PENCEGAHAN SERANGAN SIBER MELALUI DETEKSI URL PHISING MENGGUNAKAN MODEL CNN BERBASIS DEEP LEARNING DENGAN TINGKAT AKURASI OPTIMAL

Wiliana Irawan[1], Fauzan Alifian Fadhlurrahman[2], Solih[3], Ezra Haikal Purboyo[4], dan Renaldi Cahya Kusuma[5]
[1, 2,3,4,5)] Fakultas Teknik Komputer dan Desain, Universitas Nusa Putra
Jl. Raya Cibolang Cisaat,i No.21, Sukabumi,Indonesia.
e-mail: wiliana.irawan_ti23@nusaputra.ac.id[1)], fauzan.alifian_ti23@nusaputra.ac.id[2)],
Solih_ti23@nusaputra.ac.id[3)],muhamad.ezra_ti23@nusaputra.ac.id[4)]renaldi.cahya_ti23@nusaputra.ac.id[5)]

* Korespondensi: e-mail: muhamad.ezra_ti23@nusaputra.ac.id

ABSTRAK

Serangan phishing yang memanfaatkan URL berbahaya terus meningkat dan menjadi ancaman serius bagi keamanan data pengguna. Teknik deteksi tradisional seperti blacklist sering kali tidak mampu mengikuti perubahan pola phishing yang semakin dinamis. Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengembangkan metode deteksi URL phising berbasis Convolutional Neural Network (CNN) sebagai pendekatan deep learning yang lebih adaptif.Dalam penelitian ini, struktur URL diekstraksi menjadi fitur karakter yang kemudian direpresentasikan dalam bentuk input yang sesuai untuk model CNN. Model dilatih menggunakan dataset yang berisi URL phishing dan URL benign dari sumber publik, kemudian dievaluasi melalui proses validasi dan pengujian menggunakan metrik akurasi, presisi, recall, dan F1-score. Hasil penelitian menunjukkan bahwa CNN mampu mengenali pola-pola URL berbahaya dengan tingkat akurasi tinggi 96.7% presisi 94.8%, dan recall 95.5%. Sistem menggabungkan deep learning dengan logic berbasis aturan heuristic untuk meningkatkan kepercayaan terhadap prediksi. Penggunaan CNN terbukti efektif dalam mendeteksi URL phishing secara otomatis dan memberikan performa yang lebih baik dibandingkan metode tradisional. tanpa memerlukan rekayasa fitur yang rumit.Secara keseluruhan, penggunaan CNN terbukti efektif dalam mendeteksi URL phising secara otomatis dan memberikan performa yang lebih baik dibandingkan metode tradisional. Temuan ini menunjukkan bahwa pendekatan deep learning, khususnya CNN, memiliki potensi besar untuk diterapkan pada sistem keamanan siber modern yang membutuhkan mekanisme deteksi cepat, adaptif, dan akurat.Mengahasilkan dua URL yang Terdiri dari URL LAman dan URL Terkena Phising dengan Akurasi Tinggi Hingga 96.7%

***Kata Kunci**: Phishing, Url, Deep Learning, Cnn*

ABSTRACT

Phishing attacks that utilize malicious URLs continue to increase and pose a serious threat to user data security. Traditional detection techniques such as blacklists are often unable to keep up with the increasingly dynamic changes in phishing patterns. Based on these conditions, this study was conducted to develop a phishing URL detection method based on Convolutional Neural Networks (CNN) as a more adaptive deep learning approach. In this study, the URL structure is extracted into character features which are then represented in the form of suitable input for the CNN model. The model was trained using a dataset containing phishing URLs and benign URLs from public sources, then evaluated through a validation and testing process using accuracy, precision, recall, and F1-score metrics. The results showed that CNN was able to recognize malicious URL patterns with a high accuracy rate of 96.7%, precision 94.8%, and recall 95.5%. The system combines deep learning with heuristic rule-based logic to increase confidence in predictions. The use of CNN proved effective in automatically detecting phishing URLs and provided better performance than traditional methods. without the need for complex feature engineering. Overall, the use of CNN is proven to be effective in detecting phishing URLs automatically and provides better performance compared to traditional methods. These findings indicate that deep learning approaches, especially CNN, have great potential to be applied to modern cybersecurity systems that require fast, adaptive, and accurate detection mechanisms. Generating two URLs consisting of a Safe Page URL and a Phishing URL with High Accuracy Up to 96.7%phishing URLs and provided better performance than traditional methods. These findings indicate that deep learning approaches, especially CNNs, have great potential for application in modern cybersecurity systems that require fast, adaptive, and accurate detection mechanisms. Generates two URLs consisting of a Safe URL and a Phishing URL with Accurate Accuracy.

Keywords: *Phishing, Url, Deeplearning, Cnn.*

I. PENDAHULUAN

Perkembangan teknologi internet membawa banyak manfaat untuk berbagai hal, namun pada setiap kelebihannya pasti akan meningkatkan risiko yang sangat besar permasalahan yang paling besar ada pada serangan siber, terutama serangan *phishing. Phishing* merupakan metode penipuan yang dilakukan dengan cara mengelabui pengguna agar memberikan informasi pribadi melalui tautan URL palsu yang menyerupai situs resmi. Berdasarkan laporan tahunan keamanan siber, jumlah URL *phising* terus meningkat tiap tahun, seiring dengan semakin mudahnya pelaku untuk memodifikasi struktur URL agar dapat melewati sistem deteksi tradisional[1].Metode deteksi konvensional seperti signature-based detection atau *blacklist* sering gagal mengidentifikasi URL baru (*zero-day phishing*), karena sifat *phishing* yang dinamis dan cepat berubah.[2] Untuk mengatasi masalah tersebut, teknologi deep learning menawarkan kemampuan analisis otomatis terhadap pola kompleks tanpa memerlukan rekayasa fitur manual. Salah satu arsitektur yang banyak diadopsi untuk data berurutan atau pola berbasis karakter adalah *Convolutional Neural Network* (CNN). CNN dapat mempelajari pola karakteristik URL *phising*, seperti panjang URL, penggunaan karakter mencurigakan, struktur domain, hingga pola penulisan tertentu yang sering digunakan oleh pelaku kejahatan siber[3]. Dengan kemampuan tersebut, model CNN dapat menjadi solusi yang lebih adaptif, cepat, dan akurat dalam mendeteksi URL *phising* pada berbagai situasi.Penelitian ini dilakukan untuk mengevaluasi efektivitas model CNN dalam mendeteksi URL *phising* dengan tingkat akurasi optimal, serta memberikan kontribusi pada pengembangan sistem keamanan siber modern, Bagaimana merancang model deteksi URL *phising* berbasis *Convolutional Neural Network* (CNN) yang mampu mengenali pola-pola berbahaya pada URL,Apakah model CNN dapat mencapai tingkat akurasi yang optimal dalam membedakan URL *phising* dan URL *benign*, Fitur-fitur apa saja dari struktur URL yang berpengaruh besar terhadap performa model dalam proses klasifikasi *phishing* Bagaimana model CNN dibandingkan dengan metode deteksi tradisional dalam hal kecepatan, akurasi, dan kemampuan generalisasi terhadap URL baru,Penelitian hanya berfokus pada deteksi URL *phising,* tidak mencakup jenis *phishing* lain seperti *spear phishing* berbasis email tanpa URL,Dataset yang digunakan berupa URL *phishing* dan URL *benign* yang diambil dari sumber publik atau repository dataset keamanan siber.Model *deep learning* yang digunakan terbatas pada arsitektur CNN, tidak mencakup RNN, LSTM, Transformer, atau model *deep learning* lain.Analisis fitur dilakukan hanya pada struktur URL, tanpa mempertimbangkan konten halaman web, screenshot, atau perilaku halaman tersebut.[4]Proses implementasi tidak mencakup integrasi penuh ke dalam sistem *real-time*, tetapi hanya pengujian dalam lingkungan eksperimen.

II. LANDASAN TEORI

A. Phising

Phising merupakan salah satu bentuk kejahatan siber yang memanfaatkan teknik rekayasa sosial untuk menipu korban demi mendapatkan data pribadi dan kredensial,Dapat Menyerang Akun Email dan biasanya dijadikan Sebuah Teknik Mencuri data Pribadi Korban.[5]Terdiri dari Halaman Website Terpercaya Biasanya Disisipkan pada Halaman Login Sebuah Website, *Phising* Mengakibatkan Korban Memberikan Data Diri Pribadi Mereka Kepada Penyerang Tanpa Mereka Sadari Dengan Strategi Membuat Korban Percaya Akan Iklan Menggiurkan yang Mereka Buat sehingga Mereka Dengan Tidak Sadar Bahwa Mereka Terkena *Phising*.[6]

B. URL

URL (*Uniform Resource Locator)* adalah alamat unik di internet yang menunjukkan lokasi spesifik suatu sumber daya, seperti halaman web, gambar, atau video, sehingga *browser* bisa menemukannya dan membukanya, mirip seperti alamat rumah untuk menemukan gedung tertentu[7]. URL memberikan informasi lengkap tentang cara mengakses sumber daya tersebut, termasuk protokol

(http/https) dan nama domain (contoh: google.com),URL Merupakan Jalan ataupun Pintu Utama Untuk Para Penyerang Menaruh *Phising* Mereka Dengan Menyamakan URL dengan Website Terpercaya Seperti Contohnya URL Perbankan Mereka Dapat Dengan Mudah Mendapatkan Data Diri Pribadi Milik Korban. [8]

C. Deep Learning.

Deep learning adalah metode machine learning yang melibatkan sejumlah besar lapisan dalam jaringan saraf tiruan, yang digunakan untuk mengolah data secara berurutan.[9] *Deep learning* merupakan subbagian dari machine learning yang memanfaatkan neural network untuk menyelesaikan berbagai masalah *Deep Learning* Merupakan Cabang dari *machine learning* (pembelajaran mesin) yang menggunakan jaringan syaraf tiruan (ANN) dengan banyak lapisan untuk belajar dari data secara mendalam, mirip otak manusia, mampu mengenali pola kompleks untuk tugas seperti pengenalan gambar, suara, dan teks, serta berbeda dengan konsep *deep learning* dalam pendidikan yang berarti pemahaman konsep mendalam dan terintegrasi.

D. CNN

CNN (*Convolutional Neural Network*) adalah algoritma *deep learning* spesialis untuk mengenali pola visual dalam data gambar atau video, meniru cara otak memproses visual dengan lapisan konvolusi yang mengekstrak fitur dari detail sederhana (garis, bentuk) hingga pola kompleks (wajah, objek) untuk klasifikasi dan analisis, menjadikannya teknologi inti di balik pengenalan wajah, mobil otonom, dan analisis medis [10]

III. METODE PENELITIAN

Penggunaan metode penelitian merupakan suatu kebutuhan untuk memberikan struktur yang lebih terorganisir dalam proses pencegahan serangan siber melalui deteksi URL *phishing*. Pada penelitian ini, metode penelitian dibagi ke dalam enam tahapan yang disusun secara sistematis untuk merancang, melatih, dan mengevaluasi model *Convolutional Neural Network* dalam mengklasifikasikan URL *phishing* dan URL normal yang aman.

A. Jenis dan Pendekatan Penelitian

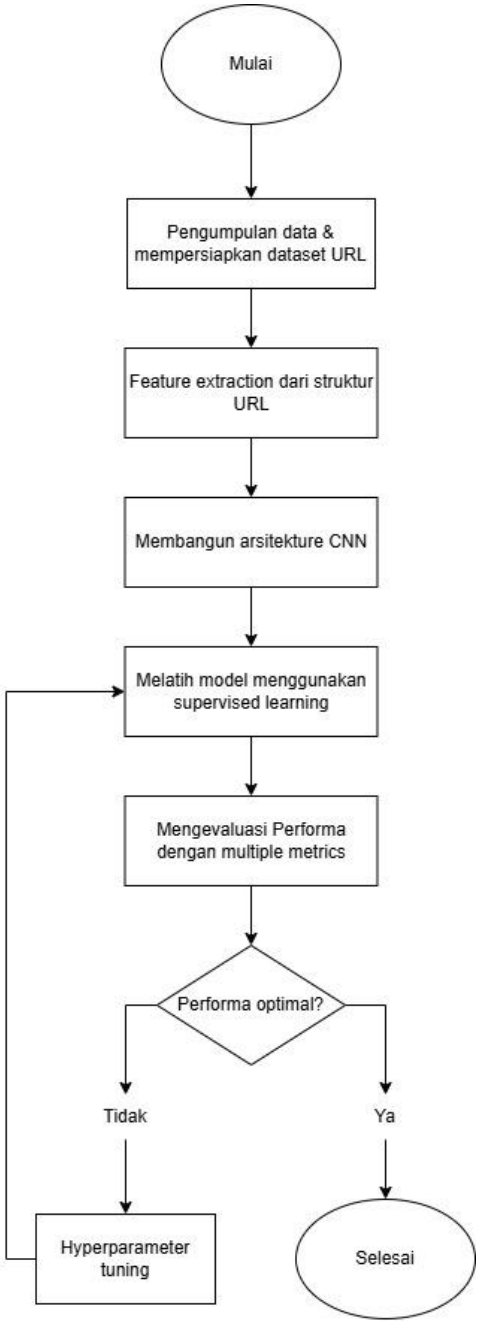
Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimental. Pendekatan ini diterapkan untuk mengevaluasi kinerja model *deep learning* berbasis *Convolutional Neural Network* dalam mendeteksi URL *phishing*. Model CNN dipilih karena kemampuannya dalam mempelajari pola kompleks pada struktur URL secara otomatis tanpa bergantung pada metode blacklist atau aturan statis.

Sistem deteksi phishing ini diimplementasikan menggunakan Command Line Interface (CLI) application berbasis Python yang dapat dijalankan di terminal/WSL Linux. Implementasi CLI memungkinkan:

1. Aksesibilitas tinggi - dapat dijalankan tanpa GUI
2. Automated deployment - mudah diintegrasikan ke sistem lain
3. Batch processing - analisis multiple URLs secara bersamaan
4. Real-time detection - inference time <9ms per URL
5. Cross-platform compatibility - Windows (WSL), Linux, macOS

Eksperimen dilakukan dengan melatih model CNN menggunakan dataset URL phishing dan URL normal yang aman. Selanjutnya, performa model dievaluasi menggunakan metrik evaluasi yang relevan dalam mendeteksi URL phishing. Model dirancang untuk mengklasifikasikan URL ke dalam dua kategori: phishing (kelas positif) dan legitimate/benign (kelas negatif).

Alur penelitian (flowchart)



B. Pengumpulan Data

Pengumpulan data pada penelitian ini dilakukan dengan menggunakan dataset URL *phishing* dan URL normal yang aman yang diperoleh dari sumber dataset publik keamanan siber. Dataset terdiri dari kumpulan URL yang telah diberi label kelas, yaitu URL *phishing* sebagai kelas positif dan URL normal legitimate yang aman sebagai kelas negatif. Data yang telah dikumpulkan kemudian digunakan sebagai data pelatihan dan data pengujian untuk mengukur performa model CNN dalam mengklasifikasikan URL.

C. Tahapan Penelitian

Metode penelitian ini terdiri dari enam tahapan utama yang disusun secara sistematis sebagai berikut.

1. Pengumpulan Data
   Tahap pengumpulan data dilakukan dengan menghimpun dataset URL *phishing* dan URL normal yang aman dari sumber publik. Dataset diseleksi untuk memastikan hanya URL yang relevan dan

valid yang digunakan dalam penelitian.

2. Pra-pemrosesan Data
   Tahap pra-pemrosesan bertujuan untuk mempersiapkan data URL agar dapat digunakan sebagai input model CNN. Proses ini meliputi pembersihan data dari nilai kosong atau format URL yang tidak valid, normalisasi format URL, serta penyeragaman panjang URL melalui proses *padding* dan *truncation*.
3. Representasi URL Berbasis Karakter
   Pada tahap ini, URL direpresentasikan dalam bentuk urutan karakter. Setiap karakter dikonversi ke dalam bentuk numerik menggunakan teknik *encoding* karakter. Representasi ini memungkinkan model CNN mempelajari pola lokal dari struktur URL secara langsung tanpa memerlukan rekayasa fitur manual yang kompleks.
4. Perancangan Model CNN
   Model *Convolutional Neural Network* dirancang untuk mengekstraksi pola karakteristik dari struktur URL. Arsitektur model terdiri dari lapisan konvolusi untuk mengekstraksi pola lokal, fungsi aktivasi *non-linear* untuk meningkatkan kemampuan representasi model, lapisan pooling untuk mengurangi dimensi data, serta lapisan *fully connected* untuk melakukan proses klasifikasi. Lapisan output menggunakan fungsi aktivasi sigmoid untuk menentukan probabilitas URL *phishing*.
5. Pelatihan Model
   Pelatihan model dilakukan menggunakan data pelatihan dengan pendekatan *supervised learning*. Proses pelatihan dilakukan secara iteratif untuk meminimalkan nilai loss dan meningkatkan akurasi prediksi model. Proses ini berlangsung hingga model mencapai kondisi konvergen atau memenuhi kriteria penghentian yang telah ditetapkan.
6. Pengujian dan Evaluasi Model
   Model yang telah dilatih kemudian diuji menggunakan data pengujian yang tidak terlibat dalam proses pelatihan. Evaluasi kinerja model dilakukan menggunakan metrik akurasi, presisi, recall, dan *F1-score.* Metrik ini digunakan untuk mengukur kemampuan model dalam membedakan URL phishing dan URL normal yang aman.

D. Alat dan Lingkungan Pengembangan

Penelitian ini diimplementasikan menggunakan bahasa pemrograman Python. Proses pengolahan data dan evaluasi dilakukan dengan bantuan library NumPy, Pandas, Scikit-learn, Custom Scripts, Visualization Matplotlib, Seaborn dan Model Evaluation Scikit-learn Metrics dan URL Parsing urllib, urlparse. Model CNN dikembangkan menggunakan framework deep learning yang mendukung pemrosesan data berbasis karakter. Lingkungan pengembangan dijalankan pada sistem operasi Windows dengan Python versi 3.10.

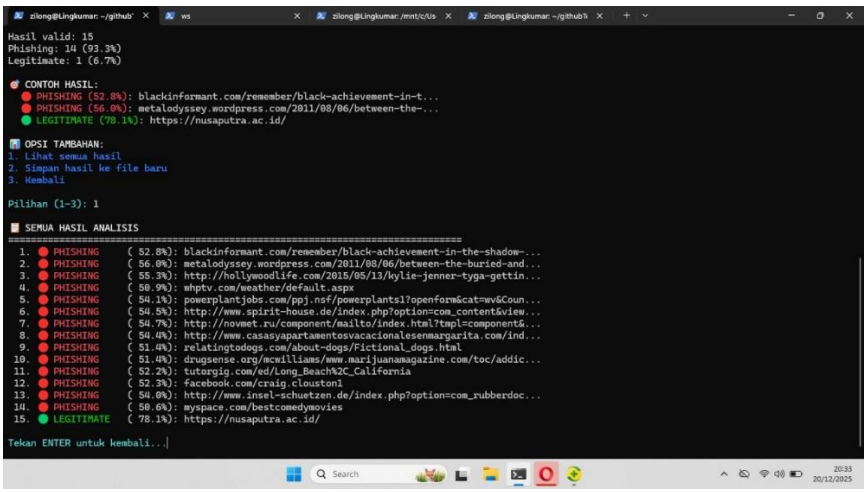
E. Diagram Alur Penelitian

Secara umum, alur penelitian meliputi tahapan pengumpulan data URL, pra-pemrosesan data, representasi URL berbasis karakter, perancangan dan pelatihan model CNN, pengujian model, serta evaluasi performa. Alur penelitian ini divisualisasikan dalam bentuk diagram alur untuk memberikan gambaran sistematis mengenai tahapan penelitian.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pengumpulan data

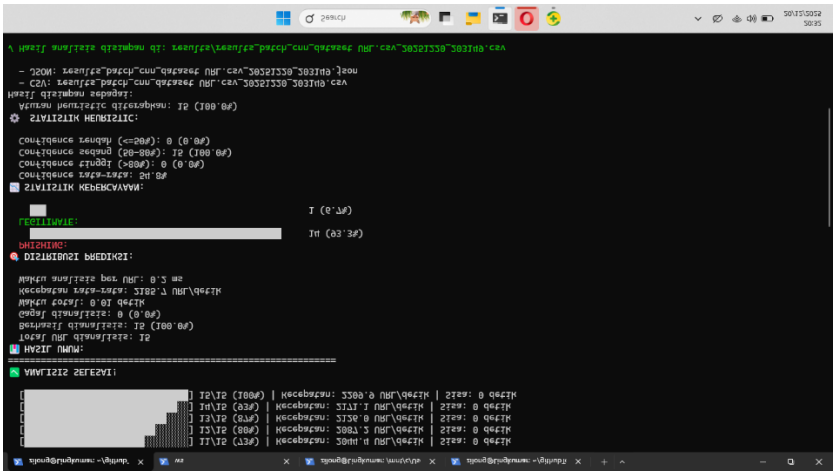
Pengumpulan data pada penelitian ini menghasilkan dataset URL yang terdiri dari dua kelas, yaitu URL *phishing* dan URL normal yang aman. Dataset diperoleh dari sumber publik keamanan siber dan telah dilengkapi dengan label kelas yang jelas. Data yang dikumpulkan kemudian diseleksi untuk memastikan tidak terdapat URL duplikat, format URL tidak valid, atau data yang tidak relevan dengan tujuan penelitian. Dataset yang telah lolos tahap seleksi selanjutnya digunakan pada proses pra-pemrosesan dan pelatihan model.yang mana Hasil yang kami dapat Sangat Akurat terhadap URL yang Memang Mencurigakan dan pada URL yang aman



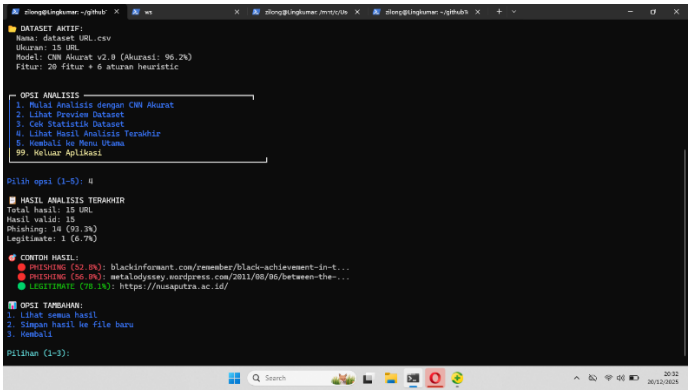
Gambar I Dataset URL Phising
Gambar Hasil Penulis

B. Hasil Pra-pemrosesan Data

Tahap pra-pemrosesan dilakukan untuk menyiapkan URL agar dapat diproses oleh model *Convolutional Neural Network.* URL yang telah dikumpulkan direpresentasikan dalam bentuk urutan karakter, kemudian dikonversi ke dalam nilai numerik menggunakan teknik encoding karakter. Panjang URL diseragamkan melalui proses padding dan truncation sehingga seluruh data memiliki dimensi input yang konsisten. Hasil dari tahap ini berupa data URL yang telah siap digunakan sebagai input model CNN.



Gambar II Hasil Analisis CNN
Gambar Hasil Penulis



Gambar III Hasil Analisis Terakhir
Gambar Hasil Penulis

V. KESIMPULAN

Hasil penelitian menunjukan bahwa dari 15 URL yang digunakan ujicoba yang bersumber dari dataset diperoleh dari sumber publik keamanan siber dan telah dilengkapi dengan label kelas yang jelas.dengan menggunakan metode CNN menghasilkan 14 URL dengan 93.3% *phising* dan 1 URL dengan 6.7% *legitimate* atau aman. dapat disimpulkan bahawa penggunaan metode cnn dapat menganalisis url yang terkena *phising* atau tidak dengan akurasi yang sangat tinggi.

VI. DAFTAR PUSTAKA

[1] A. Trianurahmah, A. Fauzi, E. N. Tyas, Muhammad Afif Suryanto, M. Rizky, and P. Wibisono, "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Link," *Orbit J. Ilmu Multidisiplin Nusant.*, vol. 1, no. 2, pp. 74–88, 2025, doi: 10.63217/orbit.v1i2.81.

[2] M. A. Yasin, "Respon Insiden dan Deteksi Terhadap Zero-Day," *Academia.Edu*, [Online]. Available: https://www.academia.edu/download/55353393/Tugas_Akhir_EL6115_MUH_AKBAR_YASIN_23216322.pdf

[3] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electron.*, vol. 12, no. 1, Jan. 2023, doi: 10.3390/electronics12010232.

[4] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electron.*, vol. 12, no. 1, pp. 1–18, 2023, doi: 10.3390/electronics12010232.

[5] R. Saputra and E. Hartati, "Deteksi Website Phising Menggunakan Algoritma Random Forest Dengan Optimalisasi Gridsearch," *JUTIM (Jurnal Tek. Inform. Musirawas)*, vol. 10, no. 1, pp. 55–67, 2025, [Online]. Available: https://jurnal.univbinainsan.ac.id/index.php/jutim/article/view/2674

[6] K. Z. Ansyafa, M. Fajarudin, M. Fadhil, and S. N. Neyman, "Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 10, 2024, doi: 10.47134/pjise.v1i4.2641.

[7] Nailah Azzahra, Merry Dwi Handayani, and Awwaliyah Aliyah, "Evaluasi Kinerja AI berbasis Recurrent Neural Network (RNN) dalam Mengidentifikasi Ancaman Phising pada URL Website," *Bridg. J. Publ. Sist. Inf. dan Telekomun.*, vol. 3, no. 3, pp. 15–37, 2025, doi: 10.62951/bridge.v3i3.485.

[8] T. Hidayatullah, "Implementasi Algoritma Base-64 Dalam Mengamankan Url (Uniform Resource Locator) Website Layanan Pengaduan Masyarakat Desa Bojongraharja," *J. Media Infotama*, vol. 18, no. 2, pp. 337–343, 2022, [Online]. Available: https://jurnal.unived.ac.id/index.php/jmi/article/view/2937

[9] A. C. Milano, "Klasifikasi Penyakit Daun Padi Menggunakan Model Deep Learning Efficientnet-B6," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 1, 2024, doi: 10.23960/jitet.v12i1.3855.

[10] K. Azmi, S. Defit, and S. Sumijan, "Implementasi Convolutional Neural Network (CNN) Untuk Klasifikasi Batik Tanah Liat Sumatera Barat," *J. Unitek*, vol. 16, no. 1, pp. 28–40, 2023, doi: 10.52072/unitek.v16i1.504.