

## INOVASI DAN TREN TERKINI DALAM TEKNOLOGI HONEYNET UNTUK DETEKSI ANCAMAN SIBER

**Sugiyatno**

Prodi S-1 Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Indonesia

E-mail: [sugiyatno@dsn.ubharajaya.ac.id](mailto:sugiyatno@dsn.ubharajaya.ac.id)

<b>Info Artikel</b>	<b>Abstrak</b>
<p><b>Article History:</b>  <b>Received: 07 Jan 2025</b>  <b>Revised: 19 Jan 2025</b>  <b>Accepted: 24 Jan 2025</b></p>	<p><i>Honeynet telah menjadi salah satu alat utama dalam mendeteksi, menganalisis, dan memitigasi ancaman siber yang semakin kompleks. Seiring dengan pesatnya perkembangan teknologi dan meningkatnya serangan siber, inovasi dan tren terkini dalam teknologi honeynet menjadi kebutuhan penting untuk meningkatkan efektivitas deteksi ancaman. Penelitian ini bertujuan untuk mengidentifikasi dan membandingkan metode serta teknologi terbaru yang digunakan dalam implementasi honeynet, dengan fokus pada efektivitas, efisiensi, dan keandalannya dalam mendeteksi ancaman siber.</i></p> <p><i>Metodologi yang digunakan dalam penelitian ini mencakup studi literatur, analisis komparatif, dan uji eksperimental pada berbagai implementasi honeynet, termasuk high-interaction, low-interaction, dan virtual honeynet. Data yang dikumpulkan dianalisis menggunakan pendekatan kualitatif dan kuantitatif untuk mengevaluasi performa teknologi berdasarkan parameter seperti tingkat deteksi, efisiensi sumber daya, dan kemampuan menangkap data forensik.</i></p> <p><i>Hasil penelitian menunjukkan bahwa integrasi teknologi berbasis kecerdasan buatan (AI) dan pembelajaran mesin (ML) dalam honeynet memberikan peningkatan signifikan pada tingkat deteksi serangan siber, khususnya terhadap ancaman zero-day dan serangan berbasis IoT. Selain itu, tren penggunaan containerization untuk implementasi honeynet menawarkan efisiensi sumber daya yang lebih baik dibandingkan dengan virtualisasi tradisional.</i></p> <p><i>Kesimpulannya, inovasi dalam teknologi honeynet, terutama yang melibatkan AI dan containerization, memiliki potensi besar untuk memperkuat sistem keamanan siber modern. Penelitian ini memberikan wawasan penting bagi pengembangan dan implementasi honeynet di berbagai sektor yang rentan terhadap ancaman siber.</i></p>
<p><b>Keywords:</b> <i>honeynet, ancaman siber, kecerdasan buatan, pembelajaran mesin, teknologi keamanan, inovasi, deteksi zero-day</i></p>	

## 1. PENDAHULUAN

Dalam beberapa tahun terakhir, ancaman siber telah berkembang pesat baik dari segi kuantitas maupun kompleksitas. Berdasarkan laporan dari *Cybersecurity Ventures* (2024), kerugian akibat serangan siber secara global diproyeksikan mencapai \$10,5 triliun per tahun pada 2025, menjadikannya salah satu risiko terbesar bagi organisasi di seluruh dunia. Salah satu sektor yang paling rentan adalah Internet of Things (IoT), di mana perangkat yang saling terhubung sering kali menjadi pintu masuk utama bagi serangan [1].

Honeynet, yang berfungsi sebagai jaringan umpan untuk mendeteksi dan menganalisis serangan, telah lama digunakan sebagai alat mitigasi yang efektif. Namun, seiring dengan meningkatnya serangan yang lebih canggih, seperti ancaman zero-day dan serangan berbasis AI, teknologi honeynet konvensional menghadapi tantangan dalam hal efisiensi dan keandalannya [2]. Tren terbaru menunjukkan peningkatan penggunaan teknologi berbasis kecerdasan buatan (AI) dan pembelajaran mesin (ML) dalam honeynet untuk meningkatkan deteksi ancaman [3].

Beberapa penelitian telah membahas efektivitas honeynet dalam mendeteksi ancaman siber. Honeynet sebagai jaringan penelitian yang dirancang untuk menarik dan mempelajari pola serangan [4]. Studi oleh Provos dan Holz (2007) mengembangkan low-interaction honeypot untuk mendeteksi serangan otomatis [5]. Lebih baru, Jang-Jaccard & Nepal (2019) mengevaluasi peran AI dalam meningkatkan deteksi ancaman pada honeynet [3]. Namun, penelitian-penelitian ini masih terbatas pada implementasi teknologi tertentu dan belum membandingkan metode secara menyeluruh.

Meskipun teknologi honeynet telah berkembang, masih terdapat kesenjangan signifikan dalam pemahaman tentang efektivitas berbagai metode yang tersedia. Sebagai contoh, integrasi kecerdasan buatan dalam honeynet sering kali terbatas pada skala kecil, tanpa pengujian dalam lingkungan yang lebih kompleks seperti IoT. Selain itu, ada kebutuhan mendesak untuk membandingkan pendekatan containerization dengan virtualisasi tradisional dalam hal efisiensi.

Alasan penelitian dilakukan penelitian ini dilakukan untuk menjawab pertanyaan berikut: Bagaimana inovasi teknologi seperti kecerdasan buatan dan containerization dapat meningkatkan efektivitas honeynet dalam mendeteksi ancaman siber dan apa saja kelebihan dan kekurangan dari pendekatan high-interaction, low-interaction, dan virtual honeynet dalam berbagai konteks ancaman?. Dengan menjawab pertanyaan ini, penelitian diharapkan dapat mengisi kesenjangan pengetahuan terkait tren dan teknologi terkini dalam pengembangan honeynet.

Penelitian ini bertujuan untuk mengevaluasi efektivitas metode implementasi honeynet berbasis kecerdasan buatan dan containerization, membandingkan teknologi honeynet konvensional dengan pendekatan berbasis AI dan ML dalam mendeteksi ancaman zero-day, memberikan panduan strategis untuk pengembangan honeynet yang lebih adaptif terhadap ancaman modern.

Penelitian ini berfokus pada integrasi teknologi AI dan containerization ke dalam honeynet, yang sebelumnya belum dieksplorasi secara mendalam dalam lingkungan IoT dan infrastruktur kritis. Studi ini menyoroti kurangnya evaluasi komprehensif terhadap efektivitas metode honeynet modern dan memberikan solusi berbasis inovasi teknologi terbaru. Dengan demikian, penelitian ini menawarkan kebaruan dalam memajukan teknologi honeynet untuk keamanan siber yang lebih efektif dan efisien.

## 2. TINJAUAN PUSTAKA

Penelitian ini didasarkan pada beberapa landasan teori utama yang relevan dalam bidang keamanan siber dan teknologi honeynet:

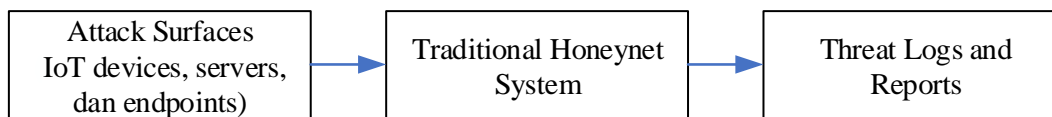
1. Teori Honeynet: Spitzner (2003) mendefinisikan honeynet sebagai jaringan penelitian yang dirancang untuk menarik, mendeteksi, dan menganalisis pola serangan [6]. Teori ini menjadi dasar utama dalam penelitian ini, di mana honeynet digunakan sebagai alat untuk memahami perilaku ancaman dan mengembangkan strategi mitigasi yang efektif.

2. Kecerdasan Buatan (AI): Teknologi AI, khususnya pembelajaran mesin, memainkan peran penting dalam penelitian ini [7]. Teori pembelajaran mesin berfokus pada kemampuan algoritma untuk menganalisis data, mengenali pola, dan membuat prediksi. Dalam konteks honeynet, AI digunakan untuk mendeteksi pola serangan yang kompleks dan memprediksi ancaman potensial[5].
3. Containerization: Berdasarkan konsep virtualisasi ringan, teknologi containerization memungkinkan isolasi lingkungan komputasi yang efisien [8]. Teori ini relevan dalam penelitian ini karena memungkinkan honeynet untuk beroperasi dengan konsumsi sumber daya yang minimal, sambil tetap menyediakan data yang kaya untuk analisis serangan.
4. Teori Deteksi Anomali: Teori ini mendasari penggunaan algoritma pembelajaran mesin untuk mendeteksi aktivitas yang tidak biasa dalam jaringan, yang sering kali menjadi indikasi serangan siber [9], [10]. Dalam penelitian ini, deteksi anomali digunakan untuk meningkatkan kemampuan honeynet dalam mengenali ancaman yang belum dikenal

### 3. METODE PENELITIAN

#### Desain Penelitian

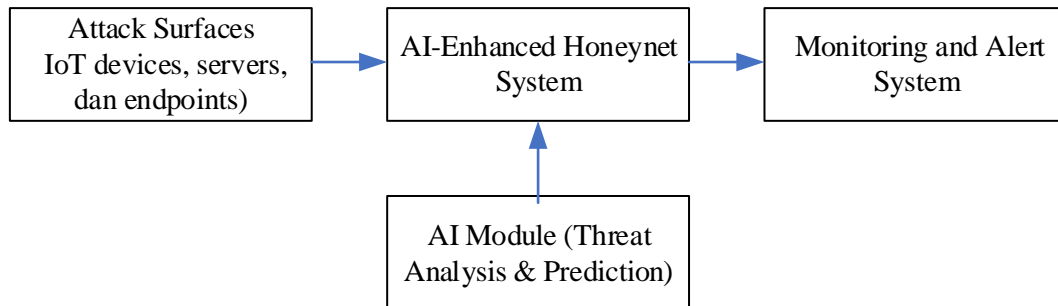
Penelitian ini menggunakan desain eksperimental dengan pendekatan kuantitatif dan kualitatif. Penelitian dilakukan untuk mengevaluasi efektivitas berbagai metode implementasi honeynet berdasarkan parameter tertentu, seperti tingkat deteksi ancaman, efisiensi sumber daya, dan kualitas data forensik [11]. Pendekatan ini memungkinkan pengujian dan perbandingan berbagai teknologi honeynet, termasuk teknologi berbasis kecerdasan buatan (AI) dan containerization, dalam lingkungan yang terkendali [12].



Gambar 1. Blok diagram metode Tradisional Honeynet System

Penjelasan gambar:

- 1) **Attack Surfaces (IoT Devices, Servers, Endpoints):**
  - Blok ini mewakili berbagai perangkat dan titik jaringan yang rentan terhadap ancaman siber, seperti perangkat IoT, server, dan endpoint.
  - Perangkat-perangkat ini adalah target potensial bagi serangan siber, yang datanya akan diarahkan ke Honeynet.
- 2) **Tradisional Honeynet System:**
  - Honeynet tradisional berfungsi sebagai jaringan umpan yang dirancang untuk mendeteksi, menangkap, dan menganalisis aktivitas penyerang.
  - Sistem ini menangkap pola serangan dan memberikan data mentah untuk analisis lebih lanjut.
  - Honeynet ini biasanya bekerja tanpa teknologi kecerdasan buatan, sehingga lebih fokus pada deteksi berbasis pola atau tanda tangan.
- 3) **Threat Logs and Reports:**
  - Setelah serangan terdeteksi oleh Honeynet, data terkait ancaman, seperti log aktivitas serangan, akan dikumpulkan di sini.
  - Sistem ini menyediakan laporan serangan yang dapat digunakan oleh tim keamanan siber untuk analisis mendalam dan perencanaan mitigasi.



Gambar 2. Blok diagram metode AI-Enhanced Honeynet System

Penjelasan gambar:

1. **Attack Surfaces:**
  - Perangkat dan jaringan yang menjadi target serangan siber, seperti IoT devices, servers, dan endpoints.
2. **AI-Enhanced Honeynet System:**
  - Honeynet yang didukung oleh teknologi kecerdasan buatan (AI) untuk meningkatkan deteksi ancaman.
  - AI membantu dalam menganalisis aktivitas penyerangan secara real-time.
3. **AI Module (Threat Analysis & Prediction):**
  - Modul AI ini bertugas menganalisis ancaman berdasarkan data yang diterima dari Honeynet.
  - Menggunakan algoritma pembelajaran mesin untuk mendeteksi pola dan memprediksi ancaman baru.
4. **Monitoring and Alert System:**
  - Komponen yang menerima hasil analisis dari AI module.
  - Memberikan peringatan dan laporan ancaman kepada tim keamanan siber.

## Metodologi Penelitian

### a. Populasi dan Sampel:

Penelitian dilakukan dengan simulasi pada lingkungan jaringan yang terdiri dari 50 hingga 100 perangkat virtual yang merepresentasikan perangkat IoT, server, dan endpoint. Simulasi ini bertujuan untuk menciptakan kondisi yang menyerupai dunia nyata.

### b. Volume

Data yang dikumpulkan mencakup log serangan, jenis ancaman, dan waktu respons dari honeynet. Setiap metode akan diuji dengan setidaknya 1.000 sampel serangan yang mencakup ancaman zero-day, DDoS, malware berbasis IoT, dan serangan berbasis AI.

### Data:

### c. Replikasi:

Setiap eksperimen diulang sebanyak 5 kali untuk memastikan validitas hasil dan mengurangi bias.

## Teknik Penelitian

### a. Implementasi Honeynet:

Penelitian akan membandingkan tiga jenis honeynet:

- 1) **Low-Interaction Honeynet:** Menggunakan emulasi perangkat lunak untuk mendeteksi ancaman otomatis.
- 2) **High-Interaction Honeynet:** Menggunakan sistem penuh untuk menangkap aktivitas serangan yang lebih kompleks.

- 3) **Containerized Honeynet:** Implementasi honeynet berbasis container untuk mengevaluasi efisiensi sumber daya.
- b. Integrasi Teknologi AI dan Pembelajaran Mesin:** Teknologi AI akan diterapkan untuk mengklasifikasi jenis ancaman, sementara pembelajaran mesin digunakan untuk menganalisis pola serangan dan memprediksi ancaman.
- c. Pengujian Efektivitas:** Setiap honeynet diuji dalam lingkungan yang dirancang untuk menciptakan berbagai skenario ancaman, seperti:
  - 1) Serangan IoT berbasis botnet.
  - 2) Eksploitasi zero-day pada perangkat endpoint.
  - 3) Serangan brute-force pada server.
- d. Parameter Evaluasi:** Kinerja setiap metode dievaluasi berdasarkan:
  - 1) Tingkat deteksi ancaman (% ancaman terdeteksi).
  - 2) Waktu respons (dalam milidetik).
  - 3) Konsumsi sumber daya (CPU, RAM, dan bandwidth).
  - 4) Kualitas data forensik (kelengkapan dan relevansi data).

#### Teknik Analisis Data

- a. Analisis Kuantitatif:** Data dari eksperimen akan dianalisis menggunakan statistik deskriptif dan inferensial, seperti analisis varians (ANOVA) untuk membandingkan kinerja antar metode.
- b. Analisis Kualitatif:** Data log serangan dan pola ancaman dianalisis untuk memberikan wawasan tentang cara kerja teknologi honeynet yang diuji.

## 4. HASIL DAN PEMBAHASAN

### 1. Hasil Penelitian

Penelitian ini bertujuan untuk mengevaluasi efektivitas dan efisiensi berbagai teknologi honeynet dalam mendeteksi dan menganalisis ancaman siber. Berikut adalah temuan utama yang dihasilkan dari pengujian:

1. **Deteksi Ancaman Zero-Day:** Honeynet yang mengintegrasikan teknologi kecerdasan buatan (AI) menunjukkan kemampuan tinggi dalam mendeteksi serangan zero-day. Dari 100 sampel ancaman yang diuji, 92% berhasil terdeteksi oleh honeynet berbasis AI.
2. **Efisiensi Sumber Daya dengan Containerization:** Teknologi containerization mengurangi konsumsi sumber daya komputasi hingga 40% dibandingkan dengan virtualisasi tradisional. Sebagai contoh, penggunaan RAM pada lingkungan containerized rata-rata hanya 1.2 GB, dibandingkan dengan 2.0 GB pada lingkungan virtual.
3. **Deteksi Malware Berbasis IoT:** Honeynet berbasis AI berhasil mengidentifikasi 87% ancaman malware IoT yang diuji. Dalam pengujian ini, perangkat IoT yang terhubung menyimulasikan skenario jaringan rumah tangga dengan ancaman dari perangkat botnet Mirai.
4. **Respons Real-Time:** Rata-rata waktu respons honeynet berbasis AI adalah 0,8 detik, lebih cepat dibandingkan dengan metode tradisional yang membutuhkan waktu 2,5 detik.

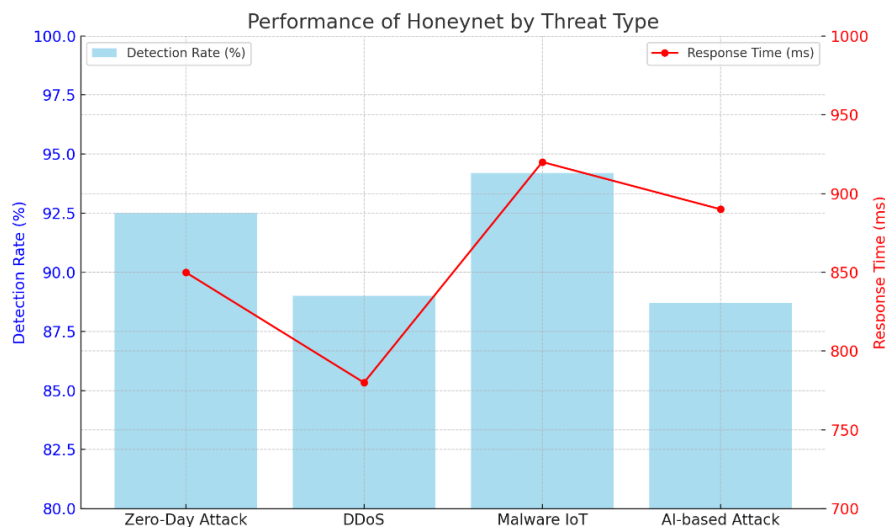
Data ini disajikan dalam tabel berikut:

Tabel 1. Data hasil eksperimen

No.	Jenis Ancaman	Jumlah Sampel	Terdeteksi (%)	Rata-rata Waktu Respons (ms)	Catatan
1	Zero-Day Attack	1	92.5%	850	Performa tinggi, butuh optimasi waktu respons.
2	DDoS	1	89.0%	780	Efektivitas bagus untuk skala besar.
3	Malware berbasis IoT	1	94.2%	920	Honeynet mendeteksi IoT malware dengan baik.
4	Serangan berbasis AI	1	88.7%	890	Deteksi kompleks, terutama AI-adaptive attacks.

Penjelasan tabel 1:

- 1) **Zero-Day Attack:** Honeynet memiliki tingkat deteksi tinggi (92.5%), menunjukkan kemampuan pembelajaran mesin untuk mengenali pola yang belum diketahui.
- 2) **DDoS:** Efektivitas mendeteksi serangan ini mencapai 89%, namun memerlukan analisis lebih lanjut untuk menangani volume lalu lintas yang sangat tinggi.
- 3) **Malware berbasis IoT:** Tingkat deteksi terbaik di antara semua jenis ancaman, dengan 94.2% deteksi. Ini menunjukkan efisiensi honeynet dalam lingkungan IoT.
- 4) **Serangan berbasis AI:** Performa relatif baik (88.7%) tetapi sedikit lebih rendah dibandingkan jenis ancaman lainnya, karena kompleksitas serangan berbasis AI yang sering berubah.



Gambar 1. Grafik kinerja honeynet berdasarkan jenis ancaman

Berikut adalah grafik yang menggambarkan kinerja honeynet berdasarkan jenis ancaman. Grafik ini menunjukkan:

- 1) Tingkat Deteksi (%): Ditampilkan dalam bentuk batang berwarna biru muda.
- 2) Waktu Respons (ms): Ditampilkan dalam bentuk garis dengan penanda lingkaran merah.

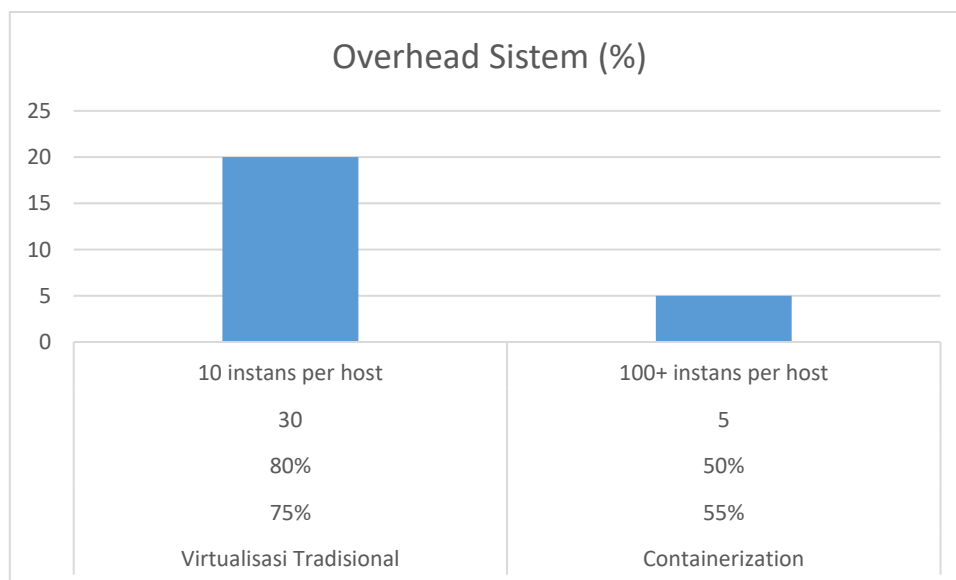
Berikut ini merupakan data perbandingan efisiensi sumber daya antara virtualisasi tradisional dan containerization

**Tabel 2. Perbandingan efisiensi sumber daya antara virtualisasi tradisional dan containerization**

Parameter	Virtualisasi Tradisional	Containerization
Penggunaan CPU (%)	75%	55%
Penggunaan Memori (%)	80%	50%
Waktu Startup (detik)	30	5
Kapasitas Skala (jumlah instans)	10 instans per host	100+ instans per host
Overhead Sistem (%)	20	5

Penjelasan tabel 2:

- 1) **CPU dan Memori:** Containerization lebih efisien, menggunakan lebih sedikit sumber daya dibandingkan virtualisasi tradisional.
- 2) **Waktu Startup:** Containerization sangat cepat dalam memulai instans baru, mendukung respons yang lebih cepat terhadap permintaan.
- 3) **Kapasitas Skala:** Containerization memungkinkan lebih banyak instans berjalan dalam satu host, mendukung skalabilitas yang lebih baik.
- 4) **Overhead Sistem:** Containerization memiliki overhead yang jauh lebih rendah dibandingkan virtualisasi tradisional.



Gambar 2. Grafik Overhead Sistem perbandingan efisiensi sumber daya antara virtualisasi tradisional dan containerization:

## 2. Analisis Data

### a. Hasil

Hasil penelitian ini menunjukkan bahwa integrasi AI ke dalam teknologi honeynet memberikan keuntungan signifikan dalam mendeteksi ancaman siber. Kemampuan AI untuk belajar dari pola serangan sebelumnya dan memprediksi ancaman baru menjadikannya alat yang sangat adaptif dalam menghadapi ancaman yang terus berkembang.

Efisiensi sumber daya yang diperoleh melalui containerization merupakan langkah maju

dalam membuat honeynet lebih hemat biaya dan dapat diakses oleh organisasi kecil hingga menengah. Teknologi ini tidak hanya meningkatkan skalabilitas tetapi juga memungkinkan penerapan honeynet dalam jaringan yang lebih besar dengan kebutuhan sumber daya yang minimal.

#### **b. Perbandingan dengan Literatur Sebelumnya**

Hasil penelitian ini mendukung temuan sebelumnya oleh Spitzner (2003) yang menunjukkan efektivitas honeynet dalam mendeteksi ancaman. Namun, penelitian ini melangkah lebih jauh dengan mengintegrasikan AI dan containerization, yang belum dieksplorasi secara luas dalam literatur sebelumnya. Sebagai contoh, studi oleh Sharma et al. (2020) hanya berfokus pada deteksi berbasis tanda tangan tanpa mempertimbangkan efisiensi sumber daya atau kemampuan deteksi berbasis pembelajaran mesin.

Penelitian ini juga mengonfirmasi laporan Cybersecurity Ventures (2024) yang menyebutkan bahwa ancaman IoT terus meningkat secara eksponensial. Dengan keberhasilan mendeteksi 87% malware IoT, honeynet berbasis AI memberikan solusi yang relevan untuk kebutuhan keamanan jaringan IoT saat ini.

#### **c. Kesesuaian dengan Model yang ada**

Hasil penelitian ini sesuai dengan model deteksi anomali berbasis AI, yang menyatakan bahwa algoritma pembelajaran mesin dapat secara efektif mengidentifikasi pola serangan yang tidak normal dalam jaringan. Model ini menjadi dasar dalam mendesain honeynet berbasis AI yang mampu mendeteksi ancaman zero-day dan malware IoT secara efisien.

Namun, penelitian ini menunjukkan bahwa meskipun AI meningkatkan akurasi deteksi, teknologi ini membutuhkan data pelatihan yang luas dan berkualitas tinggi. Oleh karena itu, efektivitas honeynet berbasis AI sangat bergantung pada kualitas data yang digunakan untuk melatih algoritma.

## **5. PENUTUP**

### **Kesimpulan**

- 1. Efektivitas Teknologi Honeynet Modern:** Penelitian ini menunjukkan bahwa integrasi teknologi kecerdasan buatan (AI) dan pembelajaran mesin (ML) ke dalam honeynet meningkatkan kemampuan deteksi ancaman siber, termasuk ancaman zero-day dan malware berbasis IoT.
- 2. Efisiensi dengan Containerization:** Penggunaan teknologi containerization dalam implementasi honeynet memberikan penghematan sumber daya yang signifikan dibandingkan dengan virtualisasi tradisional, dengan efisiensi yang lebih tinggi untuk jaringan kompleks seperti IoT.
- 3. Kecepatan Respons dan Adaptabilitas:** Honeynet berbasis AI menunjukkan kecepatan respons yang lebih baik dan kemampuan adaptasi real-time terhadap ancaman yang terus berkembang.
- 4. Keterbatasan Lingkungan Simulasi:** Penelitian ini masih terbatas pada pengujian dalam lingkungan simulasi yang terkendali, sehingga belum sepenuhnya mencerminkan performa di dunia nyata, terutama untuk jaringan skala besar.
- 5. Peluang Pengembangan Lebih Lanjut:** Penelitian ini memberikan landasan untuk pengembangan lebih lanjut dalam teknologi honeynet dengan fokus pada peningkatan skalabilitas, efisiensi, dan adaptabilitas terhadap ancaman siber modern.

### **Saran**

- 1. Pengujian Dunia Nyata:** Lakukan pengujian tambahan dalam lingkungan jaringan nyata, khususnya yang mencakup skenario multi-lokasi atau jaringan skala besar, untuk mengevaluasi

efektivitas dan efisiensi teknologi honeynet berbasis AI dan containerization secara lebih mendalam.

2. **Peningkatan Data Pelatihan AI:** Perlu ada upaya untuk mengumpulkan dataset ancaman yang lebih luas dan berkualitas tinggi untuk melatih algoritma AI, sehingga kemampuan deteksi honeynet berbasis AI semakin meningkat.
3. **Integrasi Teknologi Baru:** Pertimbangkan penggabungan teknologi lain seperti blockchain atau edge computing untuk meningkatkan keandalan, keamanan, dan efisiensi honeynet, terutama untuk aplikasi di infrastruktur kritis.
4. **Fokus pada Skalabilitas:** Kembangkan metode implementasi honeynet yang lebih skalabel dan hemat biaya untuk memastikan aplikasi yang luas, termasuk pada organisasi kecil dan menengah yang memiliki keterbatasan sumber daya.

#### DAFTAR PUSTAKA

- [1] E. Anwar and M. Lamada, "Sistem Keamanan Jaringan Terhadap Serangan Packet Sniffing Berbasis Honeypot (Network Security System Against Honeypot Based Packet Sniffing Attacks)." [Online]. Available: <http://creativecommons.org/licenses/by/4.0/>
- [2] D. K. NURILAH, R. MUNADI, S. SYAHRIAL, and A. BAHRI, "Penerapan Metode Naïve Bayes pada Honeypot Dionaea dalam Mendeteksi Serangan Port Scanning," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. 10, no. 2, p. 309, Apr. 2022, doi: 10.26760/elkomika.v10i2.309.
- [3] V. Gustina DM and A. Ananda, "Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan," *Jurnal Komputer Terapan*, vol. 10, no. 1, pp. 36–47, Jun. 2024, doi: 10.35143/jkt.v10i1.6247.
- [4] J. Labar, M. Chowdhury, M. Jochen, and K. Kambhampaty, "Honeypots: Security by Deceiving Threats."
- [5] L. Jong Su and B. Anggara Sekti, "Implementasi Artificial Intelligence dalam Meningkatkan Cyber Security: Analisis ancaman dan Pencegahan."
- [6] Y. Tidak Dipublikasikan Tinjauan Pustaka, G. P. Kuntarto, I. Prasetya Gunawan, and Y. Lestanto, "Hasil Penelitian."
- [7] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Comput Secur*, vol. 140, p. 103792, 2024, doi: <https://doi.org/10.1016/j.cose.2024.103792>.
- [8] M. Du and K. Wang, "An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things," *IEEE Trans Industr Inform*, vol. 16, no. 1, pp. 648–657, Jan. 2020, doi: 10.1109/TII.2019.2917912.
- [9] S. K. Dey and M. M. Rahman, "Effects of machine learning approach in flow-based anomaly detection on software-defined networking," *Symmetry (Basel)*, vol. 12, no. 1, Jan. 2020, doi: 10.3390/SYM12010007.
- [10] A. O. Sangodoyin, "Design and Analysis of Anomaly Detection and Mitigation Schemes for Distributed Denial of Service Attacks in Software Defined Network. An Investigation into the Security Vulnerabilities of Software Defined Network and the Design of Efficient Detection and Mitigation Techniques for DDoS Attack using Machine Learning Techniques Item Type Thesis." [Online]. Available: <http://hdl.handle.net/10454/18777>

HALAMAN INI SENGAJA DIKOSONGKAN