PROPOSAL

PROGRAM KREATIVITAS MAHASISWA

JUDUL

PKM-KC: Rancang Bangun Prototipe Aplikasi "PhisInc." sebagai Layanan Verifikasi Tautan Real-Time bagi Pengguna Internet.

Diusulkan Oleh:

- STEVEN KARUNIA, LIEM – 2802458573
- MAXIMILANO STEFAN CAHYADI, TJIU – 2802417812
- NICHOLAS HUBERT SOEGIHONO – 2802515564
- SIMON ZELOTES DIMAS COR LINTRUS – 2802511130

BINA NUSANTARA UNIVERSITY

SEMARANG

2025

DAFTAR ISI

DAFTAR GAMBAR

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Saat ini, kemajuan teknologi memang memudahkan hidup kita, tapi di sisi lain juga membuka celah bagi kejahatan siber, khususnya phishing. Phishing adalah trik penipuan di mana pelaku menyamar menjadi pihak resmi untuk mencuri data penting seperti password atau info kartu kredit. Di Indonesia, kasus ini makin sering terjadi dan caranya makin canggih, misalnya dengan membuat link palsu yang sangat mirip dengan aslinya. Akibatnya, banyak orang rugi uang dan jadi takut bertransaksi digital.

Masalahnya, meski antivirus sudah banyak, belum ada alat praktis yang bisa dipakai orang awam untuk mengecek apakah sebuah link itu aman atau tidak secara instan. Kebanyakan alat canggih cuma tersedia untuk perusahaan besar. Karena itulah, kami merasa perlu ada sistem yang bisa "membaca" struktur link secara cerdas dan memberi peringatan cepat kepada pengguna.

Untuk menjawab masalah ini, kami mengusulkan "PhisInc.", sebuah aplikasi pendeteksi link berbahaya secara real-time. Cara kerjanya simpel: pengguna tinggal menempelkan link yang mencurigakan, lalu sistem kami akan menganalisisnya secara otomatis untuk menentukan apakah link itu aman atau penipuan. Tujuan utamanya adalah memberi perlindungan yang mudah digunakan oleh siapa saja.

Proyek ini juga sejalan dengan tujuan global (SDGs). Penggunaan kecerdasan buatan (AI) dalam aplikasi ini merupakan bentuk inovasi teknologi yang mendukung SDG 9 (Industri, Inovasi, dan Infrastruktur). Selain itu, karena aplikasi ini mencegah kejahatan dan melindungi data warga, ia juga berkontribusi pada SDG 16 (Perdamaian, Keadilan, dan Kelembagaan yang Tangguh) dengan menciptakan ruang internet yang lebih aman dan bebas dari penipuan.

1.2 TUJUAN

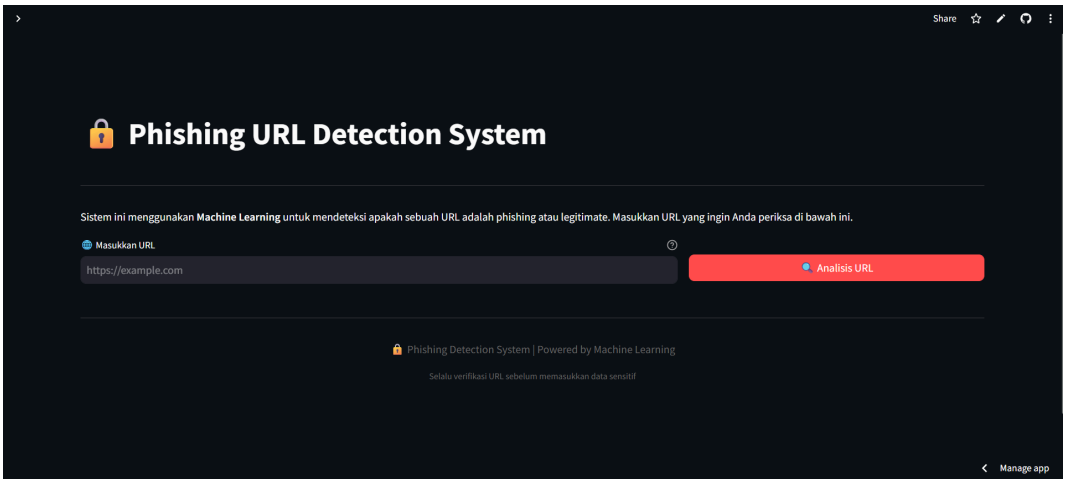
Adapun tujuan utama yang hendak dicapai melalui pelaksanaan proyek PKM-KC "PhisInc." ini adalah merancang arsitektur sistem dan UI/UX yang intuitif untuk layanan verifikasi tautan real-time. Hal ini

dilanjutkan dengan mengembangkan dan mengimplementasikan mekanisme analisis URL yang memanfaatkan fitur-fitur heuristik dan/atau model klasifikasi Machine Learning untuk mendeteksi tautan phishing secara otomatis. Puncak dari tujuan ini adalah mewujudkan prototipe Aplikasi "PhisInc." yang fungsional, akurat, dan siap diujicobakan kepada pengguna, serta melakukan pengujian fungsionalitas, performa, dan akurasi dari prototipe yang telah dikembangkan untuk memvalidasi efektivitasnya.

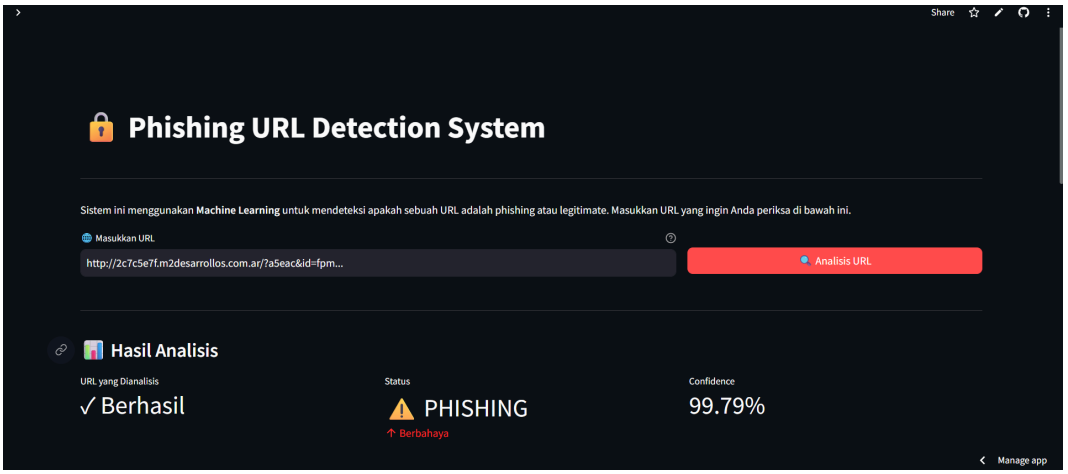
1.3 LUARAN YANG DIHARAPKAN

Luaran yang diharapkan oleh PKM-KC: Rancang Bangun Prototipe Aplikasi "PhisInc." sebagai Layanan Verifikasi Tautan Real-Time bagi Pengguna Internet, ini meliputi:

- Prototipe Aplikasi Fungsional ("PhisInc."): Sebuah website yang mampu menerima input URL, melakukan analisis fitur URL, dan menghasilkan output klasifikasi phishing atau legit dalam real-time, serta memiliki tingkat akurasi deteksi minimal 90%.



Gambar 1. Mockup Input Link



Gambar 2. Mockup Output Link

- Laporan Kemajuan dan Laporan Akhir: Dokumentasi lengkap mengenai proses perancangan, pengembangan, pengujian sistem, analisis hasil, dan kesimpulan proyek sesuai dengan format yang ditetapkan oleh Panduan PKM.

1.4 MANFAAT KEGIATAN

Kegiatan PKM-KC ini diharapkan memberikan manfaat ganda, yaitu secara praktis bagi pengguna internet dan secara keilmuan. Bagi masyarakat umum dan pengguna internet di Indonesia, manfaat yang diperoleh adalah peningkatan signifikan dalam keamanan siber individu melalui penyediaan alat preventif yang mudah diakses dan real-time, sehingga mampu mencegah kerugian finansial dan kebocoran data pribadi akibat serangan phishing. Sementara itu, dari aspek keilmuan dan teknologi, proyek ini akan memberikan kontribusi penting dalam pengembangan teknik deteksi phishing berbasis Machine Learning atau Heuristik, sekaligus menjadi studi kasus implementasi kecerdasan buatan dalam menciptakan solusi keamanan siber yang aplikatif.

BAB 2
TINJAUAN PUSTAKA

2.1 Konsep Dasar Kejahatan Siber dan Phishing

2.1.1 Definisi dan Mekanisme Serangan Phishing

Phishing merupakan salah satu ancaman siber yang paling persisten, didefinisikan sebagai aktivitas kejahatan rekayasa sosial yang bertujuan untuk mencuri informasi sensitif dengan menyamar sebagai institusi keuangan ataupun e-commerce. Mekanisme utama serangan ini adalah melalui tautan palsu yang mengarahkan korban ke halaman web tiruan. Keberhasilan serangan *phishing* bergantung pada kemampuan penyerang untuk menciptakan tautan dan halaman yang tampak sangat autentik, sehingga sulit dibedakan dari yang aslinya

2.1.2 Urgensi Perlindungan dan Kebutuhan Alat Deteksi Proaktif

Seiring meningkatnya digitalisasi di Indonesia, risiko yang ditimbulkan oleh phishing turut meningkat secara signifikan, berdampak pada kerugian finansial individu dan hilangnya kepercayaan publik. Metode perlindungan tradisional, seperti pemblokiran berbasis blacklist, sering kali gagal mendeteksi serangan baru. Oleh karena itu, diperlukan solusi deteksi proaktif yang mampu menganalisis karakteristik tautan secara otomatis dan real-time, menawarkan lapisan perlindungan yang adaptif bagi pengguna akhir.

2.2 Analisis URL dan Ekstraksi Fitur Phishing

Setiap URL memiliki struktur formal yang terdiri dari protokol, nama domain, port, dan path. Dalam konteks deteksi phishing, fokus analisis terletak pada hostname, terutama domain utama, subdomain, dan top-level domain. Perubahan atau anomali pada komponen-komponen ini, seperti penggunaan alamat IP atau typosquatting, adalah indikator kuat dari tautan berbahaya.

2.2.1 Fitur-Fitur Mencurigakan (Heuristik) pada URL

Untuk mengklasifikasikan tautan, PhisInc. akan mengekstraksi sejumlah fitur heuristik yang menjadi ciri khas phishing. Fitur-fitur ini dikategorikan berdasarkan properti leksikal, host-based, dan konten. Beberapa fitur leksikal penting meliputi:

- Panjang URL dan Hostname: Tautan phishing cenderung sangat panjang atau memiliki panjang nama domain yang tidak wajar.
- Adanya Simbol Khusus: Misalnya, simbol @ dalam URL yang digunakan untuk menyembunyikan alamat asli.

- Penggunaan Kata Kunci Sensitif: Adanya kata-kata seperti "login," "secure," atau "verify" dalam domain atau subdomain untuk menipu pengguna.
- Typosquatting: Perbedaan ejaan tipis dari domain terkenal (misalnya g0ogle.com alih-alih google.com).

2.3 Deteksi Berbasis Machine Learning (ML)

2.3.1 Klasifikasi Biner dalam Keamanan Tautan

Dalam kerangka *Machine Learning*, masalah deteksi *phishing* diperlakukan sebagai masalah Klasifikasi Biner, di mana tugas model adalah mengklasifikasikan setiap tautan yang masuk ke dalam salah satu dari dua kelas: Phishing (1) atau Legit (0). Keunggulan ML adalah kemampuannya untuk mempelajari pola kompleks dari data tanpa diprogram secara eksplisit untuk setiap aturan *phishing* baru.

2.3.2 Pemilihan dan Implementasi Algoritma Klasifikasi

Pemilihan algoritma sangat krusial untuk mencapai akurasi tinggi dengan waktu prediksi yang cepat. Algoritma yang umum dan efektif dalam konteks ini adalah Gradient Boosting Classifier (GBC).

1. Gradient Boosting Classifier: algoritma machine learning yang membangun serangkaian model prediksi sederhana secara berurutan, di mana setiap model baru bertugas memperbaiki error dari model sebelumnya. Teknik ini menggabungkan kekuatan seluruh model tersebut menjadi satu kesatuan yang cerdas, sehingga mampu menghasilkan prediksi dengan tingkat akurasi yang sangat tinggi dibandingkan model tunggal.

2.4 Penelitian Terdahulu dan Pemanfaatan Data Kaggle

Berbagai penelitian terdahulu telah membuktikan efektivitas *Machine Learning* dalam deteksi *phishing*, mencapai tingkat akurasi di atas 95% pada kondisi eksperimental. Studi-studi ini berfokus pada optimasi *feature extraction* dan tuning parameter model.

Proyek "PhisInc." secara spesifik memanfaatkan Platform Kaggle sebagai sumber utama *dataset* berlabel. Kaggle, sebagai komunitas *data science* terbesar, menyediakan akses ke *dataset* URL *phishing* yang telah dikurasi dan digunakan secara luas dalam penelitian akademik dan industri. Data ini mencakup ribuan entri tautan yang diklasifikasikan sebagai 'Phishing' atau 'Legit', memungkinkan pelatihan model ML yang *robust* dan teruji secara eksternal.

Pemanfaatan data Kaggle tidak hanya memastikan kredibilitas ilmiah dan validitas statistik dari model yang dikembangkan, tetapi juga memungkinkan tim untuk fokus pada aspek Karsa Cipta (KC), yaitu merancang dan mengembangkan

prototipe aplikasi yang *user-centric*. Dengan demikian, "PhisInc." menjadi jembatan antara temuan ilmiah terdahulu (yang berfokus pada algoritma) dengan kebutuhan pengguna di Indonesia.

BAB 3
TAHAP PELAKSANAAN

3.1 Tahap I: Analisis Kebutuhan dan Perancangan Arsitektur

Tahap ini bertujuan untuk menentukan spesifikasi teknis dan non-teknis prototipe serta menghasilkan luaran berupa *desain teknis* awal dan rancangan antarmuka pengguna (UI/UX).

1. **Analisis Kebutuhan Fungsional dan Non-Fungsional:** Menetapkan fitur-fitur wajib aplikasi (*input URL*, *proses klasifikasi real-time*, *interface hasil*), serta menentukan spesifikasi teknis platform pengembangan.
2. **Analisis Kebutuhan Data (Sekunder):** Mengidentifikasi sumber data yang kredibel untuk pelatihan model, yaitu *dataset* tautan *phishing* dan legit yang bersumber dari Kaggle.com.
3. **Perancangan Sistem (Desain Teknis):** Merancang arsitektur sistem yang modular, memisahkan lapisan *frontend*, *backend*, dan modul *Machine Learning* untuk menjamin skalabilitas dan efisiensi.
4. **Perancangan Antarmuka (UI/UX):** Menyusun *wireframe* dan *mockup* visual yang mengedepankan prinsip *user-centric*, memastikan kemudahan penggunaan dan aksesibilitas "PhisInc." oleh pengguna internet awam.

3.2 Tahap II: Pengumpulan Data dan Pra-pemrosesan (Preprocessing)

Fokus utama tahap ini adalah menyiapkan *dataset* sekunder yang bersih, terstruktur, dan siap digunakan untuk pelatihan model klasifikasi.

1. **Data Acquisition dan Konsolidasi:** Melakukan pengunduhan dan penggabungan *dataset* tautan dari sumber Kaggle, memastikan data mencakup variasi kasus *phishing* yang relevan.
2. **Feature Engineering (Ekstraksi Fitur):** Mengembangkan modul untuk mengekstrak sejumlah fitur diskrit dari setiap URL. Fitur-fitur ini meliputi panjang, simbol, kata kunci sensitif, usia domain, registrasi, dan karakteristik berbasis anomali.
3. **Data Cleaning, Normalisasi, dan Pembagian:** Menghilangkan data duplikat atau tidak lengkap, melakukan normalisasi fitur numerik, dan membagi data menjadi set pelatihan, validasi, dan pengujian untuk proses pengembangan model.

3.3 Tahap III: Pengembangan Model Machine Learning (Klasifikasi)

Tahap ini merupakan inti dari inovasi (Karsa Cipta) dan berfokus pada pengembangan dan optimasi modul kecerdasan buatan.

1. **Pemilihan dan Implementasi Algoritma:** Mengimplementasikan dan membandingkan kinerja satu atau lebih algoritma klasifikasi biner yang paling sesuai untuk data URL, seperti *Gradient Boosting Classifier (GBC)*, dengan menggunakan bahasa pemrograman berupa *script* Python.
2. **Pelatihan, Validasi, dan Optimasi Model:** Melakukan pelatihan model secara iteratif untuk meminimalkan *error* dan memaksimalkan metrik kinerja utama pada set validasi.
3. **Finalisasi Model:** Memilih model dengan kinerja terbaik dan menyimpannya dalam format yang ringan dan siap diintegrasikan pada lingkungan produksi.

3.4 Tahap IV: Implementasi Prototipe Aplikasi (Pembuatan Produk/Jasa Layanan)

Model yang sudah terlatih diintegrasikan ke dalam prototipe aplikasi **"PhisInc."** yang fungsional.

1. **Pengembangan Situs Melalui Streamlit:** Membangun sebuah situs online yang dapat diakses oleh siapapun melalui framework aplikasi berbasis Python, *Streamlit*. Situs online ini memungkinkan user untuk langsung berinteraksi dengan UI dan pemrosesan backend dalam satu kinerja yang sama. Streamlit dipilih oleh peneliti karena kesederhanaan implementasi serta memproses *input* secara *real-time.*
2. **Integrasi Modul ML:** Menghubungkan model ML yang telah difinalisasi (Tahap III) ke dalam aplikasi *Streamlit* sehingga mampu menerima permintaan URL, melakukan ekstraksi fitur secara otomatis, dan mengembalikan hasil klasifikasi.
3. **Pengembangan Antarmuka Pengguna:** Mengembangkan antarmuka pada website yang berfungsi mengirim input URL dan menampilkan hasil klasifikasi ("Phishing" atau "Legit") dengan tampilan yang informatif dan mudah dipahami pengguna. Penggunaan website dipilih karena mudah untuk diakses dan digunakan oleh pengguna yang ingin langsung melakukan pengecekan terhadap suatu link.

3.5 Tahap V: Pengujian Keandalan dan Evaluasi

Tahap akhir ini bertujuan memvalidasi keandalan dan kelayakan produk, serta melakukan prediksi penerimaan masyarakat.

1. **Pengujian Fungsionalitas (Uji Black Box):** Melakukan *cara pengujian keandalan karya* pada seluruh alur kerja aplikasi, mulai dari input pengguna hingga output hasil, untuk memastikan tidak ada *bug* atau *error* pada integrasi sistem.
2. **Pengujian Akurasi Model (Uji Kelayakan):** Menguji model yang telah terintegrasi menggunakan *dataset* pengujian untuk mengkonfirmasi bahwa *tingkat keberhasilan deteksi* tercapai, menghasilkan prediksi hasil uji yang memperkuat kelayakan produk.
3. **Penyusunan Laporan:** Menyusun Laporan Kemajuan dan Laporan Akhir sebagai dokumentasi komprehensif atas seluruh proses pelaksanaan, hasil, dan evaluasi proyek.

BAB 4
BIAYA DAN JADWAL KEGIATAN

4.1 Anggaran Biaya

Rencana anggaran biaya yang dibutuhkan untuk pelaksanaan PKM-KC ini disusun berdasarkan kebutuhan prioritas dari pengembangan aplikasi “PhisInc.” yaitu bahan yang dipakai, sewa hosting, dan kebutuhan lainnya.

Tabel 4.1. Rekapitulasi Rencana Anggaran Biaya

No	Jenis Pengeluaran	Dana yang Dikeluarkan (Rp.)
1.	Bahan yang dipakai untuk pengembangan aplikasi “PhisInc.”	3.000.000
2.	Sewa dan Jasa hosting	1.000.000
3.	Promosi	1.000.000
	Jumlah	5.000.000

4.2 Jadwal Kegiatan

Kegiatan PKM-KC ini direncanakan akan dilaksanakan selama kurang lebih 6 bulan. Rincian jadwal kegiatan untuk mengembangkan aplikasi “PhisInc.” dimulai dari mencari masalah dan juga dataset hingga penyusunan laporan akhir.

Tabel 4.2

No	Jenis Kegiatan	Bulan 1	Bulan 2	Bulan 3	Bulan 4	Bulan 5	Bulan 6	PIC
1.	Mencari Masalah dan dataset	☑	☐	☐	☐	☐	☐	Semua anggota
2.	Analisis kebutuhan	☑	☑	☐	☐	☐	☐	Semua anggota
3.	Preprocess	☐	☑	☑	☐	☐	☐	Maxi

	ing data							
4.	Pelatihan model Maching Learning	☑	☐	☑	☑	☑	☐	Maxi
5.	Penyusunan laporan	☐	☐	☐	☐	☑	☑	Semua anggota
6.	Pengujian prototype	☐	☐	☐	☐	☐	☑	Semua anggota

BAB 5
TINJAUAN ETIKA DAN KESELAMATAN

PhisInc dikembangkan berdasarkan keyakinan bahwa sistem ini dapat berperan sebagai lapisan pertahanan awal (first line of defense) bagi pengguna dalam menilai apakah suatu tautan berpotensi merupakan phishing atau tidak. PhisInc tidak dirancang untuk menjadi otoritas absolut dalam menentukan kebenaran suatu tautan, melainkan sebagai alat bantu pengambilan keputusan yang memberikan peringatan dini. Hal ini disadari karena PhisInc merupakan sistem berbasis kecerdasan buatan yang bekerja berdasarkan pola data historis, sehingga selalu memiliki kemungkinan kesalahan, baik berupa false positive maupun false negative. Oleh karena itu, sistem ini secara sadar tidak menjanjikan tingkat akurasi 100%. Meskipun demikian, penggunaan PhisInc diharapkan dapat secara signifikan menurunkan risiko pengguna terjebak dalam penipuan digital, khususnya yang memanfaatkan tautan phishing sebagai sarana utama.

Dalam proses pengembangan PhisInc, peneliti menerapkan pendekatan kolaborasi antara manusia dan AI (*Human–AI Collaboration*). AI digunakan sebagai *asisten pribadi* yang membantu peneliti dalam berbagai aspek teknis, seperti pengolahan data dalam jumlah besar, pelaksanaan perhitungan yang kompleks, eksplorasi pola, serta optimasi performa model pembelajaran mesin. Selain itu, AI juga dimanfaatkan untuk memberikan masukan awal terhadap ide-ide yang dikemukakan oleh peneliti, termasuk kemungkinan implementasi teknis dan potensi kelemahan desain. Namun demikian, seluruh hasil yang dihasilkan oleh AI tidak digunakan secara langsung tanpa evaluasi. Peneliti tetap memegang kendali penuh dalam menilai kelayakan ide, menetapkan batasan sistem, menentukan arsitektur, serta memilih dan memvalidasi model yang digunakan. Dengan demikian, AI berperan sebagai pendukung analitis, sementara tanggung jawab ilmiah dan etis sepenuhnya berada pada peneliti.

Dari sisi etika, PhisInc dikembangkan dengan prinsip bahwa ketidakpastian adalah bagian inheren dari sistem AI. Oleh karena itu, PhisInc tidak pernah memberikan penilaian yang bersifat menghakimi atau absolut terhadap suatu situs yang terdeteksi sebagai phishing. Sistem ini tidak melabeli situs tersebut sebagai “berbahaya secara pasti” atau “tidak layak diakses”, melainkan hanya memberikan peringatan berbasis probabilitas dan rekomendasi kehati-hatian. Pendekatan ini bertujuan untuk menghindari dampak negatif, seperti stigmatisasi terhadap situs yang sebenarnya sah namun terdeteksi secara keliru. PhisInc hanya menyarankan pengguna untuk tidak mengunjungi tautan yang terindikasi phishing, sembari tetap memberikan kebebasan kepada pengguna untuk mengambil keputusan akhir. Dengan

pendekatan ini, PhisInc menempatkan dirinya sebagai alat pendukung keamanan digital yang bertanggung jawab, bukan sebagai pengganti penilaian manusia.

BAB 6
DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Insiden Keamanan Siber Indonesia 2023*. Jakarta: BSSN Press.

Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques*. 3rd ed. Morgan Kaufmann.

Kaggle. (t.t.). *Phishing Website Detector*. Diakses pada 23 Oktober 2025, dari https://www.kaggle.com/datasets/eswarchandt/phishing-website-detector

Ma, J. F., & Zhou, Z. Z. (2018). Lexical and host-based feature analysis for effective URL phishing detection. *International Conference on Information Security and Cyber Crime*, 55-62.

Zhang, J., & Li, S. (2020). Phishing detection using machine learning and feature selection. *Journal of Cyber Security and Technology*, 7(2), 115-128.

LAMPIRAN

1. Website : https://phisinc.streamlit.app/
2. Video Demo : https://drive.google.com/file/d/1g-97QkhpALkl8WKZzCkgsOw6r0cDxhfs/view?usp=sharing