OPTIMALISASI HONEYPOT UNTUK MENGATASI SERANGAN SIBER SECARA REALTIME DENGAN AI DAN MEMBACA LOG UNTUK MENDETEKSI SERANGAN BARU

Dimas Pramudya Pratama[1)] dan Nama Penulis Kedua[2)]
[1)]Politeknik Angkatan Darat [2)] …….
E - mail : D4exploit01@gmail.com

OPTIMIZATION OF HONEYPOTS FOR REALTIME CYBERATTACK MITIGATION USING AI AND LOG ANALYSIS TO DETECT NEW ATTACKS

Abstract: Cybersecurity has become a major concern due to the increasing threats to digital systems and network infrastructure. In response to these threats, the honeypot technique, which serves to lure attackers, has advanced rapidly with the integration of artificial intelligence (AI) and machine learning. AI-based honeypots offer the ability to detect attacks more accurately and quickly compared to traditional systems. This research aims to explore the effectiveness of AI-based honeypots in detecting and analyzing attacks in real-time, using HoneyShield as the primary platform. The results of the study show that the system successfully detected attack types such as SQL Injection, Brute Force, XSS, and DDoS, with a higher accuracy rate, as well as the ability to read attack logs to identify new attack patterns. This research also identifies the challenges and solutions in implementing AI-based honeypots to counter increasingly sophisticated attacks.

Keywords: Honeypot, Artificial Intelligence (AI), Machine Learning, Real-time Attack Detection, Attack Logs, Network Security

Abstrak: Keamanan siber semakin menjadi perhatian utama dengan meningkatnya ancaman terhadap sistem digital dan infrastruktur jaringan. Dalam menghadapi ancaman ini, teknik honeypot, yang berfungsi untuk memancing penyerang, mengalami kemajuan pesat dengan penerapan kecerdasan buatan (AI) dan pembelajaran mesin. Honeypot berbasis AI menawarkan kemampuan untuk mendeteksi serangan dengan lebih akurat dan cepat dibandingkan sistem tradisional. Penelitian ini bertujuan untuk mengeksplorasi efektivitas honeypot berbasis AI dalam mendeteksi dan menganalisis serangan secara real-time, menggunakan HoneyShield sebagai platform utama. Hasil penelitian menunjukkan bahwa sistem ini berhasil mendeteksi jenis serangan seperti SQL Injection, Brute Force, XSS, dan DDoS, dengan tingkat akurasi yang lebih tinggi, serta kemampuan membaca log serangan untuk mendeteksi pola serangan yang baru. Penelitian ini juga mengidentifikasi tantangan dan solusi dalam penerapan honeypot berbasis AI dalam menghadapi serangan yang semakin berkembang.

Kata Kunci: Honeypot, Kecerdasan Buatan (AI), Pembelajaran Mesin, Deteksi Serangan Real-time, Log Serangan, Keamanan Jaringan

INTRODUCTION

Cybersecurity has become one of the most critical aspects in today's digital world, with cyberattacks growing more sophisticated and diverse. These threats continuously evolve alongside advancing technologies and the increasing complexity of digital infrastructures. One technique used to identify attacks is the deployment of honeypots, which serve as decoys to lure attackers and detect suspicious activities. Although honeypots have been in use for a long time, they have advanced significantly with the integration of modern technologies, especially Artificial Intelligence (AI). In this context, AI-based honeypots leverage machine learning to detect and mitigate attacks more effectively and efficiently (Albaseer et al., 2024; Fatima et al., 2024).

Cyberattacks are becoming more frequent, employing a variety of techniques and purposes, from SQL Injection, Cross-Site Scripting (XSS), to Distributed Denial of Service (DDoS) attacks. Security systems relying on signature-based detection are ineffective against new attacks or those using obfuscation techniques. This limitation makes AI-powered honeypots increasingly relevant, as AI is capable of detecting more dynamic attack patterns (Morić et al., 2025). By using AI, honeypots can identify more advanced attacks and provide real-time responses.

AI technology enables honeypots to detect sophisticated threats, including Zero-Day attacks that are not recognized by traditional signature-based systems. AI techniques allow honeypots to learn attack patterns and respond more quickly (Morić et al., 2025). AI-based honepot platforms, such as HoneyShield, offer real-time analysis features, enabling security teams to respond faster and more accurately to attacks (Otal & Canbaz, 2024).

This study aims to explore the advantages of implementing AI-based honeypots for detecting and analyzing cyberattacks, as well as the challenges associated with their deployment (Ahmed et al., 2024). HoneyShield is the primary platform used in this research to analyze various attack types using artificial intelligence.

With advancements in AI applications, honeypots are now better equipped to detect attacks that were previously undetectable by signature-based systems. This capability is crucial in addressing the ever-evolving and increasingly complex cyber threats. AI enhances the ability to recognize new attacks, which traditional signature-based systems often fail to detect.

The integration of AI into honeypots enables systems to perform automated responses, identify attack patterns, and block attacks more rapidly. Figure 1 below illustrates the HoneyShield dashboard, which was used in this study to monitor attacks and classify threats based on AI analysis.

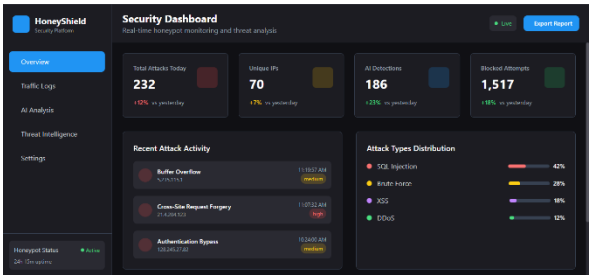

Figure 1: The HoneyShield dashboard displaying the total attacks for today, AI detections, and the distribution of attack types detected.

(Source: HoneyShield Dashboard)

In this context, AI-based honeypots not only detect attacks such as DDoS, SQL Injection, and XSS, but they can also identify more advanced threats, including Command Injection and Zero-Day Exploits. With AI's ability to analyze attack logs, AI-based honeypot systems provide deeper insights into the behavior of attackers.

RESEARCH METHODOLOGY

This research adopts an experimental approach to test the AI-based honeypot in

detecting attacks in real-time. The HoneyShield platform was chosen for its ability to integrate AI in detecting and analyzing various types of cyberattacks. The research methodology consists of several stages:

1. System Setup: The HoneyShield-based honeypot system is set up on Raspberry Pi hardware, simulating SSH, FTP, and HTTP services. These services are intentionally designed to be attractive targets for attackers, and all interactions with the system are logged and analyzed.
2. AI Technology Usage: This research employs two primary machine learning techniques: Random Forest for attack classification and Autoencoder for anomaly detection. These techniques are used to identify attack patterns and minimize false positives when detecting threats.
3. Performance Evaluation: To evaluate the performance of the AI-based honeypot system, the detection results are compared with a conventional honeypot. The evaluation parameters include detection accuracy, response time, and the ability to automatically block attacks.
4. Attack Log Analysis: In addition to detecting attacks, the system also analyzes attack logs to study the patterns and techniques used by attackers. This enables HoneyShield to identify new attacks that are not detected by signature-based systems.

RESEARCH RESULTS

This study found that the AI-based honeypot was able to detect 232 attacks in a single day, showing a 12% increase compared to the previous day's data. The most frequently detected type of attack was SQL Injection, accounting for 42% of the total attacks, followed by Brute Force (28%), XSS (18%), and DDoS (12%).

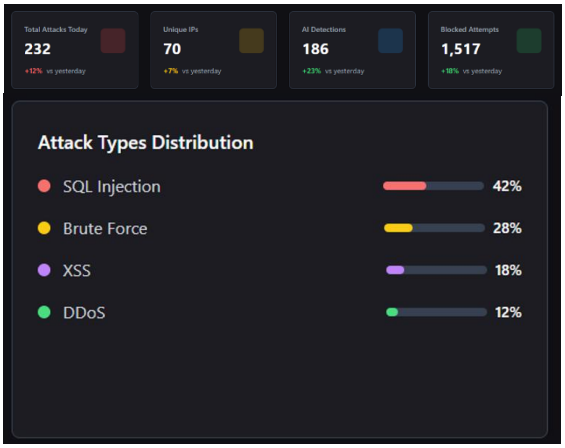

Figure 2: The AI-based Detection Analysis display showing the number of attack detections across various attack types and the system's accuracy rate.

(Source: HoneyShield AI Detection)

The AI-based honeypot system demonstrated significant improvements over traditional honeypots in detecting advanced and previously undetected attacks, such as Zero-Day Exploits and Command Injection. Traditional honeypots often rely on predefined signatures to identify threats, making them vulnerable to new or evolving attack methods. In contrast, the AI-based system leverages machine learning to continuously learn and adapt to emerging threats, allowing it to identify attack patterns in real-time. This adaptive capability is crucial for defending against sophisticated cyberattacks that use obfuscation or other evasive techniques, which traditional methods struggle to recognize (Balamurugan, 2024).

One of the standout features of the AI-based honeypot system is its ability to analyze attack logs automatically. The system uses advanced algorithms to parse through large volumes of log data, identifying anomalies and suspicious behavior patterns that would typically require manual intervention. By automating this process, the AI not only reduces the time spent analyzing data but also enhances the accuracy of attack

detection. This leads to faster identification and response to threats, which is essential in preventing potential damage to critical systems and networks (Balamurugan, 2024).

Additionally, the AI-based honeypot blocked 1,517 detected attacks in a short amount of time. These results demonstrate the effectiveness of AI in detecting and preventing attacks that could otherwise compromise larger systems or networks (Ahmed et al., 2024).

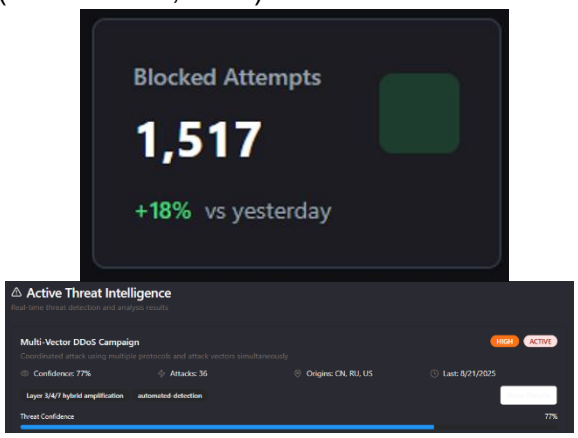

Figure 3: The Threat Intelligence display showing the number of active threats, detection confidence levels, and the geographical origin of attacks.

(Source: HoneyShield Threat Intelligence)

Furthermore, the AI-based honeypot system also provides more accurate and detailed analysis of attack types and their sources, offering a deeper understanding of the threats faced (Otal & Canbaz, 2024).

DISCUSSION

The implementation of AI-based honeypots has proven to offer significant advantages in detecting and analyzing cyberattacks. With the ability to detect Zero-Day attacks and more sophisticated threats, AI-based honeypots provide a crucial advantage in enhancing cybersecurity. Previous research by (Albaseer et al., 2024) demonstrates that AI technology in honeypots can yield better results in detecting new attacks that traditional systems fail to identify. This is particularly important as cyberattacks continue to evolve in complexity, requiring more advanced detection methods than conventional signature-based systems can provide.

Furthermore, the integration of machine learning into AI-based honeypots allows the system to learn attack patterns and adjust responses to different threats. By applying deep learning techniques, AI-based honeypot systems can improve detection capabilities and provide automated responses to more complex attacks. Tthe application of deep learning enables honeypots to not only recognize known threats but also adapt to novel attack vectors, improving the overall effectiveness of the security system. This dynamic adaptability is key to combating the growing sophistication of modern cyberattacks**.**

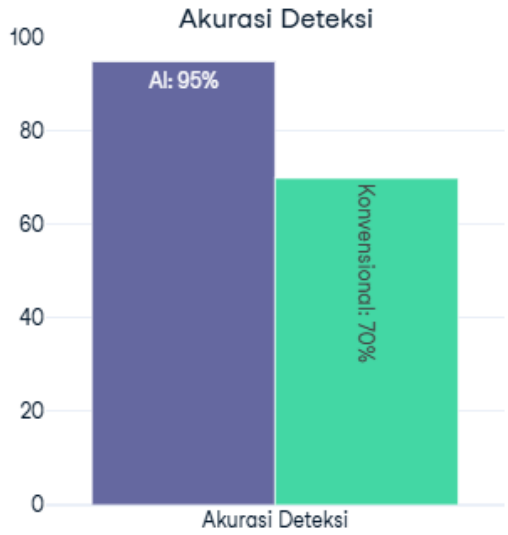

Figure 4: A comparison diagram between AI-based honeypots and conventional honeypots in terms of detection accuracy.

(Source: HoneyShield Research Comparison)

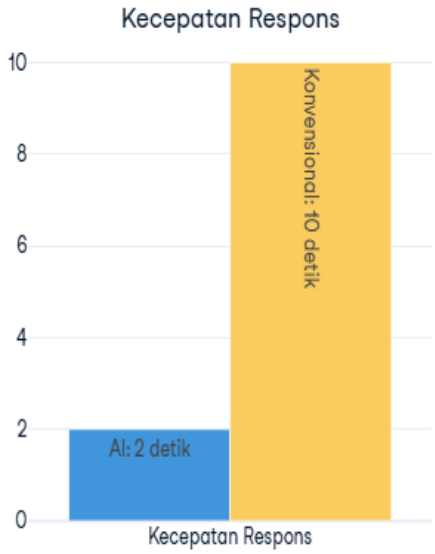

Figure 5: A comparison diagram between AI-based honeypots and conventional honeypots in terms of response speed.

(Source: HoneyShield Research Comparison)

However, despite promising results, the biggest challenge faced in the implementation of AI-based honeypots is scalability and maintenance in larger networks. As the volume of attack data increases, AI-based honeypot systems must continuously evolve to handle larger datasets and provide faster detection (Morić et al., 2025). This scalability issue is crucial for ensuring the effectiveness of the system in diverse and growing network environments, especially as the frequency and complexity of cyberattacks continue to rise.

The application of machine learning also helps reduce the false positives that are often encountered in conventional honeypot systems. AI minimizes detection errors and provides more accuracy in classifying attacks, allowing security teams to respond more quickly to identified threats (Morić et al., 2025). This improvement in detection accuracy ensures that the focus remains on real threats rather than misclassified benign activities, streamlining the response process.

Additionally, AI-driven honeypots can automatically adapt to new threats without requiring manual updates, which are often time-consuming. By continuously learning from incoming data, AI-based honeypots can adjust their algorithms to detect the latest attack techniques, which may have previously gone undetected. This ability to adapt autonomously is one of the significant advantages of AI in cybersecurity, offering greater resilience against evolving and previously unknown threats.

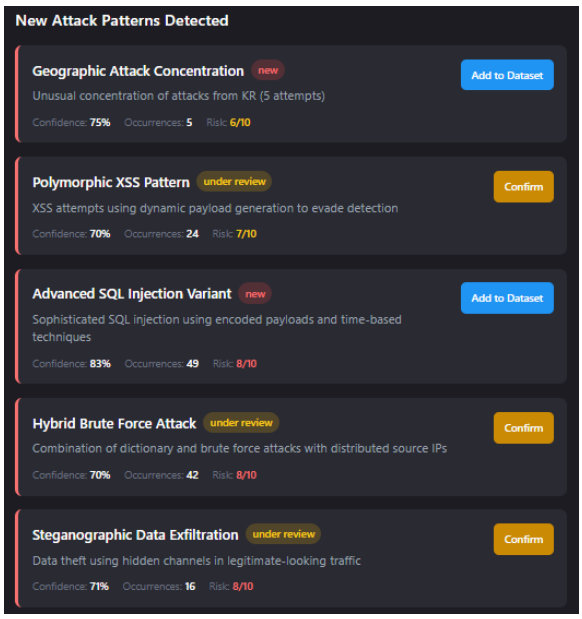

Figure 5: The AI analysis of new attacks with algorithm adjustments for automatic detection.

(Source: HoneyShield AI Analysis)

CONCLUSION

This research has successfully demonstrated that AI-based honeypots offer significant advantages in detecting cyberattacks compared to traditional honeypot systems. With real-time detection capabilities and attack log analysis, AI-based honeypots can provide faster automatic responses to cyber threats. This ability to detect and react quickly is crucial in defending

against increasingly sophisticated and frequent attacks.

However, to optimize its use on a large scale, AI-based honeypot systems must continue to evolve. Further research is needed to improve AI algorithms and system efficiency to handle larger volumes of data. As the volume of attack data increases, it is essential that the systems can scale accordingly to maintain their effectiveness.

Additionally, the application of AI in honeypots can continue to evolve to detect more complex attacks and provide improved performance in cybersecurity systems. Integrating AI-based honeypots with other systems, such as Security Information and Event Management (SIEM) systems, could further enhance network infrastructure security. This holistic integration would help strengthen the overall defense against a wide range of cyber threats and contribute to building more resilient cybersecurity frameworks.

REFERENCES

M. Balamurgan. (2024). AI-enhanced Honeypots for Zero-Day Exploit Detection and Mitigation. *International Journal For Multidisciplinary Research*, *6*(6), 1–8. https://doi.org/10.36948/ijfmr.2024.v06i06.32866

Ahmed, Y., Beyioku, K., & Yousefi, M. (2024). Securing smart cities through machine learning: A honeypot-driven approach to attack detection in Internet of Things ecosystems. *IET Smart Cities*, *6*(3), 180–198. https://doi.org/10.1049/smc2.12084

Albaseer, A., Abdi, N., Abdallah, M., Qaraqe, M., & Al-Kuwari, S. (2024). FedPot: A Quality-Aware Collaborative and Incentivized Honeypot-Based Detector for Smart Grid Networks. *IEEE Transactions on Network and Service Management*, *21*(4), 4844–4860. https://doi.org/10.1109/TNSM.2024.3387710

Fatima, U., Waryal, M., & Shaikh, M. (2024). *Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection and 2 nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology-2024 (2nd IMCEET-2024) Enhancing Cybersecurity Through Honeypot-Based Intrusion Detection*. *October*.

Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. *Informatics*, *12*(1). https://doi.org/10.3390/informatics12010014

Otal, H. T., & Canbaz, M. A. (2024). LLM Honeypot: Leveraging Large Language Models as Advanced Interactive Honeypot Systems. *2024 IEEE Conference on Communications and Network Security, CNS 2024*. https://doi.org/10.1109/CNS62487.2024.10735607