
  style: ElevatedButton.styleFrom(
    backgroundColor: const Color(0xFF027373),
    padding: const EdgeInsets.symmetric(horizontal: 40, vertical: 14),
    shape: RoundedRectangleBorder(
      borderRadius: BorderRadius.circular(12),
    ), // RoundedRectangleBorder
  ),
  child: _isLoading
      ? const CircularProgressIndicator(color: Colors.white)
      : const Text(
          "Check URL",
          style: TextStyle(
            fontFamily: 'Lato',
            fontSize: 18,
            fontWeight: FontWeight.w600,
            color: Colors.white,
          ), // TextStyle
        ), // Text
), // ElevatedButton
```

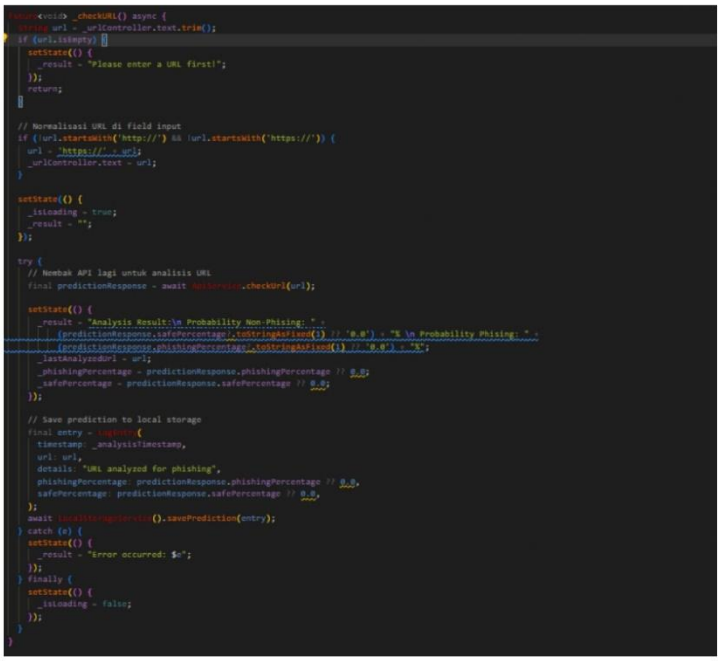
📌 Tombol “Check URL” memicu pemanggilan fungsi _checkURL() untuk mengirim URL ke backend.

```
startClipboardWatcher();  // Mendeteksi URL dari clipboard
initPlatformState();      // Mengaktifkan listener notifikasi
```

📌 Fungsi ini dijalankan di initState() dan membuat proses input URL lebih otomatis.

2.2 Fungsi Deteksi URL

Fungsi ini mengirimkan URL ke backend Flask, lalu menerima dan menampilkan hasilnya.

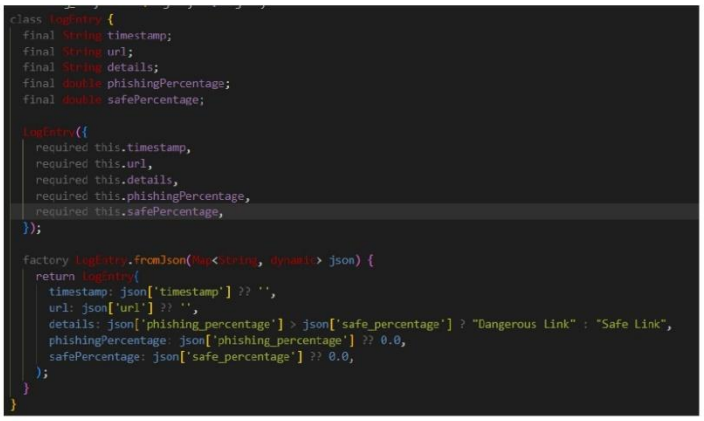


2.3 Penyimpanan Riwayat dengan Hive

Data hasil deteksi disimpan secara lokal menggunakan Hive, yang memungkinkan akses offline.

Struktur Data (Model)

LogEntry di Flutter, digunakan untuk menyimpan **hasil deteksi phishing URL**. Berikut adalah penjelasan kode tersebut secara lengkap:

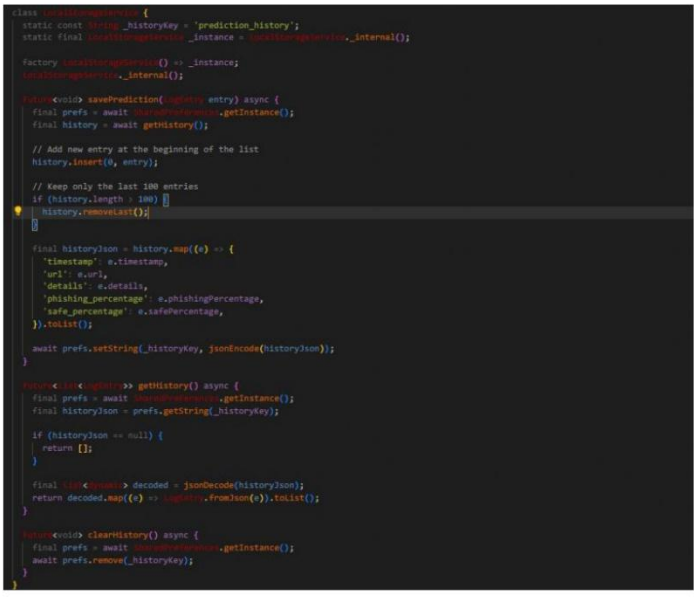


```dart
class LogEntry {
  final String timestamp;
  final String url;
  final String details;
  final double phishingPercentage;
  final double safePercentage;

  LogEntry({
    required this.timestamp,
    required this.url,
    required this.details,
    required this.phishingPercentage,
    required this.safePercentage,
  });

  factory LogEntry.fromJson(Map<String, dynamic> json) {
    return LogEntry(
      timestamp: json['timestamp'] ?? '',
      url: json['url'] ?? '',
      details: json['phishing_percentage'] > json['safe_percentage'] ? "Dangerous Link" : "Safe Link",
      phishingPercentage: json['phishing_percentage'] ?? 0.0,
      safePercentage: json['safe_percentage'] ?? 0.0,
    );
  }
}
```

Local Storage Service



```dart
class LocalStorageService {
  static const String _historyKey = 'prediction_history';
  static final LocalStorageService _instance = LocalStorageService._internal();

  factory LocalStorageService() => _instance;
  LocalStorageService._internal();

  Future<void> savePrediction(LogEntry entry) async {
    final prefs = await SharedPreferences.getInstance();
    final history = await getHistory();

    // Add new entry at the beginning of the list
    history.insert(0, entry);

    // Keep only the last 100 entries
    if (history.length > 100) {
      history.removeLast();
    }

    final historyJson = history.map((e) => {
      'timestamp': e.timestamp,
      'url': e.url,
      'details': e.details,
      'phishing_percentage': e.phishingPercentage,
      'safe_percentage': e.safePercentage,
    }).toList();

    await prefs.setString(_historyKey, jsonEncode(historyJson));
  }

  Future<List<LogEntry>> getHistory() async {
    final prefs = await SharedPreferences.getInstance();
    final historyJson = prefs.getString(_historyKey);

    if (historyJson == null) {
      return [];
    }

    final List<dynamic> decoded = jsonDecode(historyJson);
    return decoded.map((e) => LogEntry.fromJson(e)).toList();
  }

  Future<void> clearHistory() async {
    final prefs = await SharedPreferences.getInstance();
    await prefs.remove(_historyKey);
  }
}
```

kode dari LocalStorageService, yang menangani penyimpanan lokal hasil deteksi URL phishing menggunakan SharedPreferences di Flutter.

3. STRUKTUR DATABASE HIVE

Berikut adalah struktur penyimpanan data riwayat deteksi secara lokal:

No	Field	Tipe Data	Deskripsi
1.	url	String	Alamat URL yang dianalisis
2.	result	String	Hasil deteksi (phishing/aman)
3.	timestamp	DateTime	Waktu deteksi dilakukan
4.	phishing_percentage	double	Probabilitas bahwa URL termasuk phishing
5.	safe_percentage	double	Probabilitas bahwa URL aman

4. NOTIFIKASI OTOMATIS

Fitur notifikasi otomatis bertujuan untuk mendeteksi URL yang masuk dari notifikasi (seperti WhatsApp, SMS, atau browser) secara real-time, lalu mengirim hasil deteksi ke notifikasi lokal jika ditemukan URL mencurigakan.

4.1 Inisialisasi Listener

Mengaktifkan listener untuk menangkap **notifikasi dari sistem Android**, seperti WhatsApp, SMS, atau aplikasi lain yang berisi teks.

```
NotificationsListener.initialize(callbackHandle: _callback);
```

- Fungsi NotificationsListener.initialize() digunakan untuk **mendaftarkan callback** saat notifikasi masuk.
- Argumen callbackHandle menunjuk ke fungsi _callback yang akan dijalankan ketika ada notifikasi yang masuk.

4.2 Register Port untuk menerima data notifikasi

Membuat channel komunikasi antara **Isolate background** (tempat listener berjalan) dan **UI utama** aplikasi menggunakan ReceivePort.

```
// Create new port
port = ReceivePort();
IsolateNameServer.registerPortWithName(port!.sendPort, "_listener_");
port!.listen((message) => onData(message));
```

- ReceivePort dibuat agar Isolate dapat **menerima data dari background listener**.
- IsolateNameServer digunakan untuk **mendaftarkan port** agar bisa dipanggil dari static function (_callback).
- Fungsi port.listen(...) akan menjalankan fungsi onData(message) setiap kali ada notifikasi baru.

4.3 Callback Notifikasi

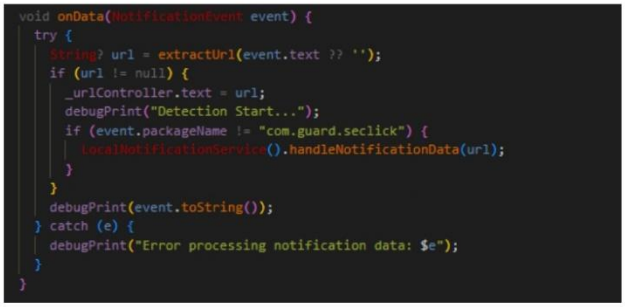
Fungsi ini dipanggil **otomatis oleh sistem** saat notifikasi masuk, dan digunakan untuk **mengirim data ke port utama**.

```
@pragma('vm:entry-point')
static void _callback(NotificationEvent evt) {
  try {
    debugPrint("send evt to ui: $evt");
    final SendPort? send = IsolateNameServer.lookupPortByName("_listener_");
    if (send == null) {
      debugPrint("can't find the sender");
      return;
    }
    send.send(evt);
  } catch (e) {
    debugPrint("Error in notification callback: $e");
  }
}
```

- Fungsi _callback **harus static dan diberi anotasi @pragma('vm:entry-point')**, karena akan dipanggil dari luar isolate utama.
- Ia akan mencari SendPort yang sudah didaftarkan dengan nama _listener_.
- Jika ditemukan, data NotificationEvent dikirim ke port tersebut.

4.4 Fungsi onData() – Memproses isi notifikasi

Menangani data yang dikirim dari listener (berisi teks notifikasi), **mencari URL**, dan **mengaktifkan deteksi phishing** jika URL ditemukan.



```
void onData(NotificationEvent event) {
  try {
    String? url = extractUrl(event.text ?? '');
    if (url != null) {
      _urlController.text = url;
      debugPrint("Detection Start...");
      if (event.packageName != "com.guard.seclick") {
        LocalNotificationService().handleNotificationData(url);
      }
    }
    debugPrint(event.toString());
  } catch (e) {
    debugPrint("Error processing notification data: $e");
  }
}
```

- event.text adalah isi notifikasi yang diterima.
- Fungsi extractUrl(...) digunakan untuk **mengambil link dari teks**.
- Jika URL valid dan bukan dari aplikasi sendiri, maka:
- Disimpan di TextField
- Fungsi LocalNotificationService().handleNotificationData(url) akan **melakukan analisis dan menampilkan notifikasi peringatan** jika berbahaya.

Lampiran 5. Sertifikat HKI Yang Terbit

REPUBLIK INDONESIA
KEMENTERIAN HUKUM

SURAT PENCATATAN CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC002025085070, 8 Juli 2025
Pencipta		
Nama	:	**Fajri Abdul Ghani, Dega Surono Wibowo, S.T., M.Kom. dkk**
Alamat	:	Desa Pakijangan RT.001/003, Bulakamba, Kab. Brebes, Jawa Tengah, 52253
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Pusat Penelitian dan Pengabdian Masyarakat (P3M) Politeknik Harapan Bersama**
Alamat	:	Jalan Mataram No. 9, Pesurungan Lor, Kecamatan Margadana, Margadana, Kota Tegal, Jawa Tengah, 52142
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Program Komputer**
Judul Ciptaan	:	**Aplikasi Deteksi URL Phishing Berbasis Machine Learning Dengan Catboost Classifier**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	8 Juli 2025, di Kota Tegal
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor Pencatatan	:	000925331

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM
DIREKTUR JENDERAL KEKAYAAN INTELEKTUAL
u.b
Direktur Hak Cipta dan Desain Industri

Agung Damarsasongko,SH.,MH.
NIP. 196912261994031001

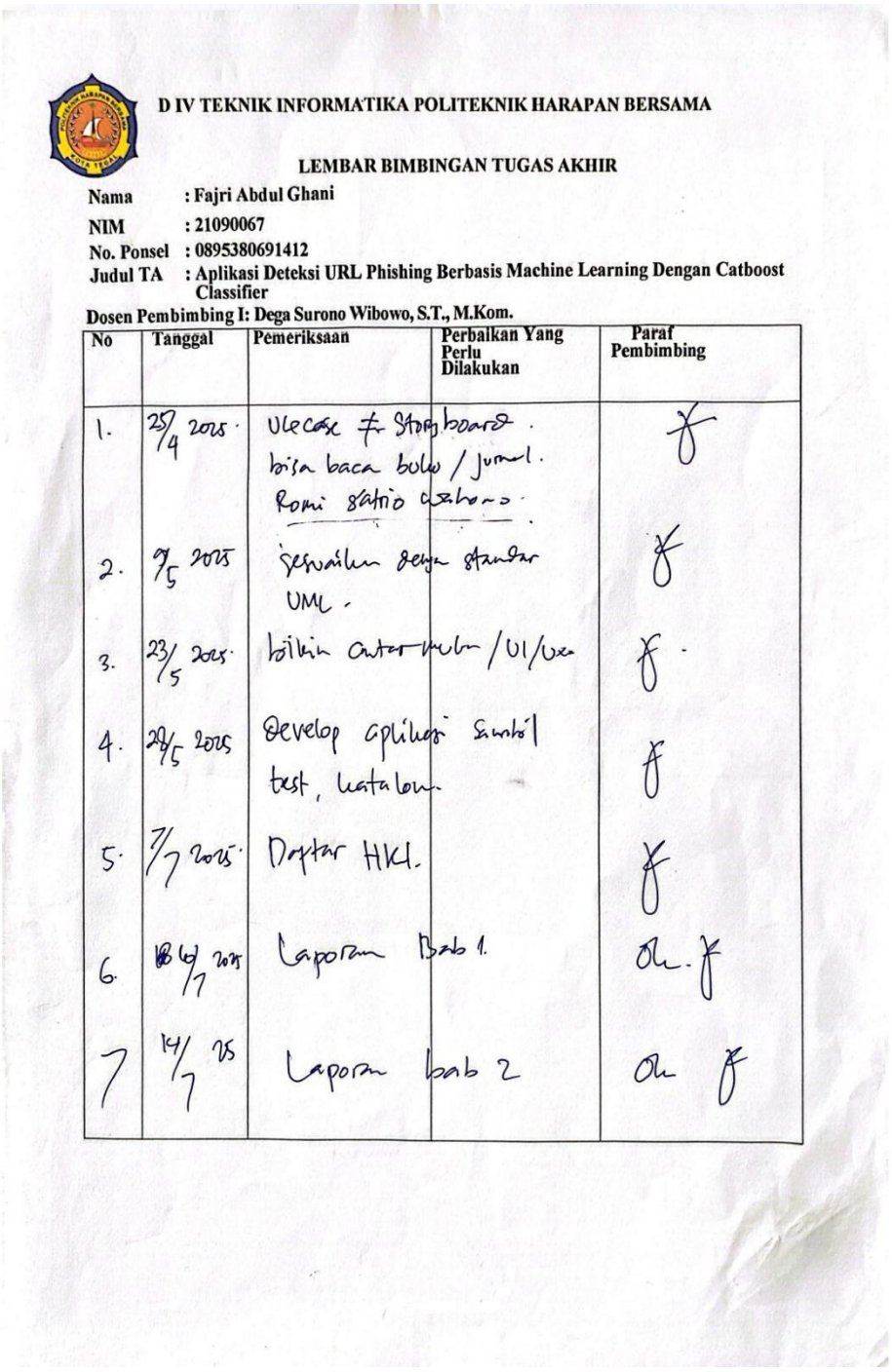
Balai Besar Sertifikasi Elektronik

Disclaimer:
1. Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.
2. Surat Pencatatan ini telah disegel secara elektronik menggunakan segel elektronik yang ditertibkan oleh Balai Besar Sertifikasi Elektronik, Badan Siber dan Sandi Negara.
3. Surat Pencatatan ini dapat dibuktikan keasliannya dengan memindai kode QR pada dokumen ini dan informasi akan ditampilkan dalam browser.

LAMPIRAN PENCIPTA

No	Nama	Alamat
1	Fajri Abdul Ghani	Desa Pakijangan RT.001/003 Bulakamba, Kab. Brebes
2	Dega Surono Wibowo, S.T., M.Kom.	Perumahan Sapphire Regency Blok H, No. 1, RT.004, RW.001, Kelurahan Pulosari Brebes, Kab. Brebes
3	M. Nishom, S.Kom., M.Kom.	Jl. Jepara, Perumahan Griya Putri Land Blok A6, RT 03/04, Margadana Margadana, Kota Tegal

Lampiran 6. Lembar Bimbingan



D IV TEKNIK INFORMATIKA POLITEKNIK HARAPAN BERSAMA

LEMBAR BIMBINGAN TUGAS AKHIR

Nama : Fajri Abdul Ghani

NIM : 21090067

No. Ponsel : 0895380691412

Judul TA : Aplikasi Deteksi URL Phishing Berbasis Machine Learning Dengan Catboost Classifier

Dosen Pembimbing I: Dega Surono Wibowo, S.T., M.Kom.

No	Tanggal	Pemeriksaan	Perbaikan Yang Perlu Dilakukan	Paraf Pembimbing
1.	25/4 2025	Usecase & Storyboard. bisa baca buku / jurnal. Romi satrio wahono.		
2.	9/5 2025	sesuaikan dengan standar UML.		
3.	23/5 2025	bikin antarmuka / UI/UX		
4.	29/5 2025	Develop aplikasi sambil test, katalog		
5.	7/7 2025	Daftar HKI.		
6.	8/7 2025	Laporan Bab 1.		
7	14/7 25	Laporan bab 2		

8.	16/7 25	Laporan	Ok	
9	18/7 25	Slah lan	Daftar	
			Acc 18/7 25	

Tegal, 18/7 2025
Dosen Pembimbing I

Dega Surono Wibowo, S.T., M.Kom.
NIPY. 06 .014.183

D IV TEKNIK INFORMATIKA
POLITEKNIK HARAPAN BERSAMA

LEMBAR BIMBINGAN TUGAS AKHIR

Nama : **Fajri Abdul Ghani**
NIM : **21090067**
No. Ponsel : **0895380691412**
Judul TA : **Aplikasi Deteksi URL Phishing Berbasis Machine Learning Dengan Catboost Classifier**
Dosen Pembimbing II : **M. Nishom, S.Kom., M.Kom.**

No	Tanggal	Pemeriksaan	Perbaikan Yang Perlu Dilakukan	Paraf Pembimbing
1.	3/6-2025	- Model	- Integrasikan model ke dalam aplikasi	
		- Dataset	- Tambahkan dataset URL dari url lokal (Indonesia) atau bisa mengajukan permohonan data ke kominfo terkait URL phishing + ekstrak data	
2.	26/6-2025	- sistem	- OK Lanjutkan pengujian sistem.	
		- Sarkom	- Lanjutkan untuk HKI - Minimal 2	

3.	10/7 - 2025	- Laporan.	- perbaiki sesuai catatan pada Laporan.	
4.	14/7 - 2025	- persiapan sidang	- persiapkan ppt. presentasi - Tools: persiapkan Vysor.	
5.	15/07 - 2025	- ppt. sidang	- perbaiki ppt sesuai catatan.	

Tegal, Juli 2025
Dosen Pembimbing II

M. Nishom, S.Kom., M.Kom.
NIPY. 09.017.337

Lampiran 7. Data Penelitian

No	Nama Fitur	Nilai -1	Nilai 0	Nilai 1
1.	UsingIP	Menggunakan IP Address (Phishing)	—	Tidak menggunakan IP (Aman)
2.	LongURL	URL sangat panjang (Phishing)	Netral	URL pendek (Aman)
3.	ShortURL	Menggunakan layanan pemendek URL	—	Tidak menggunakan pemendek URL
4.	Symbol@	Simbol @ digunakan (Phishing)	—	Simbol @ tidak digunakan
5.	Redirecting//	Redirect ganda ditemukan (Phishing)	—	Tidak ada redirect ganda
6.	PrefixSuffix-	Tanda - pada domain (Phishing)	—	Tidak ada tanda - pada domain
7.	SubDomains	Banyak subdomain (Phishing)	Subdomain moderat	Subdomain sedikit (Aman)
8.	HTTPS	Tidak menggunakan HTTPS	Netral	Menggunakan HTTPS
9.	DomainRegLen	Umur domain pendek (Phishing)	—	Umur domain panjang
10.	Favicon	Favicon tidak sesuai domain	—	Favicon berasal dari domain sendiri
11.	NonStdPort	Menggunakan port tidak standar	—	Menggunakan port standar
12.	HTTPSDomainURL	HTTPS muncul di URL tidak sesuai	—	HTTPS sesuai dan valid
13.	RequestURL	Banyak permintaan ke luar domain	—	Permintaan tetap dalam domain
14	AnchorURL	Banyak anchor link ke luar domain	—	Link anchor aman dan dalam domain
15	LinksInScriptTags	Banyak link skrip tidak aman	—	Link skrip aman
16	ServerFormHandler	Form dikirim ke domain berbeda	—	Form ditangani oleh domain sendiri

17	InfoEmail	Email langsung ditampilkan	—	Tidak menampilkan email
18	AbnormalURL	URL mencurigakan atau aneh	—	URL normal
19	WebsiteForwarding	Banyak redirect forwarding	—	Tidak ada forwarding
20	StatusBarCust	Mengubah status bar browser	—	Tidak mengubah status bar
21	DisableRightClick	Klik kanan dinonaktifkan	—	Klik kanan aktif
22	UsingPopupWindow	Sering membuka popup window	—	Tidak membuka popup
23	IframeRedirection	Menggunakan iframe mencurigakan	—	Tidak menggunakan iframe
24	AgeofDomain	Umur domain sangat pendek	—	Umur domain cukup
25	DNSRecording	Tidak ada rekaman DNS	—	Memiliki rekaman DNS
26	WebsiteTraffic	Lalu lintas sangat rendah	—	Lalu lintas tinggi
27	PageRank	PageRank rendah	—	PageRank tinggi
28	GoogleIndex	Tidak terindeks di Google	—	Terindeks di Google
29	LinksPointingToPage	Tidak ada link mengarah ke halaman	—	Banyak link menuju halaman
30	StatsReport	Terdeteksi mencurigakan di laporan	—	Tidak mencurigakan di laporan
31	class	Phishing	—	Aman (Legitimate)

Catatan:

- Tanda — berarti nilai itu **tidak digunakan** pada fitur tersebut (hanya -1 dan 1 saja).
- Jika dataset ada nilai 0, biasanya berarti **Netral** atau **tidak bisa dipastikan**.
- Tabel Mapping Nilai Numerik ke Deskripsi Semua Fitur
  Sumber Dataset https://www.kaggle.com/eswarchandt/phishing-website-detector