ORIENTASI DAN KADERISASI 2025

UKM PENDIDIKAN DAN PENALARAN

PHISHIELD: WEBSITE BERBASIS *ARTIFICIAL INTELLIGENCE* PENJAGA GADGET DALAM MEMBONGKAR PENIPUAN ONLINE

Sub Tema: Kecerdasan Buatan (*Artificial Intelligence*)

Diusulkan oleh :

Rangga Prayata Utomo	254101070087
Daffa Achmad Choridha	254101050061
Zakira Aurelia Noviansyah	254205020110
Dafa Maulana	253101010053

POLITEKNIK NEGERI MALANG

JAWA TIMUR

MALANG

2025

PENDAHULUAN

Di tengah perkembangan teknologi digital yang sangat pesat terutama di negara berkembang seperti Indonesia, terdapat sebuah permasalahan kejahatan siber, yaitu penyebaran link atau file dari orang asing atau pihak-pihak tidak dikenal yang patut diperhatikan oleh pengguna gadget. Masalah ini seringkali muncul dalam bentuk tautan atau lampiran yang ketika diakses dapat menyebarkan virus atau memberikan dampak negatif lainnya pada perangkat, seperti kebocoran data atau gangguan fungsi. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, jumlah insiden keamanan siber di Indonesia mencapai lebih dari 1.000 kasus, di mana sebagian besar melibatkan *phishing* dan penyebaran *malware* melalui email atau pesan instan, dengan peningkatan yang terlihat sejak awal tahun tersebut akibat peningkatan aktivitas online selama pandemi (BSSN, 2023). Data dari Kementerian Komunikasi dan Informatika (Kominfo) mencatat 1.730 kasus penipuan online dari 2018 hingga 2023 dengan kerugian mencapai Rp 18,7 triliun, di mana 66,6% masyarakat pernah jadi korban dengan modus utama berupa hadiah palsu (36,9%), tautan berbahaya (33,8%), jual beli di Instagram (29,4%), dan sarana paling sering digunakan adalah jaringan seluler (64,1%), media sosial (12,3%), serta aplikasi percakapan (9,1%) (Septiani, 2023). Permasalahan ini semakin relevan karena masih banyak orang menerima pesan dari sumber anonim dengan sumber yang belum jelas. Hal ini dipengaruhi oleh kurangnya kesadaran masyarakat dalam mengenali ancaman digital sehingga menjadi mereka menjadi sasaran empuk bagi pelaku kejahatan siber.

Dalam menghadapi permasalahan ini, perlu adanya sistem yang mampu melindungi pengguna secara cepat dan otomatis. Teknologi kecerdasan buatan (*Artificial Intelligence*) menawarkan potensi kuat untuk mengidentifikasi URL atau file anonim yang sulit dideteksi oleh manusia dengan cara menganalisis pola yang tidak biasa dalam URL atau file yang ingin diakses. Melalui sistem analisis berbasis *machine learning*, AI dapat mengenali indikasi berbahaya seperti domain mencurigakan, permintaan izin berlebihan, hingga pola distribusi file yang menyerupai *malware*. Penelitian yang dilakukan oleh Rosanti et al. (2025), menunjukkan bahwa sistem deteksi phishing berbasis kecerdasan buatan (AI) yang dikembangkan sangat efektif dalam

mengidentifikasi serangan phishing. Dengan demikian, teknologi ini dapat menjadi solusi yang sangat relevan dalam menghadapi ancaman phishing.

Tujuan essay ini adalah untuk membahas permasalahan tersebut lebih jauh, sekaligus memperkenalkan sebuah solusi yang dinamakan *PhiShield*, sebuah website berbasis kecerdasan buatan yang dapat digunakan oleh pengguna gadget guna memeriksa link atau file sebelum diakses. Dengan *PhiShield*, pengguna bisa menyalin tautan atau mengirim file untuk analisis, sehingga membantu mencegah dampak buruk seperti infeksi virus. PhiShield memberikan manfaat dalam melindungi pengguna dari berbagai bentuk penipuan *online* melalui sistem deteksi cerdas berbasis kecerdasan buatan (AI). Hasil analisis ditampilkan secara jelas dalam bentuk peringatan atau rekomendasi keamanan sehingga pengguna dapat mengetahui tingkat risiko dari sebuah tautan atau aplikasi sebelum mengaksesnya. Dengan adanya fitur ini, pengguna dapat lebih berhati-hati dan terhindar dari tindakan gegabah seperti mengklik tautan mencurigakan atau menginstal aplikasi berbahaya. Dengan demikian, keamanan data pribadi dan perangkat pengguna dapat terjaga secara lebih optimal.

ISI

Di era digital saat ini, maraknya kasus penipuan online di Indonesia tidak hanya meresahkan masyarakat, tetapi juga memicu munculnya berbagai tindakan kriminal lainnya. Banyak pelaku memanfaatkan situasi ini untuk melakukan kejahatan berbasis digital, mulai dari penipuan berkedok promosi judi hingga pencurian data-data pribadi. Kondisi tersebut membuat masyarakat semakin rentan terhadap serangan kejahatan siber, salah satunya adalah bentuk penipuan online yang kini semakin beragam dan sulit dikenali. Penipuan online adalah tindakan jahat di dunia digital, di mana pelaku mencoba menipu orang lain untuk keuntungan pribadi, seperti mencuri data-data yang privasi ataupun sejumlah nominal uang yang dimiliki pengguna. Hal ini seringkali terjadi di internet, seperti pengiriman *email* atau pesan-pesan palsu. Selain itu, penipuan online seringkali menggunakan teknik *phishing* misalnya pelaku menjalin kepercayaan dengan meniru institusi terpercaya agar korban secara sengaja memberi informasi sensitif seperti kata sandi, nomor kartu kredit, atau data identitas pribadi.

Bentuk umum penipuan online bisa berbagai macam, misalnya *phishing link* yaitu penyebaran *link* palsu yang mengarah ke situs penipu, aplikasi bodong atau aplikasi yang terlihat resmi tapi berisi *malware*, dan *scam* pesan teks atau *email* yang meminta uang dengan alasan darurat. Data dari *FBI Internet Crime Report* 2023 menunjukkan bahwa *phishing* menyebabkan kerugian hingga 52 juta dollar di Amerika Serikat saja. Sharma et al. (2019) menjelaskan bahwa Serangan Phising sering menyamar sebagai sarana komunikasi yang sah untuk mencuri informasi rahasia, yang menyerupai pesan resmi untuk mencuri data atau informasi dari pengguna.

Kasus lain yang juga marak terjadi adalah aplikasi bodong atau *APK* berbahaya yang dikirim melalui pesan pribadi, *WhatsApp*, SMS, atau media sosial. *APK* ini sering kali memiliki nama dan ikon menyerupai aplikasi resmi sehingga korban percaya bahwa aplikasi tersebut aman. Setelah dipasang, aplikasi akan meminta akses ke *file*, kamera, mikrofon, hingga perbankan digital di perangkat korban. Akibatnya, pelaku dapat mengambil alih seluruh perangkat korban tanpa disadari.

Meskipun penipuan digital sudah menjadi topik umum, sebagian besar masyarakat masih belum memiliki literasi digital yang memadai sehingga mudah tertipu. Mereka tidak tahu cara memeriksa *link* aman, dan tertipu karena tampilan situs yang mirip aslinya seperti desain yang meniru bank atau pihak-pihak terkenal. Selain itu, trik *social engineering* yang menyerang mental seseorang untuk membuat orang tersebut panik dan percaya. Dalam penelitian Syahlendra, Wibisono, & Masriah (2025) menjelaskan bahwa *social engineering* menggunakan manipulasi psikologis untuk mengeksploitasi kepercayaan seseorang dengan tujuan memperoleh data pribadi seperti kata sandi atau akses sistem. Biasanya trik yang seperti ini memanfaatkan emosi manusia seperti rasa terburu-buru. Alhasil korban akan percaya dan masuk ke dalam perangkap penipu.

Dampak kerugian yang ditimbulkan dari penipuan *online* tergolong sangat besar, yang mencakup kerugian kehilangan uang, pencurian identitas pribadi, dan menyebabkan tekanan stres secara psikologis. Menurut data dari Europol tahun 2022, kerugian global dari *cybercrime* diperkirakan mencapai nilai yang tinggi yaitu €10 miliar per tahun. Dengan nilai kerugian sebesar itu, dampak yang dirasakan masyarakat sangat besar, bukan hanya kehilangan pekerjaan tetapi juga dpaat merusak kepercayaan masyarakat terhadap teknologi digital di masa depan.

Kecerdasan Buatan (*Artificial Intelligence*) membawa potensi besar dalam melindungi keamanan digital dari ancaman dan kejahatan online. *Artificial Intelligence* dikenal sebagai teknologi yang memungkinkan mesin belajar dan berpikir seperti manusia, misalnya mengenali pola rumit atau membuat keputusan berdasarkan data. Berdasarkan berbagai penelitian di Indonesia, *Artificial Intelligence* dianggap sebagai teknologi yang dirancang untuk meniru kemampuan manusia dalam berpikir, menganalisis, dan mengambil keputusan. Seperti yang dijelaskan oleh Tri Wahyudi pada tahun 2023, tujuan penggunaan *Artificial Intelligence* adalah untuk mengotomatisasi kegiatan yang biasanya memerlukan kecerdasan manusia, sehingga mesin bisa membantu proses pengambilan keputusan dengan lebih efisien. Dalam hal ini *Artificial Intelligence* memakai algoritma canggih untuk meniru kecerdasan manusia dalam mendeteksi atau memprediksi sesuatu, terutama ancaman siber.

Kemampuan *Artificial Intelligence* dalam mengenali pola menjadikannya sangat penting dalam melawan kejahatan online. Berbeda dengan sistem keamanan tradisional yang bergantung pada basis data ancaman yang sudah ada, *Artificial Intelligence* bisa memeriksa perilaku mencurigakan dalam jaringan atau *file* yang diunggah. Misalnya pada inovasi situs pendeteksi tautan berbahaya, *Artificial Intelligence* dapat diajarkan untuk memeriksa ribuan elemen dari sebuah *URL* seperti umur domain, kerapatan kata kunci, dan cara pengalihannya agar dapat menebak apakah itu *phishing* atau tidak, meskipun serangannya baru. Jadi, *Artificial Intelligence* tidak hanya merespon ancaman yang sudah terjadi tetapi juga secara aktif menemukan dan mengurangi risiko dengan kecepatan dan skala lebih besar daripada analis keamanan manusia, sehingga sangat meningkatkan pertahanan digital.

Artificial Intelligence dapat bekerja dengan menganalisis data besar, seperti memeriksa *link* untuk pola yang mencurigakan misalnya *URL* aneh atau *file* dengan kode berbahaya. Teknik yang digunakan adalah *Machine Learning* yang berguna untuk menganalisis data sederhana, dan *Deep Learning* untuk menganalisis pola kompleks, seperti penggunaan *neural network* untuk memproses teks atau gambar. Teknik kecerdasan buatan (*machine learning*) di Indonesia sendiri telah berhasil diterapkan untuk mendeteksi phishing dengan menganalisis fitur-fitur URL, seperti panjang *link*, penggunaan karakter khusus, struktur direktori, dan konten halaman (Rafi & Mujiastuti, 2025)

Peningkatan signifikan dalam serangan phishing menandakan kebutuhan akan sistem deteksi canggih yang tidak hanya cepat, tetapi juga memiliki tingkat akurasi tinggi. Penelitian oleh Fauzan, et al. (2025) menunjukkan bahwa algoritma klasifikasi seperti *Random Forest, Decision Tree, dan Naïve Bayes* dapat digunakan untuk mengidentifikasi *URL phishing* dengan efektif. Menurut hasil penelitian tersebut, model *Random Forest* menunjukkan performa terbaik dengan akurasi mencapai 97,2%, sementara *Decision Tree* berada di 96,3%, dan *Naïve Bayes* sekitar 85,3%.

Berdasarkan hasil penelitian tersebut, sebagai respon terhadap meningkatnya ancaman kejahatan siber, PhiShield dikembangkan sebagai sebuah platform keamanan siber berbasis AI yang menggabungkan kekuatan *machine learning* dan *deep learning*

untuk analisis ancaman secara *real-time*. Sistem ini dirancang untuk menganalisis link (*URL*) maupun *file* yang diterima pengguna, dengan tujuan mendeteksi apakah input tersebut aman atau mengandung potensi berbahaya. Dengan pendekatan otomatis dan responsif, *PhiShield* mampu menganalisa data dalam hitungan detik, memanfaatkan model yang telah dilatih berdasarkan temuan performa algoritma klasifikasi dari penelitian seperti Fauzan et al. (2025).

Secara teknis, PhiShield menerapkan modul khusus untuk analisis *URL*, di mana sistem mengevaluasi struktur tautan, panjang URL, keberadaan karakter khusus, dan elemen lainnya yang sering menjadi ciri khas phishing. Modul ini mirip dengan fitur numerik yang digunakan dalam penelitian akademik (seperti panjang *URL*, jumlah karakter, dan kata kunci) untuk ekstraksi fitur. Untuk analisis file, PhiShield menggunakan *deep learning* untuk melakukan pemindaian perilaku dan *signature malware*, kemudian menghasilkan laporan risiko yang detail mencakup skor bahaya, klasifikasi ancaman, dan rekomendasi mitigasi yang dapat dipahami pengguna dengan mudah.

Cara penggunaan PhiShield juga dibuat sangat sederhana agar dapat digunakan oleh berbagai kalangan, termasuk yang tidak memiliki latar belakang teknis. Pengguna cukup menempelkan link atau mengunggah file pada halaman utama website, kemudian menekan tombol “Scan”. Setelah itu, sistem AI akan memproses input dan menampilkan hasil berupa status “Aman” atau “Bahaya” lengkap dengan penjelasan spesifik. Mekanisme ini membantu pengguna menghindari ancaman siber secara proaktif, sehingga risiko akses ke konten berbahaya dapat dicegah sebelum terjadi kerugian yang lebih besar

PhiShield lebih unggul daripada cara manual karena ia lebih akurat, cepat, dan tidak bergantung pada pengetahuan dari pengguna saja karena Phishield berbasis kecerdasan buatan. Cara-cara manual yang digunakan seringkali salah karena manusia bisa sedang lelah atau kurang teliti, sedangkan AI belajar dari data besar untuk memberikan hasil yang konsisten. Tanpa adanya AI, pengguna akan menebak-nebak keamanan link berdasarkan intuisi, yang seringkali gagal karena *link* penipuan seringkali mirip dengan *link* asli. Dengan PhiShield, sistem otomatis akan menganalisis dalam

hitungan detik menggunakan *Machine Learning* untuk fitur sederhana dan *Deep Learning* untuk pola yang kompleks, yang kemudian memberikan akurasi hingga 95% seperti dalam penelitian Alghamdi et al. (2021).

PhiShield berpotensi memberikan dampak besar dalam mengurangi angka penipuan *online*. Dengan menyediakan platform yang mudah diakses, masyarakat dapat terbiasa memeriksa link dan file sebelum menggunakannya. Hal ini bukan hanya mencegah kerugian pribadi, tetapi juga membantu mengurangi penyebaran link berbahaya ke masyarakat lain. Di masa depan, PhiShield juga dapat dikembangkan menjadi aplikasi *mobile* atau ekstensi *browser* sehingga memberikan perlindungan langsung tanpa perlu membuka *website* secara terpisah. Selain itu, PhiShield dapat memanfaatkan data anonim untuk mempelajari pola penipuan yang sedang tren, lalu memberikan peringatan kepada pengguna mengenai modus baru yang sedang beredar.

PENUTUP

PhiShield merupakan inovasi website keamanan siber yang memanfaatkan kecerdasan buatan, khususnya machine learning dan deep learning, untuk memverifikasi keamanan tautan serta file dari pihak tidak dikenal. Masalah penyebaran link berbahaya dan malware yang kian marak dapat menyebabkan kebocoran data pribadi hingga kerugian finansial, sehingga PhiShield hadir sebagai solusi cerdas untuk mencegah dampak buruk kejahatan digital tersebut. Dengan menggunakan sistem analisis otomatis yang mampu mengenali pola phishing maupun indikasi virus secara real-time, website ini menawarkan perlindungan yang akurat sekaligus mudah digunakan oleh berbagai kalangan tanpa memerlukan keahlian teknis. Inovasi ini berpotensi memperkuat pertahanan pengguna gadget dengan menyediakan peringatan keamanan yang jelas sebelum akses dilakukan. PhiShield tidak hanya melindungi masyarakat dari risiko penipuan online dan pencurian identitas, tetapi juga membantu mengurangi ketergantungan pada pengecekan manual yang sering kali kurang optimal. Selain itu, PhiShield berkontribusi pada terciptanya lingkungan digital yang lebih aman di tengah tingginya aktivitas online masyarakat saat ini. Dengan demikian, PhiShield menjadi langkah awal menuju interaksi digital yang lebih aman.

DAFTAR PUSTAKA

DAHROUJ, H. et al., 2021. An Overview of Machine Learning-Based Techniques for Solving Optimization Problems in Communications and Signal Processing. *IEEE Access.*

Dattatraya, K. N., 2022. Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. *Journal of King Saud University - Computer and Information Sciences,* 34(3).

EduCSIRT Pusdatin Kemendikbud, 2024. *Lanskap Keamanan Siber 2023,* s.l.: http://educsirt.kemendikdasmen.go.id.

Fauzan, R. et al., 2025. Penerapan Algoritma Klasifikasi pada Machine Learning untuk Deteksi Phishing. *Indoneisan Journal of machine learning and Computer Science,* Volume 5 No. 2.

Rosanti, M. et al., 2025. IMPLEMENTASI SISTEM KEAMANAN SIBER BERBASIS ARTIFICIAL. *Aisyah Journal of Informatics and Electrical Engineering,* 7(1).

Sahfitri, A. & Rosmalinda, R., 2024. PENIPUAN DIGITAL MELALUI TAUTAN PHISHING. *JURNAL DIALEKTIKA HUKUM,* Volume 6 No. 2.

Septiani, L., 2023. *Kominfo Catatkan 1.730 Kasus Penipuan Online, Kerugian Ratusan Triliun,* s.l.: katadata.co.id.

Wahyudi, T., 2023. STUDI KASUS PENGEMBANGAN DAN PENGGUNAAN ARTIFICIAL INTELLIGENCE (AI) SEBAGAI PENUNJANG KEGIATAN MASYARAKAT INDONESIA. *JURNAL INDONESIA TEKNIK PERANGKAT.*

Lampiran

A. Lampiran biodata Ketua

A. Identitas Diri

1	**Nama Lengkap**	**Rangga Prayata Utomo**
2	**Jenis kelamin**	**Laki-laki**
3	**Program Studi**	**DIV - Teknik Elektronika**
4	**NIM**	**254101070087**
5	**Tempat dan Tanggal Lahir**	**Mojokerto, 14 Februari 2006**
6	**Alamat E-mail**	**ranggaprayatautomo@gmail.com**
7	**Nomor Telepon/HP**	**087862241062**

B. Kegiatan Kemahasiswaan yang Sedang/Pernah Diikuti

No	Nama Kegiatan	Status Dalam Kegiatan	Waktu dan Tempat
1			

C. Penghargaan yang Pernah Diterima

No	Jenis Penghargaan	Pihak Pemberi Penghargaan	Tahun
1			

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan pengumpulan *Essay*.

Malang, 18, November 2025

Ketua

(Rangga Prayata Utomo)

B. Lampiran biodata Anggota

A. Anggota 1

1	**Nama Lengkap**	**Daffa Achmad Choiridha**
2	**Jenis kelamin**	**Laki-laki**
3	**Program Studi**	**D-IV Sistem Kelistrikan**
4	**NIM**	**254101050061**
5	**Tempat dan Tanggal Lahir**	**Bojonegoro, 19 Juli 2007**
6	**Alamat E-mail**	**achmadcdaffa19@gmail.com**
7	**Nomor Telepon/HP**	**081392292950**

B. Anggota 2

1	**Nama Lengkap**	**Zakira Aurelia Noviansyah**
2	**Jenis kelamin**	**Perempuan**
3	**Program Studi**	**D-IV Akuntansi Manajemen**
4	**NIM**	**254205020110**
5	**Tempat dan Tanggal Lahir**	**Malang, 17 November 2006**
6	**Alamat E-mail**	**zakira2006aurelia@gmail.com**
7	**Nomor Telepon/HP**	**081248021461**

C. Anggota 3

1	**Nama Lengkap**	**Daffa Maulana**
2	**Jenis kelamin**	**Laki-laki**
3	**Program Studi**	**DIII- Teknik Elektronika**
4	**NIM**	**254101010053**
5	**Tempat dan Tanggal Lahir**	**Malang, 9 September 2006**
6	**Alamat E-mail**	**Anafidia0101@gmail.com**
7	**Nomor Telepon/HP**	**0895618073010**