

**DETEKSI MALICIOUS LINK PADA KONTEN DEWASA DI
PLATFORM X MENGGUNAKAN METODE
MACHINE LEARNING**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

MUHAMAD IQBAL ASHARI

22.83.0818

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

**DETEKSI MALICIOUS LINK PADA KONTEN DEWASA DI
PLATFORM X MENGGUNAKAN METODE
MACHINE LEARNING**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

MUHAMAD IQBAL ASHARI

22.83.0818

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

HALAMAN PERSETUJUAN

SKRIPSI

**DETEKSI MALICIOUS LINK PADA KONTEN DEWASA DI
PLATFORM X MENGGUNAKAN METODE
MACHINE LEARNING**


yang disusun dan diajukan oleh

Muhamad Iqbal Ashari

. **22.83.0818**

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 3 Februari 2026

Dosah Pembimbing,


Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128

HALAMAN PENGESAHAN
SKRIPSI
DETEKSI MALICIOUS LINK PADA KONTEN DEWASA DI
PLATFORM X MENGGUNAKAN METODE
MACHINE LEARNING

yang disusun dan diajukan oleh

Muhamad Iqbal Ashari

22.83.0818

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Februari 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Muhammad Kopravi, S.Kom., M.Eng.
NIK. 190302454

Senic Destya, S.T., M.Kom.
NIK. 190302312

Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhamad Iqbal Ashari
NIM : 22.83.0818

Menyatakan bahwa Skripsi dengan judul berikut:

Deteksi Malicious Link pada Konten Dewasa di Platform X menggunakan metode Machine Learning

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Februari 2026

Yang Menyatakan,



Muhamad Iqbal Ashari

HALAMAN PERSEMBAHAN

Puji syukur senantiasa tercurah kepada Allah SWT atas segala rahmat, kelancaran, dan kekuatan yang diberikan sehingga skripsi ini dapat terselesaikan. Dengan rasa syukur yang mendalam, karya kecil ini kupersembahkan kepada:

1. Teruntuk kedua orang tua saya, Ibu dan Ayah tercinta. Terima kasih atas segala dukungan dan doa yang tak pernah putus di setiap sujud kalian. Terima kasih selalu mengupayakan yang terbaik, serta atas curahan kasih sayang dan perhatian yang luar biasa selama ini. Semoga Allah SWT senantiasa merahmati dan memberikan Jannah-Nya kepada Ibu dan Ayah.
2. Teruntuk Dosen Pembimbing saya, Bapak Dr. Dony Ariyus, S.S., M.Kom. Terima kasih atas segala kesabaran, diskusi, dan motivasi yang tak henti-hentinya diberikan kepada saya. Tanpa bimbingan, kritik membangun, dan arahan dari Bapak, karya ini tidak akan bisa terwujud hingga mencapai titik ini. Semoga Bapak senantiasa diberikan kesehatan dan keberkahan.
3. Kepada semua teman-teman saya dan seluruh *genk* yang selalu memberikan dukungan tanpa henti. Terima kasih telah menjadi bagian dari perjalanan panjang ini. Kita telah tumbuh, belajar, dan berjuang bersama untuk mewujudkan impian ini. Sebuah apresiasi khusus saya sampaikan untuk **Babayogenk**; terima kasih sudah membersamai setiap langkah dalam petualangan ini hingga kita bisa mencapai garis akhir dengan cara terbaik. Perjalanan ini tidak akan sama tanpa kehadiran kalian.
4. Kepada satu nama yang tak bisa kusebutkan secara langsung, namun doanya selalu mengiringi setiap langkahku. Terima kasih telah hadir dan menjadi bagian terindah dalam perjalanan ini. Kehadiranmu, meski tak tertulis secara aksara di sini, adalah salah satu kekuatan terbesarku hingga skripsi ini berhasil diselesaikan.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya, sehingga skripsi dengan judul "Deteksi Malicious Link pada Konten Dewasa di Platform X Menggunakan Metode Machine Learning" ini dapat diselesaikan dengan baik. Skripsi ini disusun dan diajukan sebagai salah satu syarat untuk menyelesaikan studi jenjang Strata Satu (S1) dan memperoleh gelar Sarjana Komputer pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta.

Penyelesaian skripsi ini tidak lepas dari dukungan, bimbingan, arahan, serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini disampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas AMIKOM Yogyakarta.
2. Prof. Dr. Kusriani, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Dr. Dony Ariyus, S.S., M.Kom., selaku Ketua Program Studi Teknik Komputer sekaligus Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, arahan, serta evaluasi selama proses penyusunan skripsi ini.
4. Muhammad Koprari, S.Kom., M.Eng., selaku Dosen Penguji yang telah memberikan saran, kritik yang membangun, serta masukan demi kesempurnaan penelitian ini.
5. Senie Destya, S.T., M.Kom., selaku Dosen Penguji yang juga telah memberikan evaluasi dan arahan berharga dalam penyempurnaan skripsi ini.
6. Seluruh Bapak dan Ibu Dosen Program Studi Teknik Komputer Universitas AMIKOM Yogyakarta yang telah membekali ilmu pengetahuan selama masa perkuliahan.

7. Kedua orang tua tercinta yang senantiasa memberikan doa, kasih sayang, serta dukungan moral maupun material yang tak terhingga hingga pendidikan dan penyusunan skripsi ini dapat diselesaikan.

Disadari bahwa dalam penulisan skripsi ini masih terdapat banyak kekurangan dan jauh dari kata sempurna. Oleh karena itu, segala kritik dan saran yang membangun sangat diharapkan demi perbaikan di masa yang akan datang.

Akhir kata, semoga skripsi ini dapat memberikan manfaat serta kontribusi positif bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan *machine learning*.

Yogyakarta, 23 Februari 2026

Muhamad Iqbal Ashari

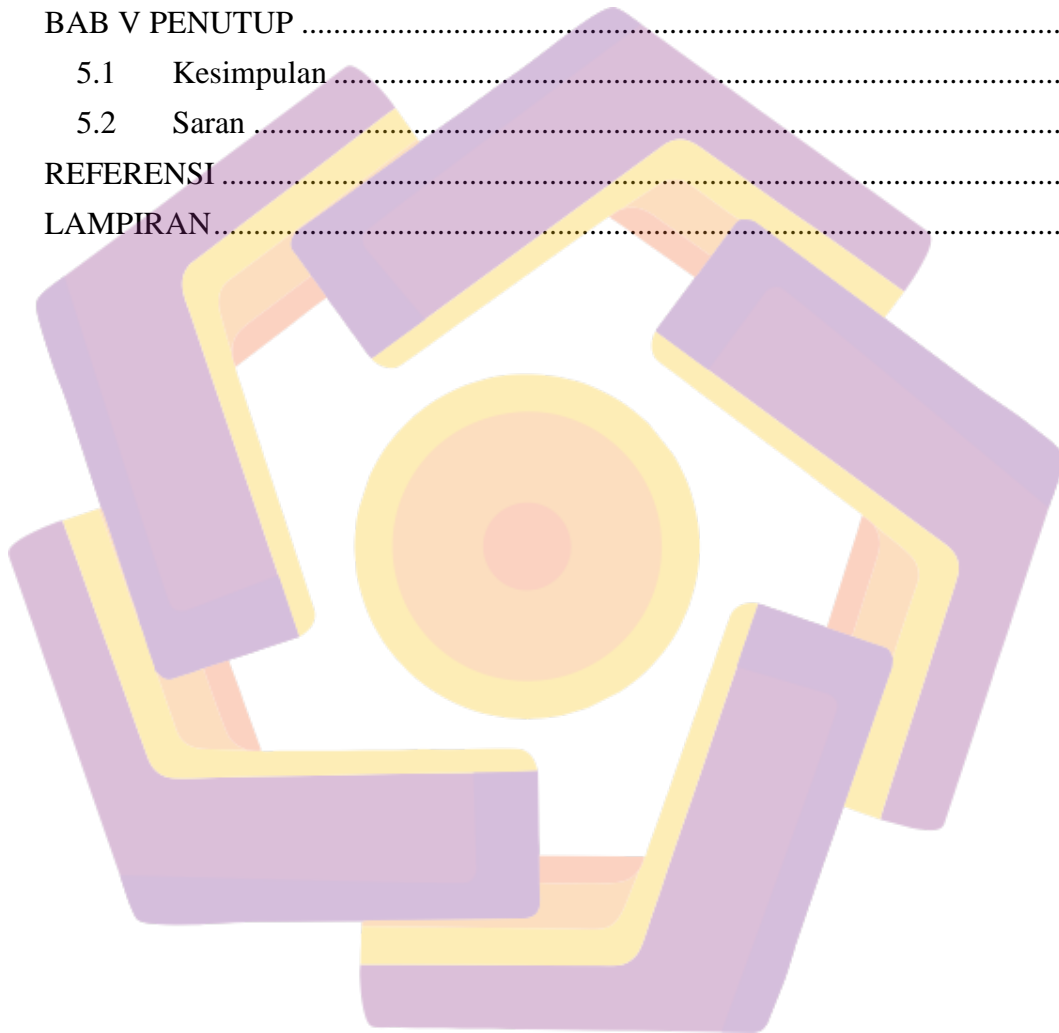


DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
DAFTAR ISTILAH	xiv
INTISARI	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	1
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	7
2.1 Studi Literatur	7
2.2 Dasar Teori.....	12
2.2.1 Konsep Phising dan Evolusi Teknik Penipuan Siber.....	12
2.2.2 Struktur URL dan Indikator Teknis Phishing	13
2.2.3 Karakteristik Tautan Pendek (Shortlink) dan Perilaku Redirect...14	
2.2.4 Media Sosial X dan Pola Penyebaran	15
2.2.5 Machine Learning dalam Deteksi Phishing	15
2.2.6 Ekstraksi Fitur URL (<i>Feature Engineering</i>).....	17
2.2.7 Evaluasi Model dan Metrik Pengukuran.....	18
BAB III METODE PENELITIAN	19
3.1 Alur Penelitian	19

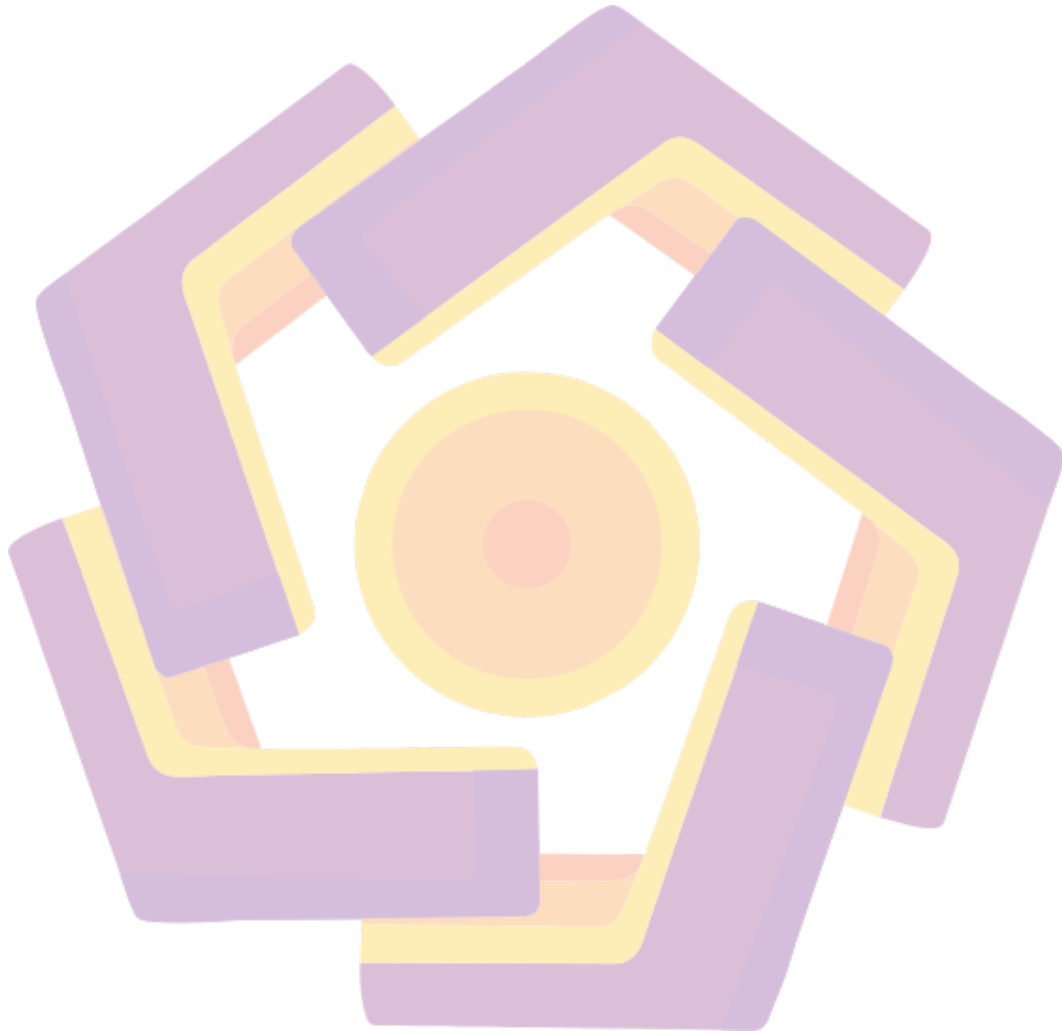
3.2	Pengumpulan Data	20
3.2.1	Dataset Sekunder (Dataset Publik - Benign)	21
3.2.2	Dataset Primer (Dataset Temuan Sendiri - Malicious)	21
3.3	Tahapan Pengolahan Data.....	22
3.4	Perancangan system	22
3.4.1	Alur Sistem Deteksi	24
3.4.2	Mekanisme Pembelajaran Model (Model Training).....	27
3.4.3	Implementasi Algoritma	28
3.4.4	Struktur Data Log	28
3.5	Skenario Pengujian	30
3.6	Evaluasi Kerja	31
3.7	Visualisasi Alur Serangan dan Studi Kasus	32
3.7.1	Studi Kasus 1: Ekosistem Perjudian Daring	33
3.7.2	Studi Kasus 2: Manipulasi SEO dan Teknik Clickjacking	36
3.7.3	Studi Kasus 3: Penipuan Afiliasi E-commerce (Affiliate Fraud – Marketplace)	38
3.7.4	Studi Kasus 4: Migrasi Platform dan Kanal Privat (Platform Funneling)	40
3.7.5	Studi Kasus 5: Taktik <i>Bait-and-Switch</i> pada Marketplace	42
3.7.6	Studi Kasus 6: Promosi Gim Dewasa dengan Manipulasi Antarmuka.....	43
3.8	Lingkungan Pengembangan Sistem	45
BAB IV HASIL DAN PEMBAHASAN		47
4.1	Deskripsi Data Penelitian.....	47
4.1.1	Dataset Yang di Gunakan	47
4.1.2	Karakteristik Dataset Malicious	48
4.1.3	Karakteristik Dataset Benign	49
4.2	Pra-pemrosesan dan Ekstraksi Fitur.....	50
4.2.3	Rasionalisasi Pemilihan Fitur.....	50
4.2.4	Fitur Leksikal dan Entropi	51
4.3	Konfigurasi Eksperimen	52
4.3.3	Skenario Pembagian Data	52
4.4	Hasil Evaluasi Kinerja Model	52
4.4.3	Performa Algoritma	53
4.4.4	Kurva Pembelajaran	54

4.4.3	Analisis Confusion Matrix	55
4.4.4	Analisis Fitur Dominan (Feature Importance)	56
4.5	Implementasi Antarmuka Pengguna	58
4.5.1	Fitur Single Scan dan Hasil Deteksi	58
4.5.2	Fitur Bulk Scan (Pemindaian Massal)	59
4.5.3	Hasil Analisis Bulk Scan	60
BAB V PENUTUP		62
5.1	Kesimpulan	62
5.2	Saran	62
REFERENSI		64
LAMPIRAN		65



DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian	9
Tabel 3.1 Rancangan Struktur Data Log.....	30
Tabel 3.2 Lingkungan Pengembangan Sistem.....	46
Tabel 4.1 Data Uji.....	53

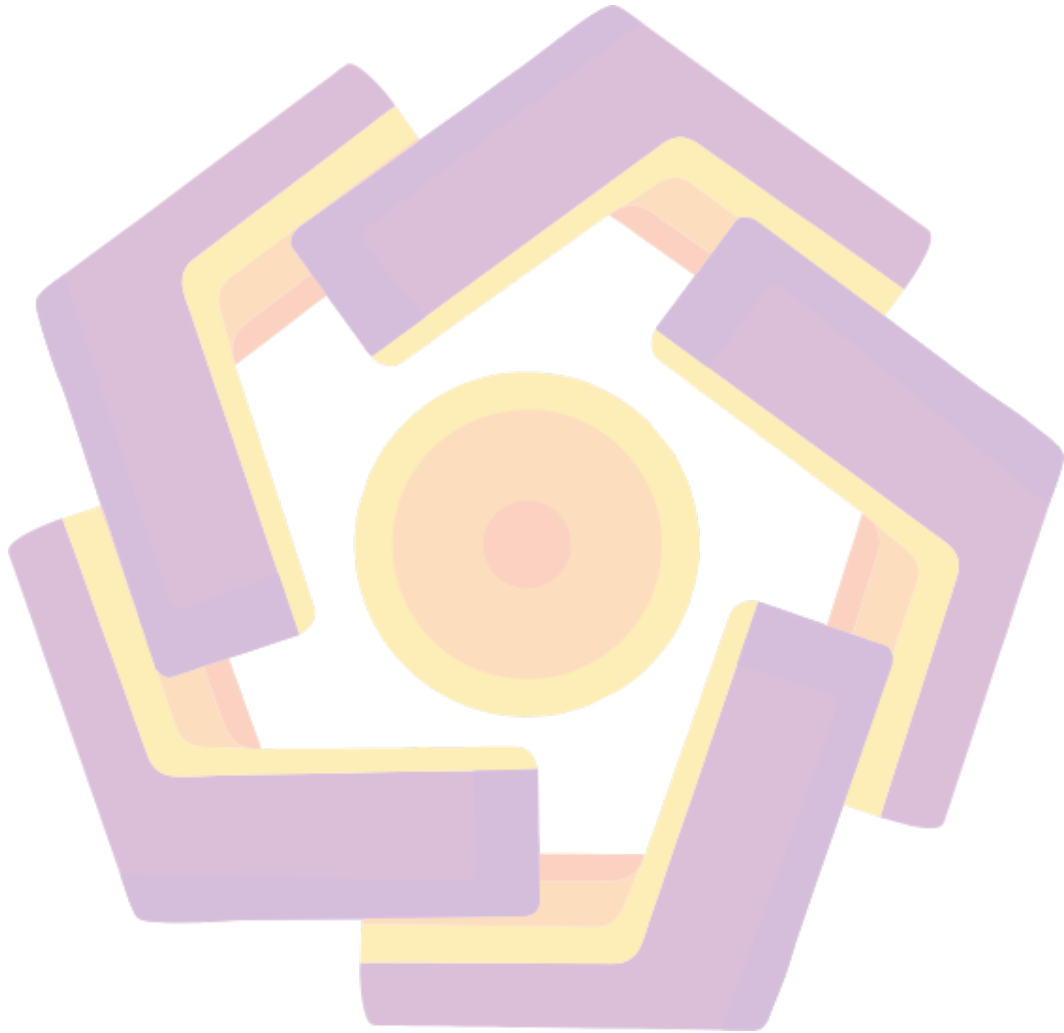


DAFTAR GAMBAR

Gambar 2.1 Struktur Data URL	13
Gambar 3.1 Alur Penelitian	19
Gambar 3.2 Alur Sistem Deteksi	24
Gambar 3.3 <i>Pseudocode</i> Implementasi Algoritma	28
Gambar 3.4 Vektor serangan awal dari akun @videy_viday	34
Gambar 3.5 Halaman Perantara pada Video VIP	35
Gambar 3.6 Link yang mengarah ke Judi Online	35
Gambar 3.7 Eksploitasi Tren Viral dari aku @stevenwangi1101	36
Gambar 3.8 Teknik Deceptive Overlay di dalam Video Player	37
Gambar 3.9 SEO Google yang mengarah ke Judi Online.....	38
Gambar 3.10 Teknik Manipulatif dari akun @Fajargangg3u.....	39
Gambar 3.11 Manipulasi Psikologis Skip Ad pada Video Player	39
Gambar 3.12 Redirect ke Blibi	40
Gambar 3.13 Teknik Gambar Vulgar dari akun @swcteur	41
Gambar 3.14 Ekosistem tertutup pada Telegram.....	41
Gambar 3.15 Tautan berantai dari akun @Majito_Squash.....	42
Gambar 3.16 Link konten dewasa yang mengarah ke Afiliate Shopee	43
Gambar 3.17 Teknik <i>Fake Warning</i> pada gim <i>Lust Goddess</i>	44
Gambar 3.18 Pengalihan ke gim <i>Lust Goddess</i>	45
Gambar 4.1 Dataset Malicious.....	48
Gambar 4.2 Dataset Benign	49
Gambar 4.3 Kurva Pembelajaran	54
Gambar 4.4 Visualisasi Confusion Matrix.....	55
Gambar 4.5 Bobot Fitur	56
Gambar 4.6 Unmask Single Scan	58
Gambar 4.7 Unmask Bulk Scan.....	59
Gambar 4.8 Log dari Hasil Bulk Scan	60

DAFTAR LAMPIRAN

Lampiran 1: Source Code Pelatihan Model	65
Lampiran 2: Source Code Antarmuka Aplikasi	69



DAFTAR ISTILAH

Akurasi	Persentase prediksi benar dari keseluruhan data uji.
<i>Blacklist</i>	Daftar situs yang diblokir karena terindikasi berbahaya.
<i>Cloaking</i>	Teknik menyembunyikan konten asli dari sistem deteksi.
<i>Crawler</i>	Program bot yang mengunduh data dari internet secara otomatis.
Data Latih	Kumpulan data untuk melatih model mengenali pola.
Data Uji	Kumpulan data untuk mengukur performa model setelah dilatih.
<i>Deep Scan</i>	Metode analisis mendalam pada isi dan struktur tautan.
Entropi	Nilai yang mengukur tingkat keacakan karakter dalam URL.
<i>False Positive</i>	Kesalahan sistem mendeteksi link aman sebagai berbahaya.
Fitur (<i>Feature</i>)	Atribut numerik yang diekstrak dari URL (misal: panjang karakter).
<i>Phishing</i>	Penipuan siber untuk mencuri data pribadi atau finansial.
Platform X	Nama baru dari media sosial Twitter.
<i>Redirect</i>	Pengalihan otomatis dari satu alamat web ke alamat lain.
<i>Unshortening</i>	Proses membuka link pendek (t.co) menjadi link asli.
URL Shortener	Layanan pemendek tautan web.
Whitelist	Daftar situs resmi yang dianggap aman dan terpercaya.
XGBoost	Algoritma pembelajaran mesin berbasis decision tree yang efisien.

INTISARI

Perubahan kebijakan platform X pada Juni 2024 yang mengizinkan konten dewasa secara konsensual telah menciptakan celah keamanan siber baru. Pelaku kejahatan siber sering memanfaatkan konten tersebut sebagai umpan (*bait*) untuk menyebarkan tautan *phishing* yang tersamar melalui layanan pemendek URL t.co. Penelitian ini bertujuan untuk membangun sistem deteksi otomatis menggunakan metode *Machine Learning* guna mengatasi keterbatasan sistem moderasi konvensional. Dataset yang digunakan berjumlah 1.000 tautan yang dikumpulkan melalui teknik *crawling* pada platform X, dengan komposisi seimbang antara kategori aman dan berbahaya. Fitur leksikal dan statistik, khususnya *Shannon Entropy*, diekstraksi dari struktur URL untuk melatih model klasifikasi berbasis algoritma XGBoost. Hasil penelitian menunjukkan bahwa fitur entropi memiliki pengaruh paling signifikan dalam mendeteksi anomali pada tautan pendek. Performa model dievaluasi menggunakan *Confusion Matrix*, menghasilkan tingkat akurasi dan stabilitas metrik yang optimal dalam mengidentifikasi ancaman siber pada ekosistem platform X. Sistem deteksi ini kemudian diimplementasikan ke dalam aplikasi purwarupa bernama "Unmask" sebagai solusi perlindungan pengguna secara *real-time*.

Kata kunci: *Phishing, Machine Learning, XGBoost, Platform X, Konten Dewasa.*

ABSTRACT

The policy change on platform X in June 2024, which allows consensual adult content, has created a new cybersecurity vulnerability. Cybercriminals frequently exploit this content as bait to distribute phishing links disguised through the t.co URL shortening service. This research aims to build an automated detection system using Machine Learning methods to overcome the limitations of conventional moderation systems. The dataset used consists of 1,000 links collected via crawling techniques on platform X, with a balanced composition of benign and malicious categories. Lexical and statistical features, specifically Shannon Entropy, were extracted from the URL structure to train a classification model based on the XGBoost algorithm. The results indicate that the entropy feature has the most significant impact on detecting anomalies in short links. The model's performance was evaluated using a Confusion Matrix, yielding optimal accuracy and metric stability in identifying cyber threats within the platform X ecosystem. This detection system was then implemented into a prototype application named "Unmask" as a practical solution for real-time user protection.

Keyword: *Phishing, Machine Learning, XGBoost, Platform X, Adult Content.*

