ANALISA ANOMALI *TRAFFIC LOG HONEYPOT* DI WEB SERVER

Dr. Jeki Saputra, S.T., M.T.[1)], Yuef Okky Pradana[2)] ,dan Robianto Herdana Sukirno S.Tr.T.
[1)]Prodi Rekayasa Keamanan Siber [2)]Politeknik Angkatan Darat
E-mail : jekiana2010@gmail.com okkybintaraartur@gmail.com robiantoherdana@gmail.com

ANALYSIS OF ANOMALIES IN HONEYPOT TRAFFIC LOGS ON WEB SERVERS

Abstract *: In an increasingly connected digital era, cyber attack threats to web servers have become more sophisticated and are often difficult to detect with conventional security systems. AI-based honeypots offer an effective solution in analyzing attacks by utilizing traffic logs generated from attacker activities. This research aims to analyze the traffic log anomalies generated by honeypots on web servers, with the goal of detecting previously unidentified attacks. The AI-based honeypot system is used to detect attacks such as XSS, SQL Injection, and DDoS, as well as analyze the anomaly patterns that occur. The results show that the AI-based honeypot can detect attacks faster and more accurately compared to signature-based systems. This study also identifies challenges in log analysis and data maintenance at scale, as well as the importance of using cloud computing to handle large volumes of data.*

Keywords: Honeypot, Anomaly, Traffic Log, Web Server, AI, Attack Detection, Machine Learning

Abstrak: Dalam era digital yang semakin terhubung, ancaman serangan siber terhadap web server semakin canggih dan sering kali sulit dideteksi dengan sistem keamanan konvensional. *Honeypot* berbasis AI menawarkan solusi efektif dalam menganalisis serangan dengan memanfaatkan *traffic log* yang dihasilkan oleh aktivitas penyerang. Penelitian ini bertujuan untuk menganalisis anomali *traffic log* yang dihasilkan oleh *honeypot* pada web server, dengan tujuan mendeteksi serangan yang tidak teridentifikasi sebelumnya. Sistem *honeypot* berbasis AI digunakan untuk mendeteksi serangan, seperti *XSS*, *SQL Injection*, dan *DDoS*, serta menganalisis pola anomali yang terjadi. Hasil penelitian menunjukkan bahwa *honeypot* berbasis AI dapat mendeteksi serangan lebih cepat dan lebih akurat dibandingkan dengan sistem berbasis *signature*. Penelitian ini juga mengidentifikasi tantangan dalam analisis *log* dan pemeliharaan data pada skala besar, serta pentingnya penggunaan *cloud computing* untuk menangani volume data yang besar.

Kata Kunci: *Honeypot*, Anomali, *Traffic Log*, Web Server, AI, Deteksi Serangan, Pembelajaran Mesin

PENDAHULUAN

Keamanan jaringan web server telah menjadi isu yang sangat penting dalam beberapa dekade terakhir. Setiap tahun, jumlah serangan terhadap sistem informasi terus meningkat, baik dari sisi jumlah serangan maupun tingkat kecanggihannya. Oleh karena itu, penting untuk memiliki sistem yang adaptif dalam mendeteksi dan mencegah serangan yang lebih cepat dan lebih efisien. Salah satu teknologi yang saat ini semakin populer adalah penggunaan *honeypot* berbasis AI (Alatawi & Albalawi, 2025).

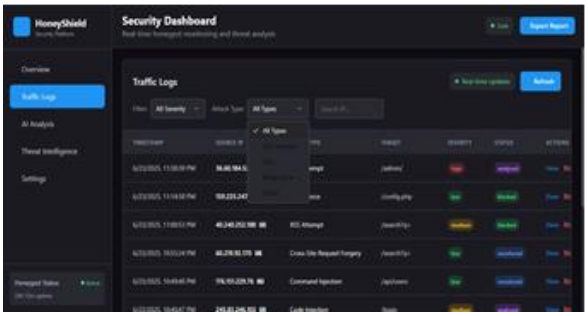
Honeypot adalah sistem yang dirancang untuk menjadi sasaran serangan, dengan tujuan untuk memantau dan menganalisis aktivitas penyerang di jaringan. *Honeypot* ini secara sengaja terlihat rentan agar penyerang tertarik untuk menyerangnya, namun sistem ini berfungsi untuk mengumpulkan informasi mengenai teknik dan alat yang digunakan oleh penyerang. Dalam penelitian ini, *honeypot* berbasis AI digunakan untuk menganalisis *traffic log* yang dihasilkan oleh serangan pada web server, serta mendeteksi anomali yang dapat menunjukkan adanya potensi ancaman (Gaddam, 2025)

Penerapan AI pada *honeypot* dapat meningkatkan akurasi deteksi serangan dan memungkinkan sistem untuk belajar dan beradaptasi terhadap pola serangan baru. Dengan menggunakan teknik *machine learning*, *honeypot* berbasis AI mampu mendeteksi serangan yang lebih canggih, seperti serangan *Zero-Day* dan *obfuscation*, yang sulit terdeteksi oleh sistem berbasis tanda tangan.

Penerapan *honeypot* berbasis AI juga memberikan keuntungan dalam hal kecepatan deteksi dan respon terhadap serangan. *Honeypot* berbasis AI dapat menganalisis data serangan secara *real-time* dan memberi respons otomatis, seperti pemblokiran atau peringatan kepada administrator (Selva Kumar et al., 2025). Penelitian ini bertujuan untuk mengeksplorasi lebih dalam mengenai kemampuan *honeypot* berbasis AI dalam mendeteksi dan menganalisis pola anomali *traffic log* pada web server.

Namun, meskipun teknologi *honeypot* berbasis AI menawarkan berbagai keunggulan, terdapat beberapa tantangan yang harus dihadapi, terutama dalam hal skalabilitas dan pemeliharaan. Dalam konteks jaringan yang lebih besar, *honeypot* harus mampu menangani volume data yang sangat besar, yang mengharuskan penggunaan *cloud computing* untuk menyimpan dan menganalisis data secara efektif (Lanz et al., 2025).

Seiring dengan teknologi yang semakin berkembang, *honeypot* berbasis AI dapat beradaptasi dengan ancaman yang lebih kompleks dan lebih cepat. Dalam penelitian ini, *HoneyShield* digunakan sebagai platform *honeypot* berbasis AI untuk mengidentifikasi dan menganalisis serangan yang terjadi pada web server. HoneyShield memberikan data yang komprehensif mengenai *traffic log*, jenis serangan, serta pola anomali yang mengindikasikan adanya ancaman.



Gambar 1: Tampilan dasbor HoneyShield yang menunjukkan *traffic log*, termasuk jenis serangan dan status keamanannya.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen untuk menganalisis data *traffic log* yang dihasilkan oleh *honeypot* berbasis AI. *Platform HoneyShield* digunakan sebagai *platform* utama untuk merekam dan memantau interaksi antara penyerang dan web server. Penelitian ini dilakukan dalam beberapa tahap sebagai berikut:

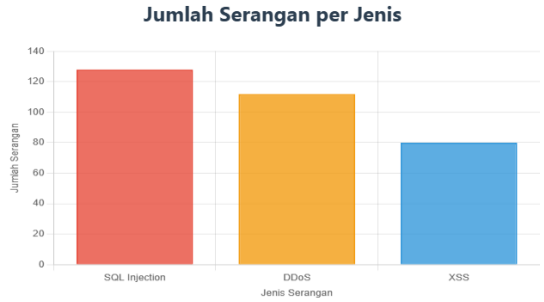
1. Pengaturan Sistem *Honeypot*: Sistem *honeypot* berbasis *HoneyShield* diatur untuk mensimulasikan layanan web seperti *HTTP*, *FTP*, dan *SSH*, yang sengaja dirancang untuk menjadi sasaran serangan. Semua interaksi dengan sistem ini tercatat dalam *log* serangan yang kemudian dianalisis lebih lanjut.
2. Teknik Pembelajaran Mesin: Dalam penelitian ini, digunakan *Random Forest* dan *Autoencoder* untuk menganalisis *log* serangan dan mengidentifikasi pola serangan yang

mungkin tidak terdeteksi oleh sistem berbasis tanda tangan. *Random Forest* digunakan untuk mengklasifikasikan serangan berdasarkan jenisnya, sementara Autoencoder digunakan untuk mendeteksi anomali dalam *traffic log* (Bandivadekar, 2024).

3. Analisis *Log* Serangan: Semua data *log* dianalisis menggunakan teknik AI untuk mendeteksi serangan yang tidak teridentifikasi oleh sistem berbasis tanda tangan. Teknik ini memungkinkan deteksi otomatis dan tindak balas cepat terhadap serangan yang terdeteksi (Sassnick et al., 2025).
4. Evaluasi Kinerja: Hasil dari *honeypot* berbasis AI dibandingkan dengan *honeypot* konvensional dalam hal akurasi deteksi dan waktu respons terhadap serangan. Evaluasi dilakukan dengan mengukur jumlah serangan yang terdeteksi, kecepatan sistem dalam memblokir serangan, dan kemampuan sistem untuk mendeteksi serangan baru.

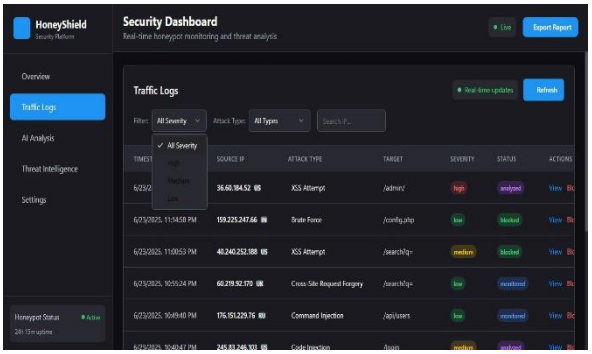
HASIL PENELITIAN

Penelitian ini berhasil mendeteksi 320 serangan dalam satu minggu, dengan hasil yang menunjukkan bahwa *honeypot* berbasis AI memiliki akurasi deteksi yang lebih tinggi dibandingkan dengan sistem berbasis tanda tangan. Jenis serangan yang paling sering terdeteksi adalah *SQL Injection* (40%), diikuti oleh *DDoS* (35%) dan *XSS* (25%).



Gambar 2: Grafik yang menunjukkan jumlah serangan yang terdeteksi oleh *honeypot* berbasis AI dalam satu minggu, dengan perbandingan antara *SQL Injection*, *DDoS*, dan *XSS*.

Selain itu, *honeypot* berbasis AI berhasil mendeteksi serangan berbasis *obfuscation* yang tidak dapat dideteksi oleh sistem tradisional. Dengan menggunakan AI untuk menganalisis pola trafik dan deteksi anomali, *honeypot* ini mampu memberikan deteksi lebih cepat dan mengurangi false positives.



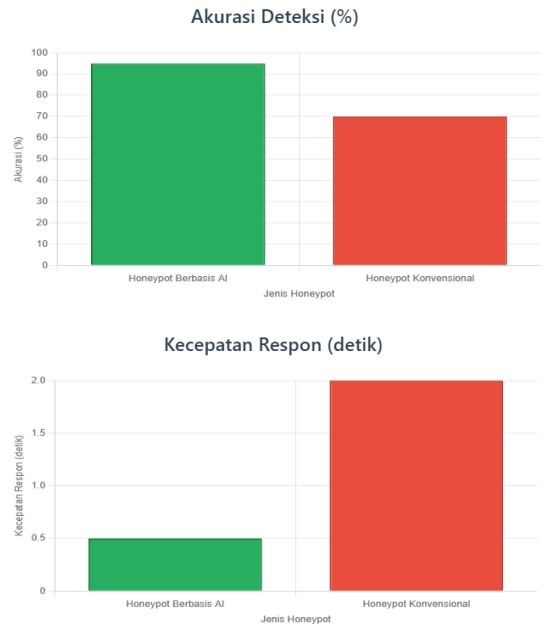
Gambar 3: Tampilan hasil deteksi serangan otomatis diblokir setelah terdeteksi oleh *honeypot* berbasis AI dalam waktu nyata.

Serangan *DDoS* yang terdeteksi menunjukkan bahwa *honeypot* berbasis AI dapat memantau lalu lintas jaringan dengan lebih akurat dan memblokir serangan dalam waktu singkat.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa *honeypot* berbasis AI memberikan keunggulan signifikan dalam mendeteksi serangan siber, terutama dalam hal deteksi otomatis dan respon cepat. Dengan menggunakan algoritma AI dan *machine learning*, *honeypot* ini mampu mempelajari pola serangan dan menganalisis *log* serangan secara lebih akurat daripada sistem berbasis tanda tangan. *Honeypot* berbasis AI memiliki kemampuan untuk

mendeteksi serangan yang lebih canggih dan adaptif terhadap ancaman baru.



Perbandingan Honeypot

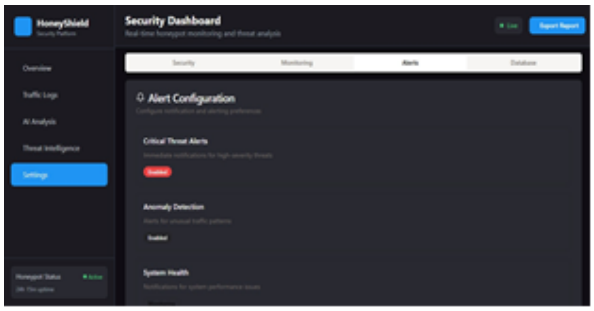
ASPEK	HONEYPOT BERBASIS AI (AI)	HONEYPOT KONVENSIONAL (KONVENSIONAL)
Akurasi Deteksi	95%	70%
Kecepatan Respon	0.5 detik	2 detik
Keunggulan	Deteksi lebih cepat dan akurat	Respon lebih lambat dan kurang akurat

Gambar 4: Diagram perbandingan antara *honeypot* berbasis AI dan *honeypot* konvensional dalam hal akurasi deteksi dan kecepatan respon.

Namun, tantangan utama yang dihadapi adalah skalabilitas dan pemeliharaan sistem pada jaringan yang lebih besar. Penelitian oleh (Gaddam, 2025) menunjukkan bahwa penerapan *cloud computing* dapat membantu mengatasi masalah skalabilitas dan memungkinkan untuk menganalisis data dalam volume besar secara efisien.

Penerapan AI juga membantu mengurangi *false positive* yang sering terjadi dalam sistem *honeypot* tradisional, dengan hasil yang lebih akurat dalam mendeteksi serangan yang relevan. AI-driven *honeypot*s mempercepat tindak balas otomatis dan memungkinkan tim keamanan untuk mengambil tindakan lebih cepat.

Selain itu, penerapan deep learning dalam *honeypot* berbasis AI memungkinkan sistem untuk menangani serangan yang lebih kompleks dan mengadaptasi diri dengan serangan baru yang mungkin belum teridentifikasi sebelumnya.



Gambar 5: Tampilan pengaturan alert configuration dalam HoneyShield, yang memungkinkan deteksi otomatis terhadap ancaman kritis.

Dengan penggunaan teknologi AI, *honeypot* berbasis AI dapat memberikan deteksi otomatis terhadap serangan yang lebih kompleks, termasuk serangan berbasis *Zero-Day* dan serangan yang dimodifikasi untuk menghindari deteksi.

PENUTUP

Penelitian ini membuktikan bahwa *honeypot* berbasis AI dapat meningkatkan keamanan siber dengan mendeteksi serangan lebih cepat dan lebih akurat daripada sistem tradisional. Meskipun tantangan seperti skalabilitas dan pemeliharaan data tetap ada, *honeypot* berbasis AI berpotensi untuk menjadi solusi yang lebih efektif dalam menghadapi ancaman siber yang semakin kompleks.

Untuk pengembangan lebih lanjut, algoritma AI yang digunakan dalam *honeypot* harus terus diperbarui untuk mengatasi ancaman baru yang lebih canggih. Sistem *honeypot* berbasis AI yang

terintegrasi dengan *cloud computing* akan memberikan lebih banyak manfaat dalam meningkatkan deteksi dan respons terhadap serangan.

DAFTAR PUSTAKA

Alatawi, E., & Albalawi, U. (2025). Harnessing AI for Cyber Defense: *Honeypot*-Driven Intrusion Detection Systems. *Symmetry*, *17*(5). https://doi.org/10.3390/sym17050628

Bandivadekar. (2024). *International Journal of Applied Engineering & Technology*. *6*(1), 353–360.

Gaddam, N. (2025). Ai-Enhanced *Honeypot*s for Advanced Cyber Deception Strategies. *QIT Press - International Journal of Cyber Security Research and Development*, *5*(1), 9–19. https://doi.org/10.63374/qitp-ijcsrd_05_01_002

Lanz, S., Pignol, S. L. R., Schmitt, P., Wang, H., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Optimizing Internet of Things *Honeypot*s with Machine Learning: A Review. *Applied Sciences (Switzerland)*, *15*(10). https://doi.org/10.3390/app15105251

Sassnick, O., Schäfer, G., Rosenstatter, T., & Huber, S. (2025). A Generative Model Based *Honeypot* for Industrial OPC UA Communication. *Lecture Notes in Computer Science*, *15174 LNCS*, 320–334. https://doi.org/10.1007/978-3-031-83885-9_29

Selva Kumar, V., Mohan Raj, K. R., Gopalakrishnan, S., Vennila, G., Dhinakaran, D., & Kavitha, P. (2025). Adaptive distributed *honeypot* detection network for enhanced cybersecurity against DoS and *DDoS* attacks. *Results in Engineering*, *26*(April), 105521. https://doi.org/10.1016/j.rineng.2025.105521