

TUGAS AKHIR

**IMPLEMENTASI ALGORITMA *LIGHTGBM* DENGAN INTEGRASI
EXPLAINABLE AI DAN FITUR ANTI-*QUISHING* PADA SISTEM DETEKSI
URL PHISHING BERBASIS WEB**



MUH. ZAQI FIRDAUS

NPM : 22120029

Dosen Pembimbing :

Dr. TJATURSARI WIDIARTIN, S.Kom., M.Kom.

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS WIJAYA KUSUMA SURABAYA
2026**

LEMBAR PENGESAHAN

Tugas Akhir Disusun Untuk Memenuhi Salah Satu

Syarat Memperoleh Gelar

Sarjana Komputer (S.kom)

Di

Universitas Wiajaya Kusuma Surabaya

Oleh :

MUH ZAQI FIRDAUS
22120029

Hari / Tanggal Sidang : Kamis, 16 Juli 2026

Menyetujui,
Dosen Pembimbing


Dr. Tjatur Sari Widiartin, S.Kom., M.Kom.
NIK : 11540A-ET

Ketua Program Studi
Informatika


Nonot Wisnu Karyanto, ST., M.Kom.
NIK : 11563-ET

Dekan
Fakultas Teknik




Dr. H. Agung Kukuh Adisusilo, ST., MT.
NIP : 197802152015041001

LEMBAR PENGESAHAN REVISI

Judul : Implementasi Algoritma *LightGBM* dengan integrasi *Explainable AI* dan fitur
Anti-Quishing pada sistem deteksi URL Phishing berbasis Web
Nama : Muh. Zaqi Firdaus
NPM : 22120029

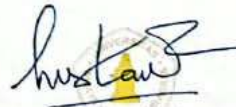
Telah Diuji Pada :

Hari : Kamis
Tanggal : 16 Juli 2026
Tempat : Ruang Asistensi Fakultas Teknik Universitas Wijaya Kusuma Surabaya

Disetujui Oleh,

Dosen Penguji I

Dosen Penguji II



Dr. Noven Indra Prasetya, S.kom. M.kom.
NIK 09414 - ET

Dr. Lestari Retnawati, S.Kom., M.MT.
NIK 16762A - ET

Mengetahui,
Dosen Pembimbing



Dr. Tjatusari Widiartin, S.Kom., M.Kom.
NIK 11540A - ET

PERNYATAAN KEASLIAN TULISAN

Yang bertanda tangan dibawah ini saya:

Nama : Muh. Zaqi Firdaus

NPM : 22120029

Program Studi : Informatika, Fakultas Teknik Universitas Wijaya Kusuma Surabaya

Menyatakan dengan sebenarnya bahwa Tugas Akhir yang saya tulis dengan judul Implementasi Algoritma LightGBM dengan Integrasi Explainable AI dan Fitur Anti-Quishing pada Sistem Deteksi URL Phishing Berbasis Web benar-benar hasil karya saya sendiri, bukan merupakan pengambilan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri. Apabila di kemudian hari dapat dibuktikan bahwa Tugas Akhir ini adalah hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Surabaya, 25 Juli 2026

Yang membuat pernyataan,



Muh. Zaqi Firdaus

IMPLEMENTASI ALGORITMA *LIGHTGBM* DENGAN INTEGRASI *EXPLAINABLE AI* DAN FITUR ANTI-*QUISHING* PADA SISTEM DETEKSI *URL PHISHING* BERBASIS *WEB*

Muh. Zaqi Firdaus

Program Studi Informatika Fakultas Teknik

Universitas Wijaya Kusuma Surabaya

muhzaqif@gmail.com

ABSTRAK

Perkembangan teknologi informasi berbasis *web* telah meningkatkan efisiensi layanan digital, namun di sisi lain juga memunculkan berbagai ancaman keamanan siber, salah satunya adalah serangan *phishing*, yaitu metode penipuan yang memanfaatkan *Uniform Resource Locator (URL)* berbahaya untuk memperoleh informasi sensitif pengguna. Selain *phishing* konvensional, muncul ancaman baru berupa *QR Code Phishing (Quishing)*, yaitu teknik *phishing* yang memanfaatkan *QR Code* untuk mengarahkan pengguna ke *URL* bahaya sehingga semakin sulit dikenali secara manual. Sistem deteksi berbasis aturan (*rule-based*) memiliki keterbatasan dalam menghadapi variasi pola serangan yang terus berkembang sehingga diperlukan pendekatan yang lebih adaptif melalui *Machine Learning*.

Penelitian ini bertujuan mengimplementasikan algoritma *Light Gradient Boosting Machine (LightGBM)* pada sistem deteksi *URL phishing* berbasis *web* secara *real-time*. Sistem juga mengintegrasikan *Explainable Artificial Intelligence (XAI)* atau kecerdasan buatan yang dapat dijelaskan menggunakan metode *SHapley Additive exPlanations (SHAP)* untuk menjelaskan hasil prediksi serta mendukung deteksi *Quishing* melalui proses decode *QR Code*. Penelitian menggunakan metodologi *Cross-Industry Standard Process for Data Mining (CRISP-DM)* dengan dataset *PhiUSIIL Phishing URL Dataset* yang diperoleh dari *Kaggle*.

Hasil penelitian menunjukkan bahwa model *LightGBM* memperoleh Akurasi 99,77%, Presisi 99,62%, *recall* 99,98%, *F1-score* sebesar 99,80%, dan *ROC-AUC* sebesar 99,84%. Berdasarkan hasil confusion matrix, model berhasil mengklasifikasikan 20.088 *URL legitimate* dan 26.964 *URL phishing* dengan benar, serta menghasilkan 101 *false positive* dan 6 *false negative*. Selain itu, pengujian implementasi sistem menggunakan 10 *URL* uji yang terdiri atas 5 *URL legitimate* dan 5 *URL phishing*, beserta representasi *QR Code* masing-masing *URL*, menunjukkan bahwa sistem mampu melakukan deteksi secara *real-time* sesuai dengan kategori *URL* yang diuji. Sistem yang dikembangkan mampu melakukan deteksi *URL phishing* secara *real-time* melalui masukan *URL* maupun *QR Code*, serta memberikan penjelasan hasil prediksi menggunakan *SHAP*.

Berdasarkan hasil pengujian, algoritma *LightGBM* berhasil diimplementasikan secara efektif pada sistem deteksi *URL phishing* berbasis *web*. Integrasi *SHAP* meningkatkan transparansi hasil prediksi, sedangkan fitur deteksi *Quishing* membantu mengidentifikasi *URL* berbahaya yang tersembunyi di dalam *QR Code*.

Kata Kunci: *Phishing, LightGBM, Machine Learning, SHAP, QR Code, Quishing.*

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul “Implementasi Algoritma LightGBM dengan Integrasi Explainable AI dan Fitur Anti-Quishing pada Sistem Deteksi URL Phishing Berbasis Web”

Tugas Akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana (S1) pada Program Studi Informatika, Fakultas Teknik, Universitas Wijaya Kusuma Surabaya. Selama proses penyusunannya, penulis memperoleh banyak bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Orang tua dan keluarga penulis yang selalu memberikan doa, dukungan, dan motivasi.
2. Bapak Dr. Ir. Anang Kukuh Adisusilo, S.T., M.T., selaku Dekan Fakultas Teknik.
3. Bapak Nonot Wisnu Karyanto, S.T., M.Kom., selaku Ketua Program Studi Informatika.
4. Ibu Dr. Tjatusari Widiartin, S.Kom., M.Kom., selaku Dosen Pembimbing yang telah memberikan arahan, bimbingan, serta masukan selama penyusunan Tugas Akhir.
5. Seluruh dosen Program Studi Informatika Universitas Wijaya Kusuma Surabaya yang telah memberikan ilmu dan pengetahuan selama masa perkuliahan.
6. Istri tercinta, Sabrina, yang senantiasa memberikan doa, kasih sayang, pengertian, semangat, serta dukungan sehingga Saya dapat menyelesaikan Tugas Akhir ini dengan baik.
7. Teman-teman seperjuangan yang selalu memberikan semangat dan dukungan selama proses penyusunan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan penelitian ini. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca serta berkontribusi dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Surabaya, Juli 2026

Muh. Zaqi Firdaus

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI.....	iii
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	viii
DAFTAR ISTILAH.....	ix
BAB I.....	1
PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian.....	3
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan	3
BAB II	5
TINJAUAN PUSTAKA	5
2.1. Penelitian Terdahulu.....	5
2.2. <i>Website</i> dan <i>URL</i>	8
2.2.1. <i>Website</i>	9
2.2.2. <i>URL</i>	9
2.3. Keamanan siber dan Ancaman	10
2.3.1. <i>Phishing</i>	10
2.3.2 <i>QR Code Phishing (Quishing)</i>	12
2.4. <i>Light Gradient Boosting Machine</i>	12
2.4.1. Karakteristik dan Logika Kerja <i>LightGBM</i>	13
2.4.2. Keunggulan <i>LightGBM</i>	15
2.4.3. <i>Explainable AI (XAI)</i>	16
2.4.4. <i>Reputation Score</i>	16
2.5. <i>Feature Engineering</i> dan Ekstraksi Fitur <i>URL</i>	17
2.5.1. Fitur Leksikal <i>URL</i>	18
2.5.2. Fitur <i>Domain</i> dan Struktur <i>URL</i>	19
2.5.3. <i>URL Obfuscation Detection</i>	19

2.5.4. Analisis SSL dan Redirect URL	20
2.6. Machine Learning	21
2.6.1. Supervised Learning	21
2.6.2. Klasifikasi	22
2.6.3. Hyperparameter Tuning.....	22
2.6.4. Evaluasi Model	23
2.7. CRISP-DM	24
2.7.1. Business Understanding	24
2.7.2. Data Understanding	24
2.7.3. Data Preparation	25
2.7.4. Modeling	25
2.7.5. Evaluation	25
2.7.6. Deployment	25
2.8. Flask Framework	26
2.9. QR Code dan QR Code Decoder.....	26
2.9.1. QR Code.....	27
2.9.2. QR Code Decoder.....	27
BAB III.....	29
METODE PENELITIAN	29
3.1. Pemahaman Bisnis (<i>Business Understanding</i>)	29
3.1.1. Kebutuhan Fungsional	30
3.1.2. Kebutuhan Non Fungsional	31
3.2. Pemahaman Data (<i>Data Understanding</i>).....	31
3.3. Prapemrosesan Data (<i>Data Preparation</i>).....	32
3.3.1. Ekstraksi Fitur (<i>Feature Engineering</i>).....	33
3.3.2. Pembersihan Data dan Validasi	36
3.3.3. Pembagian Dataset (<i>Data Splitting</i>)	36
3.4. Pemodelan (<i>Modeling</i>).....	37
3.4.1. Pelatihan Model <i>LightGBM</i>	37
3.4.2. Konfigurasi Parameter Model.....	39
3.4.3. <i>Explainable Artificial Intelligence (XAI)</i>	39
3.5. Evaluasi (<i>Evaluation</i>).....	40
3.5.1. <i>Confusion Matrix</i>	41
3.5.2. <i>Accuracy</i>	41

3.5.3. <i>Precision</i>	42
3.5.5. <i>F1-Score</i>	42
3.5.6. <i>ROC-AUC</i>	42
3.5.7. Evaluasi Sistem.....	43
3.6. <i>Deployment</i>	43
3.6.1. Implementasi <i>Backend</i>	45
3.6.2. Integrasi Model <i>LightGBM</i>	45
3.6.3. Implementasi <i>Explainable Artificial Intelligence (XAI)</i>	45
3.6.4. Implementasi <i>Reputation Score</i>	45
3.6.5. Implementasi Deteksi <i>Quishing</i>	46
3.6.6. Implementasi Antarmuka Pengguna	46
BAB IV	47
HASIL DAN PEMBAHASAN	47
4.1. Uji Coba Fungsional Sistem	47
4.1.1. Halaman Utama Sistem	47
4.1.2. Analisis <i>URL</i>	49
4.1.3. Analisis <i>QR Code</i>	50
4.1.4. <i>SHAP Explanation</i>	52
4.1.5. <i>Reputation Score</i>	53
4.1.6. Hasil Analisis <i>URL</i>	54
4.2. Hasil Training Model <i>LightGBM</i>	56
4.2.1. <i>Confusion Matrix</i>	56
4.2.2. <i>Accuracy</i>	58
4.2.3. <i>Precision</i>	58
4.2.4. <i>Recall</i>	59
4.2.5. <i>F1-Score</i>	60
4.2.6. <i>ROC-AUC</i>	61
4.3. Uji Coba Deteksi	62
4.3.1. Uji Coba <i>URL Legitimate</i>	63
4.3.2. Uji Coba <i>QR Code Legitimate</i>	63
4.3.3. Uji Coba <i>URL Phishing</i>	64
4.3.4. Uji Coba <i>QR Code Phishing</i>	65
4.4. Pembahasan.....	66
4.4.1. Analisis Performa Model.....	66

4.4.2. Analisis <i>Explainable AI (SHAP)</i>	68
4.4.3. Analisis <i>Reputation Score</i>	69
4.4.4. Analisis Fitur <i>Quishing</i>	71
4.4.5. Kelebihan dan Keterbatasan Sistem	72
BAB V	76
PENUTUP	76
5.1. Kesimpulan	76
5.2. Saran.....	77
DAFTAR PUSTAKA	79
LAMPIRAN	83

DAFTAR GAMBAR

Gambar 2.1 Flowchart Proses Pelatihan Model <i>LightGBM</i>	14
Gambar 3.1 Metode <i>CRISP-DM</i>	29
Gambar 3.2 Arsitektur Sistem <i>Deployment</i>	44
Gambar 4.1 Halaman Utama Sistem	48
Gambar 4.2 <i>Input URL</i> untuk Analisis	49
Gambar 4.3 Hasil Analisis <i>QR Code</i>	51
Gambar 4.4 Implementasi <i>SHAP Explanation</i>	52
Gambar 4.5 Hasil Deteksi <i>URL aman</i>	54
Gambar 4.6 Hasil Prediksi <i>URL</i>	55
Gambar 4.7 <i>Confusion Matrix</i> Model <i>LightGBM</i>	56

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu	5
Tabel 3.1 Fitur yang Digunakan dalam Sistem.....	33
Tabel 3.2 Parameter Model <i>LightGBM</i>	39
Tabel 4.1 Komponen <i>Confusion Matrix</i>	57
Tabel 4.2 Hasil Pengujian <i>URL Legitimate</i>	63
Tabel 4.3 Hasil Pengujian <i>QR Code Legitimate</i>	64
Tabel 4.4 Hasil Pengujian <i>URL Phishing</i>	64
Tabel 4.5 Hasil Pengujian <i>QR Code Phishing</i>	65

DAFTAR ISTILAH

1. *Accuracy*: Tingkat ketepatan model dalam mengklasifikasikan data berdasarkan label yang sebenarnya.
2. *Confusion Matrix*: Matriks evaluasi yang digunakan untuk membandingkan hasil prediksi model dengan data aktual sehingga diperoleh nilai *True Positive*, *True Negative*, *False Positive*, dan *False Negative*.
3. *Cross-Industry Standard Process for Data Mining (CRISP-DM)*: Metodologi standar yang digunakan dalam pengembangan proyek data mining dan machine learning yang terdiri atas tahapan Pemahaman bisnis, Pemahaman Data, Persiapan Data, Pemodelan, Evaluasi, dan Penerapan.
4. *Dynamic Summary*: Ringkasan hasil analisis yang dihasilkan secara otomatis berdasarkan hasil prediksi model dan karakteristik *URL* sehingga pengguna memperoleh penjelasan mengenai tingkat keamanan *URL* yang dianalisis.
5. *Explainable Artificial Intelligence (XAI)*: Pendekatan kecerdasan buatan yang memungkinkan hasil prediksi model dapat dijelaskan sehingga lebih mudah dipahami oleh pengguna.
6. *F1-score*: Metrik evaluasi yang merupakan rata-rata harmonik antara nilai *precision* dan *recall*.
7. *False Negative*: Kondisi ketika *URL phishing* diprediksi sebagai *URL legitimate* oleh sistem.
8. *False Positive*: Kondisi ketika *URL legitimate* diprediksi sebagai *URL phishing* oleh sistem.
9. *Kaggle: Platform* penyedia dataset dan kompetisi data science yang digunakan sebagai sumber dataset pada penelitian ini.
10. *Legitimate*: Istilah yang digunakan untuk menunjukkan *URL* atau *website* yang sah, aman, dan bukan merupakan phishing.
11. *Light Gradient Boosting Machine (LightGBM)*: Algoritma *machine learning* berbasis *gradient boosting* yang digunakan untuk mengklasifikasikan *URL* menjadi kategori *phishing* atau *legitimate*.
12. *Machine Learning*: Cabang kecerdasan buatan yang memungkinkan sistem mempelajari pola dari data untuk melakukan prediksi atau klasifikasi tanpa diprogram secara eksplisit.
13. *Phishing*: Teknik penipuan siber yang bertujuan memperoleh informasi sensitif pengguna melalui *URL* atau situs *web* palsu yang menyerupai layanan resmi.

14. *PhiUSIIL Phishing URL Dataset*: Dataset yang berisi kumpulan *URL phishing* dan *URL legitimate* yang digunakan sebagai data pelatihan dan pengujian model pada penelitian ini.
15. *Precision*: Kemampuan model dalam menghasilkan prediksi *phishing* yang benar dari seluruh *URL* yang diprediksi sebagai phishing.
16. *QR Code*: Kode dua dimensi yang dapat menyimpan berbagai jenis informasi, termasuk *URL*.
17. *QR Code Phishing (Quishing)*: Teknik *phishing* yang memanfaatkan *QR Code* untuk mengarahkan pengguna menuju *URL* berbahaya atau situs *phishing*.
18. *Real-time*: Kemampuan sistem dalam memproses data dan memberikan hasil analisis secara langsung atau hampir tanpa jeda setelah menerima masukan.
19. *Recall*: Kemampuan model dalam mendeteksi seluruh *URL phishing* yang sebenarnya terdapat pada data pengujian.
20. *Receiver Operating Characteristic - Area Under the Curve (ROC-AUC)*: Metrik evaluasi yang digunakan untuk mengukur kemampuan model dalam membedakan kelas phishing dan legitimate pada berbagai nilai ambang keputusan.
21. *Redirect Chain*: Rangkaian proses pengalihan *URL* dari satu alamat ke alamat lain sebelum mencapai halaman tujuan akhir yang digunakan sebagai salah satu indikator keamanan *URL*.
22. *Rule-based*: Pendekatan deteksi yang bekerja berdasarkan aturan atau pola yang telah ditentukan sebelumnya.
23. *SHapley Additive exPlanations (SHAP)*: Metode *Explainable Artificial Intelligence (XAI)* yang digunakan untuk menjelaskan kontribusi setiap fitur terhadap hasil prediksi model.
24. *Uniform Resource Locator (URL)*: Alamat unik yang digunakan untuk mengidentifikasi dan mengakses suatu sumber daya atau halaman pada jaringan internet.