



**RANCANG BANGUN APLIKASI ANDROID PENDETEKSI
PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING**

SKRIPSI

FAIZ DAFFA MAKARIM

2210314097

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS TEKNIK

PROGRAM STUDI S1 TEKNIK ELEKTRO

2026



**RANCANG BANGUN APLIKASI ANDROID PENDETEKSI
PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING**

SKRIPSI

**Diajukan untuk Memenuhi Persyaratan dalam Memperoleh Gelar
Sarjana Teknik**

FAIZ DAFFA MAKARIM

2210314097

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS TEKNIK

PROGRAM STUDI S1 TEKNIK ELEKTRO

2026

HALAMAN PENGESAHAN PENGUJI

Skripsi yang diajukan oleh:

Nama : Faiz Daffa Makarim
NIM : 2210314097
Program Studi : SI – Teknik Elektro
Judul Skripsi : RANCANG BANGUN APLIKASI ANDROID
PENDETEKSI PHISHING DENGAN 3 ALGORITMA
MACHINE LEARNING

telah berhasil dipertahankan di hadapan tim penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Pembangunan Nasional Veteran Jakarta.



Dr. Muhamad Alif Razi, S.Pi., M.Sc.

Penguji Utama



Subekti Ari Santoso, S.T., M.Eng.

Penguji Lembaga



Silvia Anggraeni, S.T., M.Sc., Ph.D.

Penguji I (Pembimbing)



**Dr. Eng. Ir. Teguh Firmansyah, S.T.,
M.T., IPM**

**Pelaksana Tugas (Plt.) Dekan
Fakultas Teknik**



Luh Krisnawati, S.T., M.T.

**Koordinator Program Studi
Teknik Elektro**

Ditetapkan di: Jakarta

Tanggal Ujian: 16 Juli 2026

HALAMAN PENGESAHAN PEMBIMBING SKRIPSI

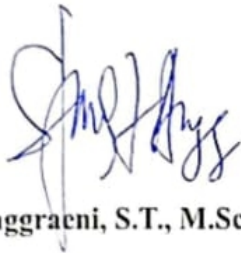
**RANCANG BANGUN APLIKASI ANDROID PENDETEKSI
PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING**

Faiz Daffa Makarim

NIM. 2210314097

Disetujui oleh,

Pembimbing I



Silvia Anggraeni, S.T., M.Sc., Ph.D.

Pembimbing II



Andhika Octa Indarso, M. MSI

Mengetahui,

Kepala Program Studi Teknik Elektro

Fakultas Teknik

Universitas Pembangunan Nasional Veteran Jakarta



Luh Krisnawati, S.T., M.T.

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini merupakan hasil karya sendiri dan semua sumber yang dikutip ataupun digunakan sebagai rujukan telah saya nyatakan benar.

Nama : Faiz Daffa Makarim

NIM : 2210314097

Program Studi : S1 – Teknik Elektro

Apabila di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 16 Juli 2026

Yang menyatakan,



Faiz Daffa Makarim

HALAMAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS

Sebagai *civitas academica* Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Faiz Daffa Makarim

NIM : 2210314097

Program Studi : S1 – Teknik Elektro

menyetujui untuk memberikan Hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

RANCANG BANGUN APLIKASI ANDROID PENDETEKSI PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING

Dengan Hak Bebas Royalti Non-eksklusif ini, Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih-media/formatkan, mengelola (dalam bentuk pangkalan data, merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan pemilik hak cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 16 Juli 2026

Yang menyatakan,



Faiz Daffa Makarim

RANCANG BANGUN APLIKASI ANDROID PENDETEKSI PHISHING DENGAN 3 ALGORITMA MACHINE LEARNING

Faiz Daffa Makarim

ABSTRAK

Phishing merupakan salah satu ancaman keamanan siber yang terus berkembang. Di saat yang sama, banyaknya penggunaan perangkat Android sebagai media layanan digital meningkatkan risiko serangan *phishing*. Penelitian ini bertujuan membandingkan performa algoritma *Long Short-Term Memory* (LSTM), *Random Forest*, dan *Extreme Gradient Boosting* (XGBoost) dalam mendeteksi URL *phishing* serta menganalisis performa layanan aplikasi Android yang mengimplementasikan model *machine learning* tersebut. Evaluasi model dilakukan menggunakan metrik akurasi, presisi, *recall*, dan *Area Under Curve* (AUC). Performa layanan aplikasi dievaluasi dengan parameter *response time*, *error rate*, dan *throughput*. Hasil penelitian menunjukkan bahwa XGBoost memberikan performa terbaik dengan akurasi 95,05%, presisi 96,78%, *recall* 93,20%, dan AUC 0,9902. Dari sisi layanan sistem Android, sistem mampu menangani seluruh skenario pengujian dengan *error rate* 0% dan tetap memberikan hasil deteksi *phishing* secara stabil. Hasil penelitian menunjukkan bahwa integrasi *machine learning* pada aplikasi Android dapat digunakan secara efektif untuk mendeteksi *phishing* dengan tingkat akurasi tinggi dan performa layanan yang baik.

Kata Kunci : Android, Deteksi *Phishing*, LSTM, *Machine Learning*, *Random Forest*, XGBoost.

DEVELOPMENT OF AN ANDROID-BASED PHISHING DETECTION APPLICATION USING THREE MACHINE LEARNING ALGORITHMS

Faiz Daffa Makarim

ABSTRACT

Phishing is one of the continuously evolving cybersecurity threats. At the same time, the use of Android devices as a platform for digital services increases the risk of phishing attacks. This study compares the performance of Long Short-Term Memory (LSTM), Random Forest, and Extreme Gradient Boosting (XGBoost) algorithms in detecting phishing URLs and to analyze the service performance of an Android application implementing these machine learning models. Model evaluation was conducted using accuracy, precision, recall, and Area Under the Curve (AUC) metrics. The application's service performance was evaluated using response time, error rate, and throughput parameters. The results show that XGBoost achieved the best performance with an accuracy of 95.05%, precision of 96.78%, recall of 93.20%, and an AUC score of 0.9902. From the Android system service perspective, the application successfully handled all testing scenarios with a 0% error rate and consistently delivered stable phishing detection results. The findings indicate that the integration of machine learning into Android applications can be effectively utilized for phishing detection, providing high classification accuracy and good service performance.

Keywords : *Android, Machine Learning, Phishing Detection, LSTM, Random Forest, XGBoost.*

KATA PENGANTAR

Puji dan syukur kepada Allah SWT yang memungkinkan penulis untuk menyelesaikan Tugas Akhir ini. Keberhasilan dari Tugas Akhir ini dapat terjadi dengan pengaruh dari beberapa pihak yang telah membantu penulis. Dengan ini, penulis ingin menyampaikan terima kasih kepada:

1. Allah SWT, yang telah memberi kesempatan kepada penulis untuk menyelesaikan Tugas Akhir ini.
2. Keluarga penulis, yang menjadi salah satu motivasi utama bagi penulis untuk menyelesaikan Tugas Akhir ini.
3. Ibu Luh Krisnawati, S.T., M.T., sebagai Koordinator Program Studi Teknik Elektro, Fakultas Teknik Universitas Pembangunan Nasional Veteran Jakarta.
4. Ibu Silvia Anggraeni, S.T., M.Sc., Ph.D., selaku Dosen Pembimbing I yang telah banyak memberikan saran konstruktif selama proses penulisan Tugas Akhir ini.
5. Bapak Andhika Octa Indarso, M. MSI, sebagai Dosen Pembimbing II yang telah memberikan berbagai masukan yang sangat penting.
6. Kepada sepuluh orang yang penulis temui di masa kuliah ini yang tidak bisa disebutkan namanya, terimakasih banyak karena telah menjadi inspirasi utama bagi penulis di masa kuliah ini. Terimakasih karena telah menjadi diri kalian sendiri.
7. Teman-teman di Program Studi S1 Teknik Elektro yang telah memberikan bantuan dalam penyusunan tugas akhir ini.

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan saran dan kritik konstruktif untuk perbaikan laporan ini. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca dan rekan-rekan mahasiswa, khususnya di Universitas Pembangunan Nasional Veteran Jakarta.

Jakarta, Juli 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN PENGUJI	ii
HALAMAN PENGESAHAN PEMBIMBING SKRIPSI	iii
HALAMAN PERNYATAAN ORISINALITAS	iv
HALAMAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xii
DAFTAR LAMPIRAN.....	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah	2
1.5 Sistematika Penulisan	3
BAB 2 TINJAUAN PUSTAKA	5
2.1 Penelitian Terdahulu	5
2.2 Landasan Teori	8
2.2.1 <i>Phishing</i>	8
2.2.2 Android	9
2.2.3 Algoritma <i>Machine Learning</i> LSTM.....	10
2.2.4 Algoritma <i>Machine Learning</i> <i>Random Forest</i>	12
2.2.5 Algoritma <i>Machine Learning</i> XGBoost	13
2.2.6 Mendeley Data	14
2.2.7 Virtual Studio Code	15
2.2.8 Android Studio.....	15
2.2.9 Kotlin	16
2.2.10 Railway	17
2.2.11 Apache JMeter	18
BAB 3 METODOLOGI PENELITIAN.....	19
3.1 Tahapan Penelitian.....	19
3.2 Pengumpulan dan Pembagian Data	21
3.3 Pelatihan Model	24

3.4 Integrasi Ke Aplikasi Android	26
3.5 Analisis Hasil	28
3.6 Jadwal Penelitian	29
BAB 4 HASIL DAN PEMBAHASAN.....	30
4.1 Algoritma <i>Machine Learning</i>	30
4.1.1 XGBoost	30
4.1.2 <i>Random Forest</i>	36
4.1.3 LSTM.....	40
4.2 Perbandingan Performa Model	45
4.3 Perbandingan Menggunakan Dataset Pribadi	46
4.4 Implementasi Model di Aplikasi.....	48
4.5 Pengujian Performa Sistem Dengan Apache JMeter	49
4.6 Hasil Akhir Model dan Aplikasi	52
BAB 5 PENUTUP	54
5.1 Kesimpulan	54
5.2 Saran	55
DAFTAR PUSTAKA	
DAFTAR RIWAYAT HIDUP	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 Cara Kerja Algoritma LSTM.....	11
Gambar 2.2 Analogi Cara Kerja Algoritma <i>Random Forest</i>	12
Gambar 2.3 Cara Kerja Algoritma XGBoost	14
Gambar 2.4 Tampilan Awal Apache JMeter	18
Gambar 3.1 <i>Flowchart</i> Penelitian.....	19
Gambar 4.1 Kode Pengunggahan Dataset Untuk XGBoost	30
Gambar 4.2 Kode Training Untuk XGBoost.....	31
Gambar 4.3 Kode Validasi Untuk XGBoost	32
Gambar 4.4 Kode Testing Untuk XGBoost.....	33
Gambar 4.5 Hasil Pengujian XGBoost.....	33
Gambar 4.6 <i>Confusion Matrix</i> XGBoost.....	34
Gambar 4.7 Grafik ROC Curve XGBoost.....	35
Gambar 4.8 Kode Pengunggahan Dataset Untuk <i>Random Forest</i>	36
Gambar 4.9 Kode Training Untuk <i>Random Forest</i>	36
Gambar 4.10 Kode Validasi Untuk <i>Random Forest</i>	37
Gambar 4.11 Kode Testing Untuk <i>Random Forest</i>	37
Gambar 4.12 Hasil Pengujian <i>Random Forest</i>	38
Gambar 4.13 <i>Confusion Matrix</i> <i>Random Forest</i>	38
Gambar 4.14 Grafik ROC Curve <i>Random Forest</i>	39
Gambar 4.15 Kode Pengunggahan Dataset Untuk LSTM.....	40
Gambar 4.16 Kode Training Untuk LSTM	40
Gambar 4.17 Kode Validasi Untuk LSTM.....	41
Gambar 4.18 Kode Testing Untuk LSTM	42
Gambar 4.19 Hasil Pengujian LSTM	42
Gambar 4.20 <i>Confusion Matrix</i> LSTM	43
Gambar 4.21 Grafik ROC Curve LSTM	44
Gambar 4.22 Tampilan Antarmuka Pengguna (<i>User Interface</i>) Aplikasi	48

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	5
Tabel 3.1 Tabel Rumus Metrik Evaluasi Model.....	20
Tabel 3.2 Contoh Data <i>Whitelist</i> dan <i>Blacklist</i>	21
Tabel 3.3 Contoh Proses <i>Encoding</i> URL	22
Tabel 3.4 Contoh Proses Ekstraksi Fitur	22
Tabel 3.5 Contoh Pembagian Dataset URL	23
Tabel 3.6 Contoh Dataset URL Baru	24
Tabel 3.7 Deskripsi Parameter Evaluasi Model	25
Tabel 3.8 Deskripsi Parameter Pengujian Performa.....	27
Tabel 3.9 <i>Timeline</i> Penelitian	29
Tabel 4.1 Tabel Perbandingan Performa Model.....	45
Tabel 4.2 Tabel Perbandingan Model pada URL <i>Phishing</i> Pribadi	46
Tabel 4.3 Tabel Perbandingan Model pada URL Aman Pribadi.....	46
Tabel 4.4 Hasil Pengujian Performa Sistem.....	49
Tabel 4.5 Hasil Grafik <i>Response Time</i> Pengujian Performa Sistem	51

DAFTAR LAMPIRAN

- Lampiran 1** Kode Pelatihan, Validasi, dan Testing Algoritma XGBoost
- Lampiran 2** Kode Pelatihan, Validasi, dan Testing Algoritma *Random Forest*
- Lampiran 3** Kode Pelatihan, Validasi, dan Testing Algoritma LSTM
- Lampiran 4** Hasil Simulasi Performa Sistem Pada Apache JMeter