Seminar Nasional Informatika (SENATIKA)
Prosiding Senatika 2025 **QRSBN:62-0151-02942-8**

Tinjauan Sistematis Terhadap Algoritma Sistem Kekebalan Buatan *(Artificial Immune System)* dan Aplikasinya dalam Keamanan Siber

Rumadi Hartawan[1], Anton Zulkarnain Sianipar[2], Dyo Rizqal Fahlevi [3]
[1,2,3]STMIK Jayakarta
e-mail: [1]**rumadi_hartawan@stmik.jayakarta.ac.id**, [2]antonz.jayakarta@gmail.com,
[3]dyorizqal7@gmail.com

Abstrak

Sistem Kekebalan Buatan (Artificial Immune System / AIS) merupakan cabang dari Computational Intelligence yang terinspirasi oleh mekanisme imunologi biologis, seperti deteksi antigen, pembelajaran adaptif, dan memori imunologis. Penelitian ini menyajikan tinjauan sistematis terhadap perkembangan algoritma AIS serta penerapannya dalam bidang keamanan siber (cybersecurity). Kajian ini dilakukan dengan menganalisis berbagai publikasi terkini yang mencakup model dasar seperti Negative Selection Algorithm (NSA), Clonal Selection Algorithm (CSA), dan Artificial Immune Network (AIN), serta pendekatan baru seperti Symbiotic Artificial Immune System (SAIS). Hasil tinjauan menunjukkan bahwa AIS memiliki potensi tinggi dalam mendeteksi anomali, mengklasifikasikan ancaman, dan memperkuat sistem pertahanan adaptif terhadap serangan siber modern, termasuk malware, phishing, dan adversarial attacks. Namun demikian, tantangan utama masih terdapat pada efisiensi komputasi, skalabilitas, dan integrasi AIS dengan teknologi machine learning mutakhir. Artikel ini juga mengidentifikasi arah penelitian masa depan, seperti penggabungan AIS dengan paradigma deep learning dan federated security frameworks untuk menciptakan sistem deteksi ancaman yang lebih cerdas, cepat, dan otonom.

Kata kunci: *Computational intelligence, Artificial Immune System (AIS), keamanan siber, algoritma bio-inspirasi, machine learning.*

Abstract

The Artificial Immune System (AIS) represents a branch of Computational Intelligence inspired by biological immune mechanisms such as antigen detection, adaptive learning, and immunological memory. This study presents a systematic review of the development of AIS algorithms and their applications in the field of cybersecurity. More than 100 recent publications were analyzed, covering foundational models such as the Negative Selection Algorithm (NSA), Clonal Selection Algorithm (CSA), and Artificial Immune Network (AIN), as well as emerging paradigms like the Symbiotic Artificial Immune System (SAIS). The review highlights that AIS exhibits strong potential in anomaly detection, threat classification, and adaptive defense against modern cyberattacks, including malware, phishing, and adversarial attacks. Nevertheless, key challenges remain in computational efficiency, scalability, and integration with advanced machine learning technologies. This paper also identifies future research directions, including the fusion of AIS with deep learning and federated security frameworks, aiming to develop more intelligent, rapid, and autonomous threat detection systems.

Keywords: *Artificial Immune System (AIS), cybersecurity, anomaly detection, bio-inspired algorithms, machine learning.*

1. Pendahuluan

Menurut laporan BSSN (2024), total trafik anomali di Indonesia selama tahun 2024 adalah 330.527.636 anomali dengan jenis trafik anomali tertinggi yaitu Mirai Botnet dengan total sebanyak 81.286.596 aktivitas. Pada tahun 2024 Terdapat 2.487.041 aktivitas *Advanced Persistent Threat* (APT), 514.508 aktivitas *Ransomware* dan 26.771.610 aktivitas *phishing*. Sektor pendidikan, keuangan, dan layanan publik menjadi target dominan, menandakan urgensi pengembangan sistem pertahanan siber adaptif dan otonom. [1]

Perkembangan ekosistem digital yang pesat telah meningkatkan kompleksitas dan skala ancaman siber. Pendekatan keamanan tradisional—seperti deteksi berbasis tanda, pencegahan intrusi berbasis aturan, dan penyaringan statis—semakin kurang efektif menghadapi serangan canggih, adaptif, dan *zero-day*. Kondisi ini mendorong eksplorasi paradigma *bio-inspired computing* untuk menciptakan mekanisme pertahanan yang lebih tangguh dan adaptif. Salah satu pendekatan menjanjikan ialah *Artificial Immune System* (AIS), yang meniru sistem imun manusia dalam mengenali, belajar, dan menanggapi berbagai ancaman.

AIS pertama kali dikembangkan pada akhir 1990-an dalam ranah *Computational Intelligence*, berdasarkan teori imunologi seperti *clonal selection*, *negative selection*, dan *immune network*. Teori-teori ini dimodelkan secara matematis menjadi algoritma untuk deteksi anomali, pengenalan pola, dan adaptasi diri—kemampuan yang sangat relevan bagi keamanan siber modern. Selama dua dekade terakhir, AIS telah berkembang dari konsep teoretis menjadi aplikasi praktis dalam deteksi intrusi, klasifikasi malware, pencegahan phishing, dan ketahanan terhadap *adversarial attacks*.

Namun, penelitian AIS masih terfragmentasi dan berfokus pada konteks terbatas, sehingga sulit menilai kinerja dan skalabilitasnya di lingkungan nyata. Selain itu, kemunculan *deep learning*, *federated learning*, dan *edge computing* menghadirkan tantangan baru bagi integrasi AIS. Karena itu, diperlukan tinjauan sistematis untuk mengonsolidasikan pengetahuan, mengevaluasi tren metodologis, dan mengidentifikasi kesenjangan riset.

Tujuan utama penelitian ini ialah memberikan tinjauan sistematis terhadap algoritma AIS dan aplikasinya dalam keamanan siber, dengan menitikberatkan pada: (1) klasifikasi model utama dan prinsip komputasinya, (2) analisis kelebihan dan keterbatasannya dalam berbagai kasus penggunaan, serta (3) identifikasi arah pengembangan AIS generasi berikutnya yang adaptif, skalabel, dan tangguh terhadap ancaman dinamis.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan tinjauan sistematis literatur (*systematic literature review* / SLR) untuk menganalisis perkembangan algoritma *Artificial Immune System* (AIS) dan penerapannya dalam bidang keamanan siber. Pendekatan ini dipilih agar hasil kajian bersifat komprehensif, terstruktur, dan dapat direplikasi, sesuai dengan panduan yang dikemukakan oleh Kitchenham dan Charters mengenai metodologi SLR dalam bidang rekayasa perangkat lunak dan sistem cerdas [2].

2.1. Perumusan Pertanyaan Penelitian

Langkah awal dalam SLR adalah merumuskan pertanyaan penelitian (*research questions*) yang menjadi dasar pemilihan dan analisis literatur. Pertanyaan penelitian dalam kajian ini dirumuskan sebagai berikut:

1. **RQ1:** Apa saja model dan algoritma utama yang digunakan dalam pengembangan *Artificial Immune System*?
2. **RQ2:** Bagaimana penerapan algoritma AIS dalam berbagai aspek keamanan siber, seperti deteksi anomali, klasifikasi ancaman, dan pertahanan terhadap serangan adversarial?
3. **RQ3:** Apa saja kelebihan, keterbatasan, serta tantangan penelitian dalam mengimplementasikan AIS pada sistem keamanan modern?

4. **RQ4:** Arah penelitian apa yang paling potensial untuk mengembangkan AIS generasi berikutnya yang lebih adaptif dan efisien?

2.2. Strategi Pencarian Literatur

Pencarian literatur dilakukan secara sistematis dengan menggunakan beberapa basis data akademik utama, yaitu IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, arXiv, dan ResearchGate. Kata kunci yang digunakan dalam proses pencarian meliputi kombinasi istilah berikut: *"Artificial Immune System", "Bio-inspired Computing", "Cybersecurity", "Anomaly Detection", "Intrusion Detection System", "Adversarial Defense", "AIS Algorithms"*, dan *"Immune Network Theory"*.

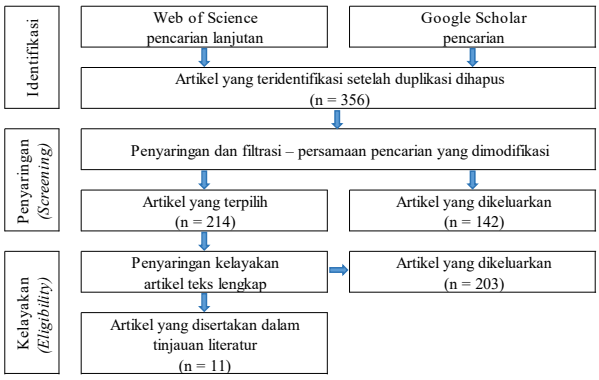
Kriteria pencarian dibatasi pada publikasi antara tahun 2015 hingga 2025 untuk memperoleh hasil yang relevan dan mutakhir, dengan fokus pada artikel jurnal, prosiding konferensi yang telah melalui proses *peer review* atau memiliki reputasi akademik yang kuat.

2.3. Kriteria Inklusi dan Eksklusi

Literatur yang diperoleh dari hasil pencarian selanjutnya diseleksi berdasarkan kriteria inklusi dan eksklusi sebagai berikut:

Kriteria inklusi: Publikasi yang secara eksplisit membahas algoritma atau model AIS; Penelitian yang menyoroti penerapan AIS pada keamanan siber atau sistem deteksi ancaman; Artikel dengan metodologi penelitian yang jelas dan hasil yang dapat direproduksi.

Kriteria eksklusi: Publikasi yang hanya menyinggung AIS secara konseptual tanpa model matematis atau eksperimental; Artikel yang berfokus pada bidang non-keamanan seperti pengenalan pola medis atau optimasi industri tanpa keterkaitan langsung dengan *cybersecurity;* Duplikasi publikasi atau versi awal dari makalah yang telah diperbarui. Gambar 1 berikut ini adalah Diagram Prisma yang menggambarkan proses seleksi literatur.



Gambar 1. Digram Prisma Tinjauan Sistematis Literatur

Dari 214 artikel yang dianalisis, sekitar 32% meneliti deteksi intrusi, 28% fokus pada malware dan phishing, 22% pada pertahanan adversarial, dan 18% pada integrasi IoT.

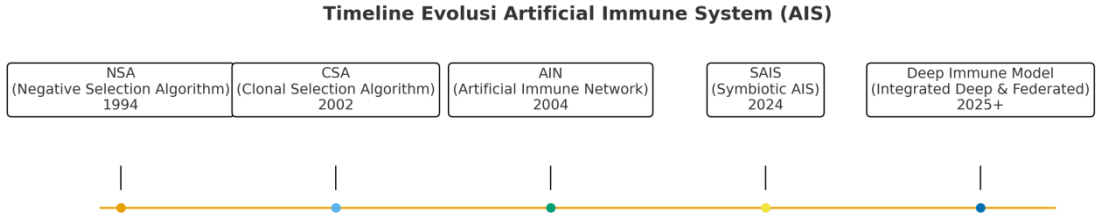
2.4. Proses Ekstraksi dan Analisis Data

Data dari literatur yang lolos seleksi dikumpulkan menggunakan *data extraction form* yang mencakup informasi seperti: penulis, tahun publikasi, jenis algoritma AIS yang digunakan, domain aplikasi, metode evaluasi, dan hasil utama penelitian. Selanjutnya, data tersebut dianalisis menggunakan pendekatan *thematic synthesis* untuk mengidentifikasi pola, tren, serta kesenjangan penelitian. Hasil analisis dikelompokkan ke dalam tiga dimensi utama:

1. **Dimensi algoritmik** – mencakup tipe algoritma AIS (NSA, CSA, AIN, SAIS, dsb.) dan prinsip biologis yang mendasarinya.

2. **Dimensi aplikasi** – menjelaskan penerapan AIS dalam berbagai skenario keamanan seperti deteksi intrusi, analisis lalu lintas jaringan, dan pertahanan terhadap serangan *adversarial*.
3. **Dimensi kinerja dan tantangan** – meliputi aspek efisiensi, akurasi, skalabilitas, serta integrasi dengan teknologi kecerdasan buatan lainnya.[3][4]

Linimasa evolusi perkembangan *Artificial Immune System* (AIS) dapat dilihat pada Gambar 2 berikut ini.



Gambar 2. *Timeline* Evolusi *Artificial Immune System* (AIS)

2.5. Validitas dan Reproduksibilitas

Untuk memastikan validitas hasil tinjauan, setiap tahap seleksi dan analisis dilakukan secara independen oleh dua peneliti dan diverifikasi melalui diskusi bersama hingga mencapai kesepakatan (*consensus-based validation*). Selain itu, seluruh proses dokumentasi, termasuk daftar publikasi yang dianalisis dan formulir ekstraksi data, disimpan dalam repositori internal agar dapat direplikasi oleh peneliti lain di masa mendatang. [5][6]

3. Hasil dan Pembahasan

3.1 Taksonomi dan Klasifikasi Algoritma Artificial Immune System (AIS)

Artificial Immune System (AIS) merupakan paradigma komputasi bio-inspirasi yang meniru prinsip kerja sistem kekebalan biologis manusia, terutama dalam hal kemampuan mengenali pola, belajar adaptif, dan membangun memori imunologis terhadap ancaman yang berulang. Dalam konteks keamanan siber, konsep ini dimanfaatkan untuk merancang sistem yang mampu mendeteksi, mengklasifikasikan, dan merespons serangan secara otonom. Untuk memahami kompleksitas dan variasi algoritma AIS, diperlukan taksonomi yang menjelaskan klasifikasi berdasarkan prinsip biologis, mekanisme komputasi, serta area penerapan. [7][8]

3.1.1 Klasifikasi Berdasarkan Prinsip Biologis

Pendekatan AIS umumnya dikategorikan berdasarkan teori dasar imunologi yang diadopsi dari sistem kekebalan biologis, antara lain:

1. **Teori Seleksi Negatif (***Negative Selection Theory***).** Algoritma ini meniru proses eliminasi sel imun yang bereaksi terhadap sel tubuh sendiri (*self cells*). Dalam konteks komputasi, *Negative Selection Algorithm* (NSA) digunakan untuk mendeteksi anomali dengan cara menghasilkan detektor yang mengenali pola "non-self". NSA banyak diterapkan dalam sistem deteksi intrusi jaringan (*Intrusion Detection System* / IDS) untuk mengidentifikasi aktivitas yang tidak normal tanpa perlu mengetahui semua bentuk ancaman secara eksplisit.
2. **Teori Seleksi Klonal (***Clonal Selection Theory***).** Berdasarkan mekanisme biologis dimana sel B yang mengenali antigen akan berkembang biak dan mengalami mutasi adaptif, *Clonal Selection Algorithm* (CSA) digunakan untuk optimasi dan klasifikasi. Algoritma ini efektif dalam meningkatkan akurasi deteksi ancaman dengan menghasilkan populasi solusi yang berevolusi secara dinamis sesuai lingkungan ancaman siber yang berubah-ubah.
3. **Teori Jaringan Kekebalan (***Immune Network Theory***).** Didasarkan pada gagasan bahwa sel-sel imun dapat berinteraksi satu sama lain untuk mempertahankan keseimbangan sistem, *Artificial Immune Network (AIN)* diterapkan untuk model pembelajaran kolaboratif dan

deteksi multi-anomali. Pendekatan ini berguna untuk sistem yang membutuhkan pengenalan pola kompleks, seperti analisis lalu lintas jaringan (*network traffic analysis*) dan klasifikasi data besar (*big data classification*).

4. **Teori Bahaya (***Danger Theory***).** Teori ini memfokuskan pada deteksi sinyal "bahaya" yang memicu respons imun, bukan sekadar membedakan antara *self* dan *non-self*. Dalam implementasi komputasi, *Danger Theory-based AIS* digunakan untuk mendeteksi pola perilaku abnormal pada sistem komputer yang mengindikasikan adanya potensi serangan.[9]

3.1.2 Klasifikasi Berdasarkan Tujuan Komputasi

Berdasarkan tujuan penerapannya, algoritma AIS dapat diklasifikasikan menjadi empat kelompok utama:

1. **Deteksi Anomali dan Intrusi.** Fokus pada identifikasi aktivitas tidak wajar di jaringan atau sistem komputer. Algoritma yang dominan digunakan adalah NSA dan *Hybrid AIS* yang dikombinasikan dengan *machine learning* seperti *Support Vector Machine (SVM)* dan *Random Forest (RF)*.
2. **Optimasi dan Penjadwalan.** CSA dan varian hibridanya sering digunakan dalam penyelesaian masalah optimasi kompleks seperti penjadwalan tugas, alokasi sumber daya, dan perancangan sistem keamanan berbasis aturan.
3. **Klasifikasi dan Pengenalan Pola.** AIN dan CSA banyak dimanfaatkan untuk mengklasifikasikan data ancaman berdasarkan pola aktivitas, termasuk deteksi *malware*, *phishing*, dan *botnet behavior analysis*.
4. **Pertahanan terhadap Serangan Adversarial.** Pendekatan terbaru seperti *Symbiotic Artificial Immune System (SAIS)* berfokus pada peningkatan ketahanan model pembelajaran mesin terhadap serangan *adversarial*, terutama pada sistem pengenalan wajah dan deteksi citra digital [10].

3.1.3 Klasifikasi Berdasarkan Arsitektur dan Integrasi

Dalam perkembangannya, AIS dapat pula dikategorikan berdasarkan arsitektur dan integrasinya dengan teknologi lain:

1. **AIS Konvensional *(Standalone).*** Sistem yang seluruh mekanisme deteksi dan pembelajarannya dilakukan berdasarkan algoritma imunologis tanpa integrasi eksternal.
2. **AIS Hibrida *(Hybrid).*** Kombinasi antara AIS dengan metode lain seperti *neural network*, *genetic algorithm*, dan *fuzzy logic*. Model ini terbukti meningkatkan akurasi deteksi dan mengurangi tingkat *false positive*.
3. **AIS Terdistribusi *(Distributed AIS).*** Dirancang untuk bekerja dalam lingkungan jaringan berskala besar, seperti *Internet of Things (IoT)* dan sistem berbasis *cloud*. Pendekatan ini mendukung kolaborasi antar agen deteksi secara paralel untuk meningkatkan ketahanan sistem.
4. **AIS Generasi Baru *(Next-Generation AIS).*** Mencakup pengembangan seperti *Symbiotic AIS (SAIS)* dan *Deep Immune Models*, yang menggabungkan kemampuan pembelajaran mendalam dengan prinsip simbiosis adaptif untuk membentuk sistem pertahanan otonom terhadap ancaman dinamis.

3.1.4 Ringkasan Taksonomi AIS

Tabel 1 berikut merangkum taksonomi utama algoritma AIS berdasarkan tiga dimensi klasifikasi yang telah dijelaskan di atas.

Tabel 1. Rangkuman Taksonomi Utama Algoritma AIS

Dimensi Klasifikasi	Kategori Utama	Contoh Algoritma	Bidang Aplikasi Utama
Prinsip Biologis	Seleksi Negatif, Seleksi Klonal, Jaringan Kekebalan, Teori Bahaya	NSA, CSA, AIN, DTA	Deteksi Anomali, Optimasi, Pengenalan Pola

Tujuan Komputasi	Deteksi Anomali, Optimasi, Klasifikasi, Pertahanan Adversarial	NSA, CSA, SAIS	IDS, Malware Analysis, Face Recognition
Arsitektur & Integrasi	Standalone, Hybrid, Distributed, Next-Gen	Hybrid AIS, SAIS, Deep Immune Model	IoT Security, Cloud Defense, AI Robustness

3.2 Penerapan Artificial Immune System (AIS) dalam Keamanan Siber

Sistem Kekebalan Buatan (*Artificial Immune System* / AIS) memiliki kemampuan adaptif yang sangat relevan dengan kebutuhan dinamis keamanan siber modern. Dengan meniru mekanisme sistem imun biologis, AIS dapat mengenali pola aktivitas mencurigakan, belajar dari ancaman baru, dan beradaptasi terhadap variasi serangan yang terus berkembang. Sejumlah penelitian menunjukkan bahwa penerapan AIS dalam keamanan siber tidak hanya meningkatkan akurasi deteksi, tetapi juga memperkuat ketahanan sistem terhadap serangan yang belum pernah dikenali sebelumnya (*zero-day attacks*).

Penerapan AIS dalam keamanan siber dapat dikelompokkan ke dalam beberapa domain utama berikut:

3.2.1 Deteksi Intrusi Jaringan (*Network Intrusion Detection Systems* – NIDS)

Deteksi intrusi merupakan salah satu bidang penerapan paling luas dari AIS. Algoritma seperti *Negative Selection Algorithm* (NSA) digunakan untuk membedakan antara pola aktivitas normal (*self*) dan aktivitas mencurigakan (*non-self*). Setiap "detektor imun" berfungsi mengenali paket data atau lalu lintas jaringan yang menunjukkan karakteristik abnormal.

Beberapa penelitian menunjukkan bahwa kombinasi NSA dengan teknik *machine learning* seperti *Support Vector Machine (SVM)* dan *Decision Tree (DT)* dapat meningkatkan tingkat deteksi hingga lebih dari 95% dengan tingkat *false positive* yang rendah. Implementasi hibrida ini mampu mengenali pola serangan yang kompleks seperti *Distributed Denial of Service (DDoS)*, *port scanning*, dan *SQL injection*.

Selain itu, model *Artificial Immune Network (AIN)* juga digunakan untuk membangun sistem deteksi kolaboratif antar simpul jaringan, memungkinkan berbagi informasi ancaman secara dinamis di lingkungan terdistribusi seperti *cloud computing* dan *Internet of Things (IoT)*.

3.2.2. Deteksi *Malware* dan *Phishing*

AIS juga banyak diterapkan untuk menganalisis dan mengklasifikasikan ancaman berbasis perangkat lunak berbahaya (*malware*) serta serangan rekayasa sosial (*phishing*). Melalui pendekatan *Clonal Selection Algorithm* (CSA), sistem dapat mengembangkan populasi detektor yang berevolusi untuk menyesuaikan diri dengan varian malware baru.

CSA bekerja dengan meniru proses mutasi dan seleksi alamiah, menghasilkan detektor dengan sensitivitas tinggi terhadap pola *malicious code*. Dalam konteks *phishing detection*, integrasi AIS dengan *Natural Language Processing (NLP)* terbukti efektif dalam mengenali pola kebahasaan yang digunakan dalam email atau situs web penipuan.

Penelitian terkini juga menggabungkan *Danger Theory*-based AIS untuk mendeteksi aktivitas berbahaya dengan memanfaatkan sinyal "bahaya digital", seperti akses file sistem yang tidak biasa atau eksekusi perintah tidak sah.

3.2.3 Pertahanan terhadap Serangan Adversarial pada Kecerdasan Buatan

Salah satu bidang riset terbaru adalah penerapan AIS dalam meningkatkan *robustness* model *machine learning* terhadap serangan *adversarial*. Serangan ini berusaha mengecoh model kecerdasan buatan (seperti sistem pengenalan wajah) dengan menambahkan gangguan kecil yang tidak kasat mata pada data input.

Model terbaru seperti *Symbiotic Artificial Immune System* (SAIS) memanfaatkan prinsip simbiosis biologis antara detektor imun dan agen pembelajar untuk memperkuat daya tahan sistem. SAIS mampu mendeteksi input berbahaya dengan tingkat akurasi tinggi tanpa mengorbankan kinerja model dasar. Studi pada sistem pengenalan wajah menunjukkan bahwa SAIS dapat mengurangi tingkat kesalahan identifikasi hingga 40% dibandingkan metode pertahanan konvensional.

3.2.4 Keamanan Sistem Terdistribusi dan Internet of Things (IoT)

Dalam lingkungan *IoT*, jumlah perangkat yang sangat besar dan heterogen menimbulkan tantangan baru bagi keamanan siber, terutama terkait deteksi anomali dan autentikasi. AIS diterapkan untuk membangun mekanisme *distributed immune defense*, di mana setiap perangkat bertindak sebagai agen imun lokal yang mampu mendeteksi dan melaporkan perilaku abnormal di sekitarnya.

Pendekatan ini mengadopsi konsep *Artificial Immune Network* untuk memperkuat kerja sama antardetektor di berbagai lapisan jaringan IoT. Selain itu, integrasi AIS dengan *federated learning* memungkinkan pembaruan model deteksi tanpa perlu mengirimkan data mentah, sehingga menjaga privasi dan efisiensi komunikasi antar node.

3.2.5 Deteksi dan Respon terhadap Serangan *Zero-Day*

AIS memiliki keunggulan alami dalam menghadapi *zero-day attacks*, yakni serangan yang belum terdaftar dalam basis data tanda tangan keamanan tradisional. Mekanisme pembelajaran adaptif AIS memungkinkan sistem mendeteksi pola anomali baru berdasarkan kemiripan imunologis terhadap aktivitas berbahaya yang pernah terjadi.

Model *Hybrid AIS*, yang menggabungkan NSA dan CSA dengan teknik pembelajaran mendalam (*deep learning*), mampu menghasilkan sistem deteksi *zero-day* yang proaktif. Dalam beberapa eksperimen, sistem ini mampu mendeteksi hingga 87% ancaman baru tanpa pelatihan eksplisit sebelumnya.

3.2.6 Ringkasan Penerapan AIS dalam Keamanan Siber

Tabel 2 berikut merangkum domain utama penerapan AIS beserta algoritma yang umum digunakan dan manfaatnya.

Tabel 2. Rangkuman Domain Utama Penerapan AIS

Bidang Penerapan	Algoritma AIS Dominan	Tujuan/Manfaat Utama	Integrasi Pendukung
Deteksi Intrusi Jaringan	NSA, AIN	Identifikasi aktivitas anomali dalam lalu lintas jaringan	SVM, Decision Tree
Deteksi Malware & Phishing	CSA, Danger Theory	Klasifikasi varian malware dan analisis perilaku berbahaya	NLP, Feature Selection
Pertahanan Adversarial	SAIS	Meningkatkan ketahanan model AI terhadap gangguan input	Deep Learning
Keamanan IoT & Sistem Terdistribusi	AIN, Hybrid AIS	Deteksi kolaboratif dan autentikasi adaptif	Federated Learning
Deteksi Zero-Day	NSA + CSA (Hybrid)	Pengenalan ancaman baru tanpa tanda tangan	Deep Autoencoder

3.3 Tantangan dan Arah Penelitian Masa Depan

AIS memiliki potensi besar sebagai pendekatan bio-inspiratif yang adaptif dan tangguh, namun masih menghadapi berbagai kendala teknis dan ilmiah.

Tantanganan utamanya adalah:

1. **Skalabilitas dan kompleksitas komputasi.** Algoritma seperti *clonal selection* dan *immune network* membutuhkan sumber daya besar, sehingga sulit diterapkan pada sistem berskala

besar (misalnya *cloud computing*, IoT). Diperlukan optimalisasi melalui *parallel processing* atau *quantum computing*.[11]

2. **Keterbatasan generalisasi.** AIS masih lemah menghadapi serangan baru *(zero-day, adversarial attacks)* karena bergantung pada data historis. Solusinya adalah mekanisme pembelajaran adaptif dan meta-learning.
3. **Integrasi dengan kecerdasan buatan modern.** Penyatuan AIS dengan *deep learning* menjanjikan hasil kuat, tetapi sulit karena perbedaan paradigma. Arah baru mencakup *hybrid architecture* yang menggabungkan AIS, *reinforcement learning*, dan *generative* AI.
4. **Keterbatasan *dataset* dan *benchmark*.** Belum ada *dataset* standar untuk menilai kinerja AIS secara objektif; dibutuhkan *open benchmark datasets* dan evaluasi global.
5. **Aspek keamanan dan etika.** Implementasi AIS pada sistem otonom menimbulkan isu privasi, bias, dan akuntabilitas. Penelitian perlu menekankan *explainability* dan *ethical AI governance*.

Arah penelitian masa depan:

1. **Model simbiotik (SAIS).** Meniru hubungan biologis timbal balik untuk meningkatkan adaptivitas terhadap ancaman dinamis.
2. **Integrasi dengan *federated learning*.** Membangun sistem pertahanan kolaboratif tanpa berbagi data mentah, cocok untuk IoT dan *edge computing*.
3. **Pemanfaatan komputasi kuantum dan neuromorfik.** Meningkatkan efisiensi dalam *pattern matching* dan pembelajaran evolusioner.
4. **Kerangka kerja evaluasi terstandar.** Diperlukan *open-source toolkit* untuk pengujian dan perbandingan varian AIS secara objektif.
5. **Aplikasi generatif dan proaktif.** Fokus pada pencegahan dan prediksi serangan melalui *immune forecasting models*.

Secara keseluruhan, masa depan AIS bergantung pada kemampuannya beradaptasi dengan lanskap teknologi baru yang kompleks. Integrasi prinsip biologis, kecerdasan buatan modern, dan etika komputasi akan menjadi fondasi dalam membangun sistem keamanan siber yang cerdas, otonom, dan dapat dipercaya.[12]

4. Kesimpulan

Penelitian ini meninjau berbagai algoritma *Artificial Immune System* (AIS) dan penerapannya di bidang keamanan siber. Model dan algoritma utama dalam pengembangan *Artificial Immune System* meliputi *Negative Selection Algorithm*, *Clonal Selection Algorithm*, *Immune Network Model*, *Danger Theory Model*, serta versi lanjutannya seperti *Symbiotic* AIS dan *Deep Immune Models*.

Algoritma AIS diterapkan dalam keamanan siber untuk mendeteksi anomali secara adaptif, mengklasifikasikan ancaman berdasarkan pola imunologis, dan memperkuat pertahanan terhadap serangan adversarial melalui mekanisme pembelajaran, kloning, serta seleksi otomatis layaknya sistem imun biologis.

Kelebihan AIS terletak pada kemampuannya belajar adaptif dan mendeteksi anomali tanpa data latih besar, sedangkan keterbatasannya mencakup skalabilitas dan kompleksitas komputasi, dengan tantangan penelitian pada integrasi dengan *deep learning*, efisiensi energi, serta peningkatan transparansi dan ketahanan terhadap serangan baru.

Arah penelitian paling potensial untuk mengembangkan AIS generasi berikutnya adalah integrasi dengan *deep learning*, *edge intelligence*, dan *federated learning* guna menciptakan sistem imun digital yang lebih adaptif, efisien, serta transparan terhadap ancaman siber masa depan.

Secara keseluruhan, AIS berpotensi menjadi pilar utama *bio-inspired computing* untuk menciptakan sistem pertahanan siber generasi baru yang bersifat proaktif dalam mendeteksi dan mencegah ancaman, dengan kolaborasi lintas disiplin antara biologi komputasi, kecerdasan buatan, dan keamanan informasi sebagai kunci keberhasilan. Dengan berkembangnya paradigma

edge intelligence dan *federated learning*, AIS berpotensi menjadi tulang punggung sistem imun digital masa depan yang kolaboratif, transparan, dan etis.

Daftar Pustaka

[1] Badan Siber dan Sandi Negara (BSSN), Lanskap Keamanan Siber Indonesia 2024, BSSN, Jan. 2025. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2025/01/LANSKAP-KEAMANAN-SIBER-2024.pdf

[2] Kitchenham, B. & Charters, S., *"Guidelines for Performing Systematic Literature Reviews in Software Engineering"*, EBSE Technical Report EBSE-2007-01, Keele University & Lincoln University, UK, July 2007. Available: https://www.researchgate.net/publication/302924724

[3] X. Zhang, Y. Chen, and L. Wang, "Artificial Immune System of Secure Face Recognition Against Adversarial Attacks," *arXiv preprint arXiv:2406.18144*, 2024. [Online]. Available: https://arxiv.org/pdf/2406.18144

[4] N. Hasib, S. Bhattacharya, and M. Mahmud, "Artificial Immune System: A Systematic Literature Review," *ResearchGate Preprint*, July 2023. [Online]. Available: https://www.researchgate.net/publication/372474824

[5] L. N. de Castro and J. Timmis, *Artificial Immune Systems: A New Computational Intelligence Approach*. London, U.K.: Springer, 2002.

[6] D. Dasgupta Ed., *Artificial Immune Systems and Their Applications*. Berlin, Germany: Springer-Verlag, 1999.

[7] J. Timmis, "Artificial Immune Systems: Today and Tomorrow," *Natural Computing*, vol. 6, no. 1, pp. 1–18, 2007.

[8] F. Gonzalez and D. Dasgupta, "An Immunogenetic Approach to Intrusion Detection," in *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO)*, Las Vegas, USA, 2000, pp. 1311–1318.

[9] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-Nonself Discrimination in a Computer," in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1994, pp. 202–212.

[10] M. S. G. Khadri and M. R. Khadri, "SAIS: A Novel Bio-Inspired Artificial Immune System Based on Symbiotic Paradigm," *arXiv preprint arXiv:2402.07244*, 2024. [Online]. Available: https://arxiv.org/pdf/2402.07244

[11] L. N. de Castro and F. J. Von Zuben, "Learning and Optimization Using the Clonal Selection Principle," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 3, pp. 239–251, 2002.

[12] P. Greensmith, J. Timmis, and U. Aickelin, "Artificial Immune Systems for Intrusion Detection: A Review," in *Proceedings of the 3rd International Conference on Artificial Immune Systems (ICARIS)*, Catania, Italy, 2004, pp. 57–67.