(2024), 2 (8): 103–107 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

Penerapan Teknologi AI dalam Deteksi dan Pencegahan Ancaman Terhadap File

Arya Hadid Pangestu[1], Muhammad Abbas Adika[2], Alan Setiyawan[3], Edy Waluyo[4], Ridwan Prasetyo[5], Raka Rossian Saputra[6]
[1,2,3,4,5,6,]Teknik Industri, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya
e-mail: [1]202210215058@mhs.ubharajaya.ac.id, [2]202210215201@mhs.ubharajaya.ac.id, [3]202210215056@mhs.ubharajaya.ac.id, [4]202210215051@mhs.ubharajaya.ac.id, [5]202210215044@mhs.ubharajaya.ac.id, [6]202210215042@mhs.ubharajaya.ac.id,

* Korespondensi author: tubagus.hedi@dsn.ubharajaya.ac.id

Abstract
This research aims to explore the application of AI technology in the detection and prevention of threats to files, identifying the benefits it offers, as well as the challenges that must be overcome. The author applies qualitative research methods and conducts a literature study evaluating literature and journals that are in accordance with the theory discussed, especially in the scope of Security Management and Information Systems. The results of the research on the use of AI technology involve machine learning techniques, deep learning, and big data analysis to provide a broad view of potential threats. However, the implementation of AI technology in file security faces challenges such as the need for quality training data, high computing resources, and specialised expertise. Therefore, there is a need for necessary applications including Stateful Firewall for network surveillance, AI-IDS for cyber threat detection, and cryptography for data security. The incorporation of AI into this system increases the efficiency of the technology in dealing with cyber threats.

Article History
Submitted: 14 June 2024
Accepted: 23 June 2024
Published: 24 June 2024

Key Words
Artificial Intelligence (AI), Digital, File Security

Abstrak
Penelitian ini bertujuan untuk mengeksplorasi penerapan teknologi AI dalam deteksi dan pencegahan ancaman terhadap file, mengidentifikasi manfaat yang ditawarkannya, serta tantangan yang harus diatasi. Penulis menerapkan metode penelitian kualitatif dan melakukan studi Pustaka Mengevaluasi literatur dan jurnal yang sesuai dengan teori yang dibahas, khususnya dalam lingkup Manajemen Keamanan dan Sistem Informasi. Hasil penelitian penggunaan teknologi AI melibatkan teknik *machine learning*, *deep learning*, dan analisis *big* data untuk memberikan pandangan luas tentang potensi ancaman. Meskipun demikian, implementasi teknologi AI dalam keamanan file menghadapi tantangan seperti kebutuhan akan data pelatihan yang berkualitas, sumber daya komputasi tinggi, dan keahlian khusus. Oleh karena itu, perlu adanya sebuah aplikasi yang diperlukan termasuk *Stateful Firewall* untuk pengawasan jaringan, AI-IDS untuk mendeteksi ancaman siber, dan kriptografi untuk keamanan data. Penggabungan AI ke dalam sistem ini meningkatkan efisiensi teknologi dalam menghadapi ancaman *cyber*.

Sejarah Artikel
Submitted: 14 June 2024
Accepted: 23 June 2024
Published: 24 June 2024

Kata Kunci
Kecerdasan Buatan (AI), Digital, Keamanan File

PENDAHULUAN

Dalam era digital yang terus berkembang, keamanan data dan file menjadi prioritas utama bagi individu dan organisasi. Ancaman siber yang semakin kompleks dan canggih menuntut para profesional keamanan untuk mengadopsi teknologi yang lebih maju dalam melindungi informasi sensitif. Salah satu teknologi yang kini menjadi sorotan dalam bidang keamanan siber adalah kecerdasan buatan (*Artificial Intelligence*/AI). Teknologi ini telah menyentuh hampir setiap aspek kehidupan kita, termasuk dalam sistem informasi. (Wulantari et al., 2023). AI menawarkan potensi besar dalam mendeteksi dan mencegah ancaman terhadap file dengan efisiensi dan efektivitas yang lebih unggul dibandingkan dengan metode konvensional.

Selama beberapa tahun belakangan ini, penerapan AI dalam pengamanan sistem informasi sudah tumbuh secara eksponensial. Keberhasilan teknologi ini dalam memproses data besar dan kompleks, mengenali pola, serta menghasilkan wawasan berharga telah membuka berbagai peluang baru (Tambos, 2023). Kecerdasan buatan, dengan kemampuannya untuk belajar dari data dan membuat prediksi berdasarkan pola yang dikenali, telah membuktikan kehandalannya dalam berbagai aplikasi, mulai dari pengenalan wajah hingga pengolahan bahasa alami.

Dalam konteks keamanan file, AI dapat digunakan untuk menganalisis pola akses file, mendeteksi aktivitas yang mencurigakan, serta mengidentifikasi potensi ancaman sebelum mereka dapat menyebabkan kerugian yang signifikan (Diaba et al., 2023). Para penyerang berupaya mengeksploitasi keterbukaan dan kekurangan dalam sistem tersebut untuk merampas data rahasia, membuat operasi terganggu, atau mencemari dengan *software* berbahaya. Serangan macam itu dapat menyebabkan kerugian finansial, penurunan reputasi dan yang paling memprihatinkan, kemungkinan penyalahgunaan informasi (Omer et al., 2023).

Penggunaan teknologi AI dalam deteksi dan pencegahan ancaman terhadap file mencakup berbagai teknik, seperti *machine learning*, *deep learning*, dan analisis *big* data. Dengan algoritma *machine learning*, sistem keamanan dapat dilatih untuk mengenali perilaku normal pengguna dan file, sehingga dapat mendeteksi anomali dengan cepat. *Deep learning*, yang merupakan salah satu bagian dari *machine learning*, memungkinkan pengetahuan pola yang lebih kompleks dan mendalam, sehingga mampu mengidentifikasi ancaman yang lebih tersembunyi. Selain itu, analisis *big* data memungkinkan pengolahan dan interpretasi data dalam jumlah besar, Menyediakan pandangan yang lebih luas dan mendalam tentang potensi ancaman.

Namun, penerapan teknologi AI dalam keamanan file juga menghadapi berbagai tantangan. Salah satunya adalah kebutuhan akan data pelatihan yang berkualitas dan representatif untuk menghindari bias dan memastikan keakuratan deteksi. Selain itu, ancaman siber yang terus berkembang mengharuskan sistem AI untuk selalu diperbarui dan ditingkatkan. Integrasi AI dalam sistem keamanan juga memerlukan sumber daya komputasi yang tinggi serta keahlian khusus dalam bidang data science dan keamanan siber.

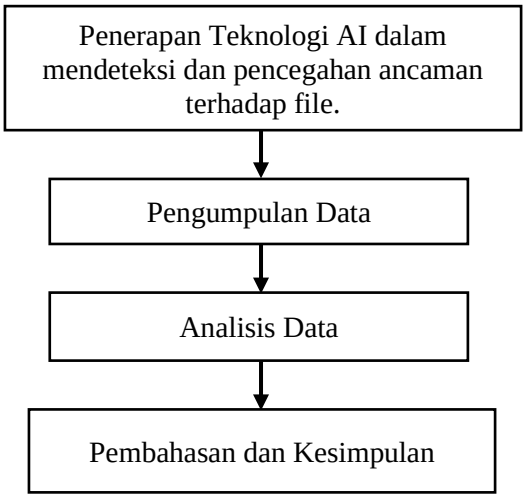
Penelitian ini akan mengeksplorasi penerapan teknologi AI dalam deteksi dan pencegahan ancaman terhadap file, mengidentifikasi manfaat yang ditawarkannya, serta tantangan yang harus diatasi. Dengan memahami dinamika ini, diharapkan dapat diperoleh wawasan yang lebih baik mengenai bagaimana AI dapat dioptimalkan untuk meningkatkan keamanan data dan file dalam lingkungan digital yang terus berkembang.

METODE PENELITIAN

Analisis dalam penelitian ini adalah tentang Penerapan AI dalam mendeteksi dan mencegah ancaman terhadap file. Penulis menerapkan metode penelitian kualitatif dan melakukan studi pustaka (*Library Research*). Mengevaluasi literatur dan jurnal yang sesuai dengan teori yang dibahas, khususnya dalam lingkup Manajemen Keamanan dan Sistem Informasi. Semua artikel ilmiah yang dikutip berasal dari Mendeley, Google Scholar, dan sumber online lainnya. Salah satu alasan utama untuk melakukan penelitian kualitatif adalah karena penelitian tersebut sifat eksploratifnya. (Ali & Limakrisna, 2013).

Fokus dalam penelitian ini adalah pada keadaan asli atau keadaan alamiah (natural setting), di mana data disajikan tanpa diubah menjadi simbol atau angka. Penelitian ini fokus kepada: (1) Penerapan Teknologi AI (2) Deteksi dan Ancaman Terhadap File. Berdasarkan rumusan masalah dan analisis literatur sebelumnya berikut ini kerangka penelitian tentang Penerapan Teknologi Ai dalam medeteksi dan mencegah ancaman terhadap file :

(2024), 2 (8): 103–107 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi



Gambar 1 Kerangka Penelitian

HASIL DAN PEMBAHASAN

Penelitian dengan menggunakan metode kualitatif dengan pendekatan *review journal* yang diambil dari beberapa penelitian dan dapat disimpulkan melalui pendapat-pendapat yang diberikan oleh peneliti terdahulu mengenai seputar teknologi AI. Berikut adalah hasil dari penelitian-penelitian terdahulu:

Tabel 1. Hasil Penelitian Terdahulu

Judul	Penulis	Hasil Penelitian
Pengetahuan Dasar untuk Mengidentifikasi dan Mendeteksi Serangan Kejahatan Siber Secara Dini Mencegah Terjadinya Pencurian Data Perusahaan 1	(Laksana & Mulyani, 2024)	Peneliti menjelaskan bahwasannya sertifikasi dan pelatihan khususnya dalam bidang AI atau *Cyeber Crime* karena bisa meningkatkan keterampilan dan keamanan siber dalam mencegah atau meminimalisir risiko penyerangan kejahatan siber di perusahaan.
Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan 2	(Firmansyah et al., 2024)	Peneliti menjelaskan bahwasannya dalam mencegah ancaman data siber perlu dibuatkannya aplikasi seperti pencegah virus tetapi selain dari itu harus dibentuknya AI sebagai proteksi dalam menanggulangi ancaman siber, dibentuknya AI sebagai proteksi pencegahan kejahatan siber karena seiring maju nya teknologi dan rekayasa yang harus dikembangkan menjadi lebih baik.
AI Shield: Protecting Business Data from Cybercrime 2	(Putri & Aswar, 2023)	Peneliti menjelaskan bahwasannya

Judul	Penulis	Hasil Penelitian
		pengkolaborasikan aplikasi seperti *Stateful Firewall*, AI-IDS, dan Kriptografi dengan AI sangatlah penting, karena dapat mendeteksi kegiatan mencurigakan dan membuat kode kode tertentu serta pengawasan jaringan yang dapat menguntungkan perusahaan dalam mengawasi dan mencegah ancaman siber dan kebocoran data.
Penerapan Artificial Intelligence Pada Pendidikan Dalam Zaman Industri 4.0 1	(Maola et al., 2024)	Peneliti menjelaskannya bahwasannya memberikan Pendidikan seputar AI pada generasi 4.0 dapat meningkatkan kemampuan dan kinerja pada semua orang, semua orang harus melek akan teknologi yang semakin banyak dikembangkan dan lebih di tingkatkan dalam penciptaan aplikasinya.
Keamanan Perangkat Lunak: Tantangan Dan Solusi Terkini	(Pratama, 2024)	Peneliti mengatakan bahwa perlunya solusi dalam menciptakan teknologi khususnya AI, karena seiring majunya teknologi pastinya saja semakin banyaknya teknologi terbarukan dalam mencegah kejahatan siber.

Hasil dari studi literatur menggunakan berbagai jenis penelitian yang dilakukan oleh pendahulu mengenai tentang penerapan AI untuk mencegah dari ancaman kejahatan siber dalam file adalah sebagai berikut:

1. Awal dari pengembangan dan pembentukan AI yaitu dengan memberikan edukasi dan doktrin seputar apa saja yang ada di AI dan algoritma apa saja yang digunakan, untuk melalui ini bisa dengan menempuh pendidikan salah satunya sertifikasi dan pelatihan mengenai pencegahan kejahan siber ataupun tentang AI.
2. Solusi dalam pencegahan agar tidak terjadi banyaknya ancaman ataupun serangan file perlunya juga dibuatnya aplikasi pengendali virus dan ancaman lainnya, dan jika terjadi ancaman baru dan sudah tidak bisa dikendalikan maka perlunya kolaborasi antara AI dan aplikasi tersebut.
3. Aplikasi yang dimaksud adalah aplikasi yang bisa membaca dan mendeteksi jaringan sebagai contoh *Stateful Firewall* yang berfungsi untuk mengawasi jaringan agar tidak terjadi masuknya jaringan mencurigakan, AI-IDS yaitu aplikasi yang digunakan untuk mengawasi keluar masuknya data sehingga dapat menyaring ancaman siber yang mencurigakan dan kriptografi yaitu aplikasi yang membuat sistem keamanan dengan cara membentuk tanda seperti kode morse. Ketiga aplikasi tersebut bisa lebih di kembangkan lebih lanjut menjadi AI yang satu tetapi fungsinya masih sama supaya tidak terjadi ketidakefisiensian penggunaan teknologi, dari sini kita dapat bahwasannya penerapan AI dalam mencegah ancaman siber yaitu dengan cara di kembangkan kembali sistem AI dengan mengkolaborasikan berbagai aplikasi.

KESIMPULAN

Penelitian kualitatif dipilih karena sifat eksploratifnya, yang memungkinkan peneliti untuk mempelajari secara menyeluruh aspek penerapan AI dan deteksi ancaman terhadap file dengan mengumpulkan data dalam keadaan kewajaran (natural setting). Pendidikan tentang konsep dan penggunaan algoritma AI dimulai dengan pengembangan AI. Untuk menangani ancaman kejahatan siber secara efektif, pendidikan dan sertifikasi diperlukan. Solusi pencegahan termasuk pengembangan aplikasi pengendali virus dan ancaman lainnya. Untuk menangani ancaman yang sulit dikendalikan, AI dan aplikasi ini harus bekerja sama. Aplikasi yang diperlukan termasuk Stateful Firewall untuk pengawasan jaringan, AI-IDS untuk mendeteksi ancaman siber, dan kriptografi untuk keamanan data. Penggabungan AI ke dalam sistem ini meningkatkan efisiensi teknologi dalam menghadapi ancaman *cyber*.

DAFTAR PUSTAKA

Diaba, S. Y., Anafo, T., Tetteh, L. A., Oyibo, M. A., Alola, A. A., Shafie-khah, M., & Elmusrati, M. (2023). SCADA securing system using deep learning to prevent cyber infiltration. *JURNAL ILMIAH INFORMATIKA GLOBAL*, *14*(2), 321–332.

Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (2024). Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan. *JKMT : Jurnal Kewirausahaan Dan Multitalenta*.

Laksana, T. G., & Mulyani, S. (2024). PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN. *JUKIM : Jurnal Ilmu Multidisiplin*.

Maola, P. S., Handak, I. S. K., & Herlambang, Y. T. (2024). Penerapan Artificial Intelligence Dalam Pendidikan Di Era Revolusi Industri 4.0 . *Educatio: Jurnal Ilmu Kependidikan* .

Omer, N., Samak, A. H., Taloba, A. I., & Abd El-Aziz, R. M. (2023). A novel optimized probabilistic neural network approach for intrusion detection and categorization. *JURNAL ILMIAH INFORMATIKA GLOBAL*, *14*(2), 351–361.

Pratama, D. N. (2024). KEAMANAN PERANGKAT LUNAK: TANTANGAN DAN SOLUSI TERKINI. *Jurnal Dunia Data*.

Putri, A. A., & Aswar, M. A. (2023). AI Shield: Protecting Business Data from Cybercrime. *Prosiding Seminar Nasional Ilmu Manajamen, Ekonomi, Keuangan Dan Bisnis*.

Tambos, C. A. (2023). Insinyur Teknik Informatika: Kini Dan Masa Depan. *Jurnal Kependudukan Dan Pembangunan Lingkungan*, *4*(1), 65–74.

Wulantari, N. P., Rachman, A., Sari, M. N., ktolseja, L. J., & Rofi'i, A. (2023). The Role Of Gamification In English Language Teaching: A Literature Review. *Journal On Education*, *6*(1), 2847–2856.