JIMU: Jurnal Ilmiah Multidisipliner
Vol. 04 No. 01, Tahun 2025, Hal. 2614-2622 e-ISSN: 3031-9498

Perancangan Sistem Keamanan Jaringan Menggunakan *Instruction Detection System* (IDS) Berbasis AI (*Artificial Intelligence*)

Muhammad Genta Dwiputra[1], Ikhwan Fadhilah Putra[2], Reva Arati Manik[3], Samso Supriyatna[4]

Progam Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang

Email: gentadwi0305@gmail.com[1], putraikhwan76@gmail.com[2],revamanik90@gmail.com[3], dosen02830@unpam.ac.id[4]

Article Info

Article history:

Received Desember 10, 2025
Revised Desember 21, 2025
Accepted Desember 23, 2025

Keywords:

Network Security, Intrusion Detection System, Artificial Intelligence, Machine Learning.

ABSTRACT

The rapid development of computer network technology is accompanied by an increasing number of cyber threats that require reliable and adaptive network security systems. Attacks such as Denial of Service (DoS), malware, and unauthorized access can threaten data security and network stability. Conventional security mechanisms such as firewalls are considered insufficient to detect attacks quickly and accurately. Therefore, an automatic intrusion detection system, known as an Intrusion Detection System (IDS), is needed. This study aims to develop a network security system using an Artificial Intelligence-based Intrusion Detection System (IDS). The research method used is a quantitative approach with an experimental method. The data used in this study were obtained from public IDS datasets, namely NSL-KDD and CICIDS2017. The data processing stages include preprocessing, data splitting into training and testing sets, machine learning model training, and system evaluation using performance metrics such as accuracy, precision, recall, and F1-score.

Article Info

Article history:

Received Desember 10, 2025
Revised Desember 21, 2025
Accepted Desember 23, 2025

Keywords:

Keamanan Jaringan, Intrusion Detection System, Artificial Intelligence, Machine Learning, IDS..

ABSTRACT

Perkembangan teknologi jaringan komputer yang semakin pesat seiring dengan meningkatnya ancaman serangan siber menuntut adanya sistem keamanan jaringan yang andal dan adaptif. Serangan seperti *Denial of Service* (DoS), *malware*, dan akses tidak sah dapat mengancam keamanan data serta kestabilan sistem jaringan. Penggunaan mekanisme keamanan konvensional seperti firewall dinilai belum cukup untuk mendeteksi serangan secara cepat dan akurat. Oleh karena itu, diperlukan sebuah sistem yang mampu melakukan pendeteksian intrusi secara otomatis, yaitu *Intrusion Detection System* (IDS). Penelitian ini bertujuan untuk mengembangkan sistem keamanan jaringan menggunakan *Intrusion Detection System* (IDS) berbasis *Artificial Intelligence* (AI). Metode penelitian yang digunakan adalah metode kuantitatif dengan pendekatan eksperimen. Data yang digunakan berasal dari dataset publik IDS, yaitu NSL-KDD dan CICIDS2017. Proses pengolahan data meliputi tahap *preprocessing*, pembagian data latih dan data uji, pelatihan model *machine learning*, serta pengujian sistem menggunakan metrik evaluasi berupa akurasi, *precision*, *recall*, dan *F1-score*.

JIMU: Jurnal Ilmiah Multidisipliner
Vol. 04 No. 01, Tahun 2025, Hal. 2614-2622 e-ISSN: 3031-9498

Corresponding Author:

Muhammad Genta Dwiputra[1]
Universitas Pamulang, Indonesia
Email: gentadwi0305@gmail.com

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat membawa banyak manfaat dalam mendukung aktivitas manusia di berbagai bidang, mulai dari pendidikan, bisnis, pemerintahan, hingga layanan publik. Namun, kemajuan tersebut juga diiringi dengan meningkatnya ancaman keamanan siber, seperti serangan malware, *denial of service* (DoS), phishing, hingga intrusi pada jaringan komputer. Serangan-serangan ini dapat menyebabkan kebocoran data, kerugian finansial, bahkan merusak reputasi suatu institusi.

Salah satu upaya yang banyak dikembangkan untuk mengatasi masalah ini adalah penggunaan *Intrusion Detection System* (IDS)**,** yaitu sistem yang berfungsi untuk mendeteksi aktivitas mencurigakan atau berbahaya pada jaringan komputer. IDS tradisional biasanya mengandalkan aturan statis (rule-based), sehingga sering kali kurang efektif dalam mendeteksi serangan baru (zero-day attack) atau pola intrusi yang lebih kompleks.

Berkembangnya teknologi *Artificial Intelligence* (AI), khususnya *machine learning* dan *deep learning*, IDS dapat dikembangkan agar lebih cerdas dalam mengenali pola serangan. Model AI mampu belajar dari dataset serangan jaringan, kemudian mengklasifikasikan aktivitas jaringan apakah normal atau merupakan intrusi. Hal ini menjadikan IDS berbasis AI lebih adaptif, akurat, dan mampu memberikan deteksi lebih dini terhadap potensi ancaman.

Penelitian ini akan berfokus pada pengembangan sistem IDS berbasis AI dengan memanfaatkan dataset keamanan jaringan, sehingga diharapkan mampu menghasilkan model deteksi intrusi yang efektif dan dapat menjadi dasar bagi pengembangan sistem keamanan jaringan yang lebih komprehensif di masa depan.

Berdasarkan latar belakang di atas, permasalahan yang dapat di ideentifikasi adalah sebagai berikut: 1) Masih sering terjadi ancaman keamanan pada jaringan universitas yang tidak terdeteksi secara dini. 2) Diperlukan metode yang mampu meningkatkan akurasi dan kecepatan deteksi serangan jaringan. 3) Belum diterapkannya algoritma machine learning seperti Random Forest dalam sistem IDS universitas. 4) Perlunya evaluasi kinerja metode Random Forest agar dapat dijadikan acuan pengembangan sistem keamanan jaringan selanjutnya.

Masalah- masalah yang akan di pecahkan di dalam penelitian ini yaitu 1) Bagaimana merancang dan mengembangkan system Instrusion Detection System berbasis AI untuk mendeksi instruksi jaringan, 2) Algoritma AI apa yang paling efektif digunakan dalam mendeteksi serangan jaringan dalam akurasi tinggi, 3) Bagaimana performa IDS berbasis AI yang di bangun di bandingkan dengan metode deteksi intrusi tradisional.

Agar penelitian lebih terarah dan tidak menyimpang dari tujuan utama, maka batasan masalah dalam penelitian ini adalah 1) Penelitian hanya berfokus pada penerapan metode Random Forest untuk mendeteksi intrusi jaringan. 2) Dataset yang digunakan bersumber dari dataset publik IDS seperti *NSL-KDD* atau *CICIDS2017*. 3) Analisis kinerja difokuskan pada nilai akurasi, precision, recall, dan F1-score. 3) Penelitian dilakukan dalam bentuk simulasi atau model eksperimental, bukan implementasi langsung di jaringan universitas sebenarnya

LANDASAN TEORI

1. **Pengertian Keamanan Jaringan**
   Menurut [2] Keamanan jaringan merupakan suatu sistem yang bertujuan untuk mencegah aktivitas yang tidak diinginkan dengan cara mengidentifikasi pengguna yang tidak memiliki hak akses dalam jaringan. Saat menghubungkan komputer ke dalam jaringan, baik menggunakan kabel maupun nirkabel
2. **Pengertian *Intrusion Detection System* (IDS)**
   Menurut [2]Intrusion Detection System (IDS) ialah sebuah sistem yang khusus dirancang untuk mengenali aktivitas yang mencurigakan pada jaringan komputer atau sistem komputer. Sistem ini bertugas memantau lalu lintas jaringandan aktivitas sistem guna mendeteksi tanda-tanda adanya serangan atau kegiatan yang illegal
3. **Pengertian AI**
   Menurut [3]Kecerdasan buatan (AI) adalah "payung istilah" yang digunakan untuk menyebut simulasi yang dilakukan oleh mesin-mesin atau alat, yang terhubung dengan samudera data, yang menyerupai kecerdasan manusia

METODE

1. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian ekperimen terapan. Pendekan kuantitatif dipilih karena ini melibatkan pengolahan data numerik serta pengukuran kinerja sistem menggunakan parameter statistik seperti akurasi, precision, recall, dan F1-score. Penelitian ekperimen terapan di gunakan karena penelitian ini tidak hanya membahas konsep teori, tetapi juga melakukan penerapan langsung metode Artifical Intelligence pada sistem *Instrusion Detection System* (IDS) untuk mendeteksi jaringan. Metode pengumpulan data merupakan tahapan penting dalam penelitian ini karena berkaitan langsung dengan sumber data yang akan digunakan untuk proses pelatihan dan pengujian sistem IDS berbasis *Artificial Intelligence*. Metode pengumpulan data yang digunakan adalah sebagai berikut:

a. Metode Pengumpulan Data

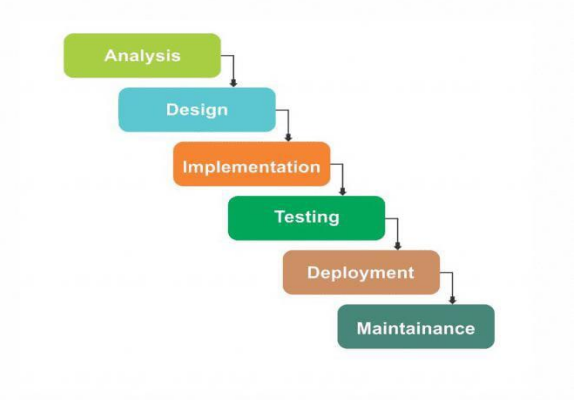
Data diperoleh penelit melalui berbagai prosedur data seperti :

1) Studi Literatur, Studi literatur dilakukan dengan cara mempelajari berbagai sumber pustaka seperti buku, jurnal ilmiah, artikel penelitian, serta publikasi online yang berkaitan dengan: Keamanan jaringan komputer, Intrusion Detection System (IDS) Artificial Intelligence, Machine Learning dalam bidang keamanan jaringan Studi literatur bertujuan untuk memperoleh landasan teori yang kuat serta mengetahui perkembangan metode IDS berbasis AI yang telah dilakukan sebelumnya.

2) Observasi, Observasi dilakukan dengan mengamati secara langsung sistem jaringan komputer yang digunakan, khususnya terkait: Proses lalu lintas data jaringan,Potensi terjadinya serangan jaringan, Proses pemantauan keamanan jaringan yang berjalan saat ini Observasi ini bertujuan untuk mengetahui permasalahan nyata yang terjadi pada sistem keamanan jaringan sebelum diterapkannya *Instrusion Detection System* (IDS) berbasis *Artificial Intelligence* (AI).
3) Penggunaan Dataset, Dataset yang di gunakan dalam penilitian ini di peroleh dari dataset publik yang umum di gunakan dalam penelitian Instrusion Detection System (IDS) seperti NSL-KDD Dataset dan CICIDS2017 Dataset, data tersebut di gunakan sebagai training data dan testing data untuk membangun dan mengguji model Artificial Intelligence dalam mendeteksi serangan jaringan

2. Metode Perancangan Sistem

Menurut [4] Waterfall merupakan sebuah metodologi pengembangan sistem informasi yang termasuk kedalam bagian dari SDLC. Metode ini mengharuskan pengerjaan nya dilaksanakan secara berurutan atau sekuensial, yang dimulai dari tahapan perencanaan konsep (*requirement analysis*), pemodelan sistem (*desain sistem*), implementasi, pengujian dan pemeliharaan (*maintenance*)



Gambar 1. Metode Perancangan Sistem

3. Analisa dan Perancangan

a. Analisa Sistem

Analisis sistem dilakukan untuk mengetahui kondisi sistem keamanan jaringan sebelum diterapkannya *Intrusion Detection System* (IDS) berbasis *Artificial Intelligence*. Pada kondisi awal, sistem keamanan jaringan masih mengandalkan perangkat pengamanan dasar seperti firewall serta pemantauan manual oleh administrator jaringan. Sistem yang berjalan belum memiliki kemampuan untuk mendeteksi serangan secara otomatis dan real-time, sehingga potensi terjadinya serangan yang tidak terdeteksi masih cukup tinggi. Selain itu, proses identifikasi aktivitas mencurigakan masih memerlukan pengecekan log jaringan secara manual, yang membutuhkan waktu dan ketelitian tinggi.

Kepadatan lalu lintas data jaringan juga menjadi kendala dalam proses pengawasan keamanan. Banyaknya data yang masuk dan keluar dalam waktu singkat menyebabkan administrator jaringan sulit melakukan pemantauan secara menyeluruh. Akibatnya, sistem keamanan menjadi kurang efektif dalam menghadapi berbagai bentuk serangan siber yang

semakin kompleks dan berkembang. Berdasarkan kondisi tersebut, diperlukan sebuah sistem yang mampu melakukan pendeteksian serangan secara otomatis, cepat, dan akurat agar keamanan jaringan dapat ditingkatkan secara optimal. karena itu, pada penelitian ini diusulkan penerapan *Intrusion Detection System* (IDS) berbasis *Artificial Intelligence* yang mampu menganalisis pola lalu lintas jaringan, mengklasifikasikan aktivitas sebagai normal atau serangan, serta memberikan informasi secara langsung kepada administrator jaringan melalui tampilan sistem monitoring. Sistem ini diharapkan dapat membantu meningkatkan efektivitas pengamanan jaringan serta meminimalkan risiko terjadinya serangan yang tidak terdeteksi.

b. **Perancaan Sistem**

Perancangan sistem dilakukan setelah tahap analisis sistem selesai, dengan tujuan untuk menghasilkan gambaran struktur sistem yang akan dikembangkan. Perancangan ini meliputi perancangan alur kerja sistem, hubungan antar komponen, serta perancangan antarmuka pengguna. Sistem IDS berbasis *Artificial Intelligence* dirancang untuk menerima data lalu lintas jaringan sebagai input, kemudian data tersebut diproses melalui tahapan *preprocessing* sebelum dilakukan proses klasifikasi menggunakan model *machine learning*.Model *Artificial Intelligence* yang telah dilatih menggunakan dataset IDS akan digunakan untuk melakukan proses deteksi serangan secara otomatis.

Hasil dari proses klasifikasi kemudian disimpan ke dalam basis data dan ditampilkan kepada administrator jaringan melalui dashboard sistem dalam bentuk tabel, grafik, serta laporan hasil deteksi. Tampilan antarmuka dirancang agar mudah dipahami dan digunakan, sehingga administrator jaringan dapat dengan cepat mengetahui kondisi keamanan jaringan. Perancangan sistem ini juga memperhatikan aspek keandalan, keamanan data, serta kemudahan dalam proses pengembangan lebih lanjut. Dengan adanya perancangan sistem yang terstruktur, diharapkan sistem IDS berbasis *Artificial Intelligence* yang dikembangkan dapat berjalan secara optimal, stabil.

HASIL DAN PEMBAHASAN

1. Implementasi dan Pengujian

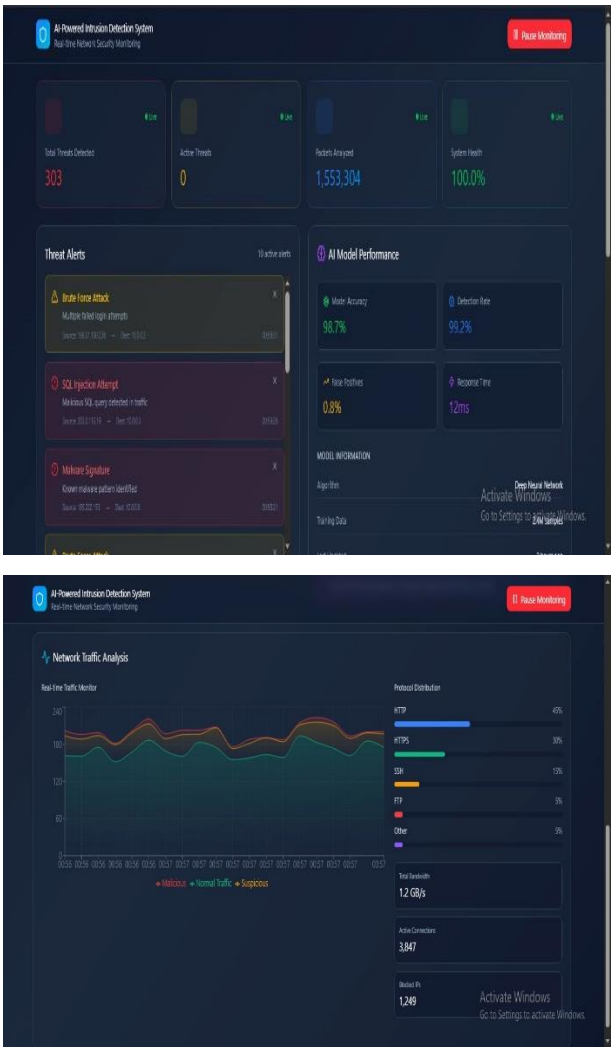
Implementasi sistem merupakan tahap penerapan hasil perancangan ke dalam bentuk sistem yang dapat dijalankan. Pada penelitian ini, implementasi dilakukan dengan membangun sistem *Intrusion Detection System* (IDS) berbasis *Artificial Intelligence* yang mampu mendeteksi aktivitas jaringan secara otomatis. Sistem dirancang untuk menerima data trafik jaringan yang berasal dari dataset IDS, kemudian memproses data tersebut menggunakan model *machine learning* yang telah dilatih sebelumnya.

Proses implementasi diawali dengan menyiapkan lingkungan pengembangan sistem, termasuk perangkat lunak yang digunakan untuk pengolahan data dan pelatihan model *Artificial Intelligence*. Dataset IDS yang digunakan terlebih dahulu melalui tahap *preprocessing*, seperti pembersihan data, normalisasi, dan seleksi fitur, agar data dapat diproses dengan baik oleh model AI. Setelah itu, data dibagi menjadi data latih dan data uji untuk keperluan pelatihan dan evaluasi sistem. Model *Artificial Intelligence* yang telah dilatih kemudian diintegrasikan ke dalam sistem IDS. Sistem ini berfungsi untuk menganalisis data trafik jaringan dan mengklasifikasikan aktivitas jaringan menjadi dua kategori, yaitu aktivitas normal dan aktivitas serangan. Hasil klasifikasi tersebut disimpan ke dalam basis data dan

ditampilkan kepada administrator jaringan melalui antarmuka sistem dalam bentuk tabel, grafik, serta laporan hasil deteksi.

2. Implementasi Aplikasi

Halaman Dashboard dan Main Monitoring system



Gambar 2. Halaman Dashboard

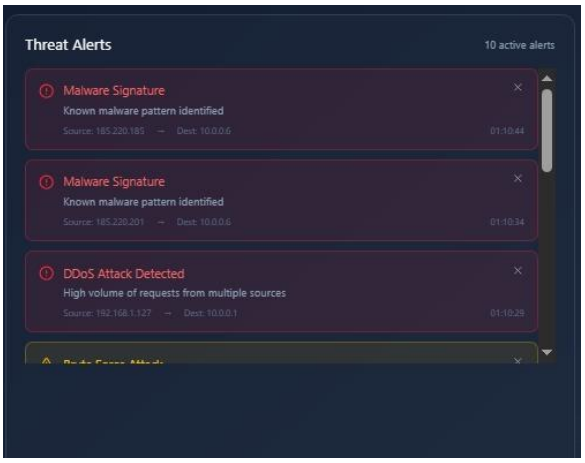
Gambar 3. Main Monitoring system

Pada Dashboard ini berfungsi sebagai dashboard pemantauan utama pada sistem Intrusion Detection System (IDS) berbasis Artificial Intelligence. Tujuan utamanya adalah memberikan gambaran kondisi keamanan jaringan secara cepat, ringkas, dan real-time kepada administrator jaringan., Monitoring Keamanan Jaringan Secara Real-Time Dashboard ini digunakan untuk memantau aktivitas jaringan yang sedang berlangsung dan mendeteksi adanya ancaman atau serangan secara langsung tanpa menunggu analisis manual.

Dashboard ini menyajikan ingkasan tingkat keamanan jaringan, sehingga administrator dapat langsung mengetahui apakah jaringan dalam kondisi aman, waspada, atau

berbahaya. Sistem ini membantu melihat apakah terdapat ancaman yang sedang aktif dan seberapa sering ancaman terjadi.

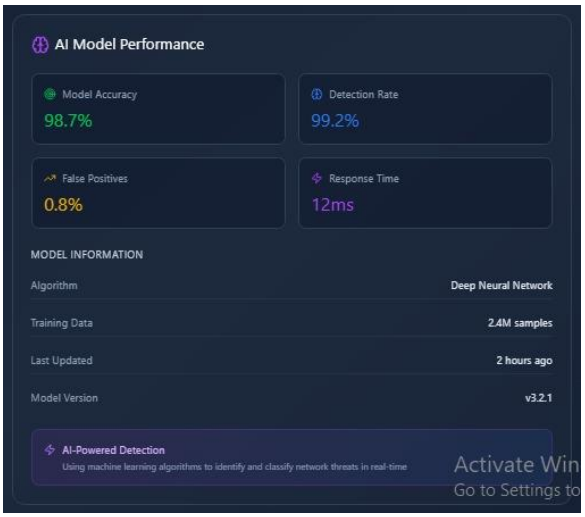
Threat Alerts



Gambar 4. Threat Alerts

Panel ini digunakan untuk menampilkan daftar ancaman jaringan yang terdeteksi secara real-time dan menjadi pusat perhatian utama saat terjadi insiden keamanan. Panel ini berfungsi untuk memberikan peringatan ketika sistem IDS mendeteksi aktivitas jaringan yang mencurigakan atau berbahaya, sehingga administrator dapat segera menyadari adanya potensi serangan. Karena Sistem IDS berbasis AI yang penulis buat mengelompokkan ancaman berdasarkan pola serangan tertentu (misalnya injeksi, pemindaian port, atau pola anomali), yang membantu administrator memahami jenis risiko yang dihadapi

AI Model Performance



Gambar 5. AI Model Performance

Dashboard ini berfungsi sebagai halaman evaluasi dan pemantauan kinerja model AI yang digunakan dalam sistem Intrusion Detection System (IDS). Tujuannya adalah untuk menilai seberapa efektif dan andal model AI dalam mendeteksi ancaman jaringan.Evaluasi Akurasi Deteksi Ancaman. Tampilan ini digunakan untuk memastikan bahwa model AI mampu mengenali serangan jaringan dengan tingkat ketepatan yang tinggi, sehingga meminimalkan kesalahan deteksi. Pemantauan Kualitas Hasil Deteksi AI Dashboard ini

membantu menilai keseimbangan antara deteksi ancaman yang benar dan kesalahan deteksi, sehingga sistem IDS tidak terlalu sensitif maupun terlalu longgar.

Network Traffic Analysis

Gambar 6. Network Traffic Analysis

Gambar ini berfungsi sebagai halaman analisis lalu lintas jaringan secara real-time dalam sistem Intrusion Detection System (IDS) berbasis AI. Tampilan ini digunakan untuk memahami pola, volume, dan karakteristik trafik jaringan, serta mendukung proses deteksi anomali dan serangan. Fungsi-Fungsi yang Diwakili oleh Gambar IniPemantauan Lalu Lintas Jaringan Secara Real-Time Tampilan ini digunakan untuk melihat pergerakan trafik jaringan yang sedang berlangsung, sehingga administrator dapat mengetahui kondisi jaringan secara langsung. Dashboard ini membantu membedakan antara trafik normal, trafik mencurigakan, dan trafik berbahaya, yang menjadi dasar utama deteksi anomali berbasis AI.

KESIMPULAN

Penelitian ini berhasil mengembangkan sistem keamanan jaringan menggunakan *Intrusion Detection System* (IDS) berbasis *Artificial Intelligence*. Sistem yang dikembangkan mampu mendeteksi aktivitas jaringan dan mengklasifikasikannya menjadi aktivitas normal dan serangan secara otomatis. Hasil pengujian menunjukkan bahwa sistem IDS berbasis *Artificial Intelligence* memiliki kinerja yang baik dalam mendeteksi serangan jaringan. Hal ini dibuktikan melalui nilai akurasi dan metrik evaluasi lainnya yang menunjukkan hasil yang memuaskan. Dengan demikian, sistem ini dapat membantu meningkatkan keamanan jaringan dan mempermudah administrator jaringan dalam melakukan monitoring keamanan.

DAFTAR PUSTAKA

[1] Oki Firnando1,Samso Supriyatna2, "Analisis Dan Perancangan Sistem Informasi Penggajian Karyawan Berbasis Webdengan Metode Agilestudi Kasus:Pt.Media Reformasi Indonesia," *urnal E-Bisnis, Sistem Informasi , Teknologi Informasi ESI*, 2025.

[2] T. Purnama, "Implementasi Instrusion Detection System (Ids) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telengram Sebagai Media Notifikasi," *Jurnal Ilmiah Teknologi Informasi Dan Komunikasi(JTIK)*, 2023.

[3] M. R. Pabubung, "Epistemologi Kecerdasan Buatan (AI) dan Pentingnya Ilmu Etika dalam Pendidikan Interdisipliner," *Jurnal Filsafat Indonesia*, 2021.

[4] Jadid Alif Ramadhan, Diandara Tresya Haniva, Aries Suharso, "Systematic Literature Review Penggunaan Metodologi Pengembangan Sistem Informasi Waterfall, Agile, danHybrid," *ournal Information Engineering and Educational Technology*, 2023.

[5] Aditya Pratama Putraa, Muhammad Darwisb, "Perancangan Jaringan Sistem Smart Home berbasis IoT menggunakan Cisco Packet Tracer dengan Metode Waterfall," *Jurnal Teknologi Dan Sistem Informasi Bisnis* , 2025.