www.ijarp.com ISSN 2456-9992 Page: 01-08

International Journal Advanced Research Publications

Research Article

Volume: 02
Issue: 03

ENTROSENTRY: A BEHAVIORAL ANALYSIS USING DECOY FRAMEWORK FOR ZERO-DAY THREAT DETECTION

Kathija Sirajun Nisha B [a], Mrs. Sharon Nisha[b]*

a. Department of Computer Science Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu – 627003.

b. Department of Computer Science Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu – 627003.

Article Received: 31 January 2026, Article Revised: 21 February 2026, Published on: 13 March 2026

***Corresponding Author: Mrs. Sharon Nisha**

Department of Computer Science Engineering, Francis Xavier Engineering, College, Tirunelveli, Tamil Nadu – 627003.

DOI: https://doi-doi.org/101555/ijarp.3834

ABSTRACT

The rising complexity of contemporary cyberattacks has greatly diminished the efficacy of conventional signature-based detection mechanisms. Zero-day threats, which target unknown vulnerabilities, are particularly hard to detect since there are no prior attack signatures available during the time of attack exploitation [2], [3]. This paper introduces EntroSentry, a proactive detection framework that combines behavioral monitoring based on entropy and deception-driven intelligence gathering. The proposed system analyzes the statistical anomalies in real-time traffic patterns and uses machine learning algorithms to categorize the anomalies [4], [10]. Simultaneously, an adaptive honeypot module is used to monitor attacker behavior in specially designed decoy environments [5], [6]. By correlating entropy anomalies with attacker interaction information, EntroSentry improves the detection accuracy and minimizes false positives. Simulation outcomes show better robustness against unknown attacks compared to traditional intrusion detection systems [11], [22].

KEYWORDS: Zero-Day Detection; Entropy-Based Anomaly Detection; Cyber Deception; Honeypot Systems; Machine Learning; Behavioral Intrusion Detection.

1. INTRODUCTION

The methodology of the proposed system involves continuous packet capture, feature extraction and aggregation, entropy analysis, machine learning-based anomaly classification,

conditional decoy activation, and behavioral feedback integration. Unsupervised learning algorithms identify anomalies in system behavior without the need for labeled training data [7]. Semi-supervised learning algorithms improve classification accuracy when labeled data is limited [24]. The decoy system provides insight into attacker behavior and validates entropy-based alerts in a contextual manner [6], [16]. This two-tiered validation system reduces false positives compared to traditional anomaly detection systems [22].

2. RELATED WORK

2.1 Machine Learning in Intrusion Detection

Recent research has shown the potential of deep learning and hybrid AI models in enhancing intrusion detection performance [3], [11]. Various surveys have confirmed that AI-powered systems outperform rule-based systems in detecting unknown threats [4], [22]. Unsupervised learning methods are especially beneficial in zero-day attacks since they do not require labeled attack data [2], [7]. Semi-supervised learning methods further improve classification accuracy even when labeled data is limited [24]. GAN-based anomaly detection models have also been investigated to enhance recognition of sophisticated or evolving attack behaviors [14].

2.2 Deception and Honeypot-Based Monitoring

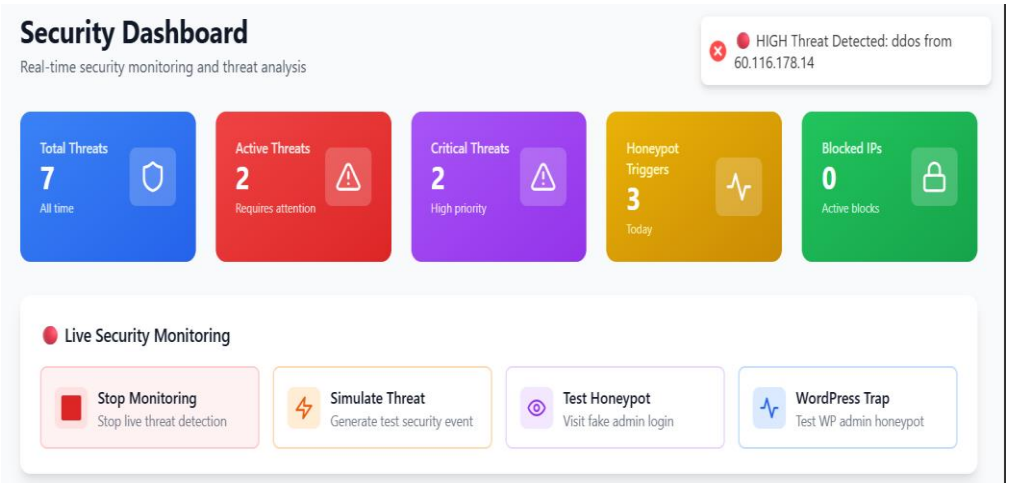
Honeypot-based monitoring systems have matured from simple traps to dynamic and containerized deception systems that can realistically mimic services [5], [18]. Research has shown that interactive honeypot systems can record attacker strategies and tools [6], [9]. AI-powered honeypot systems have further improved threat intelligence analysis by examining behavioral patterns in interactive honeypot systems [17], [21]. SSH honeypot systems and web-interaction honeypots have been successfully employed to monitor real-world intrusion attempts [18], [19]. However, most of the previous work considers anomaly detection and deception systems independently. There are very few frameworks that combine entropy-based behavioral analysis with honeypot intelligence in a continuous feedback loop

3. PROPOSED FRAMEWORK

The EntroSentry framework has an architecture that is divided into three layers.

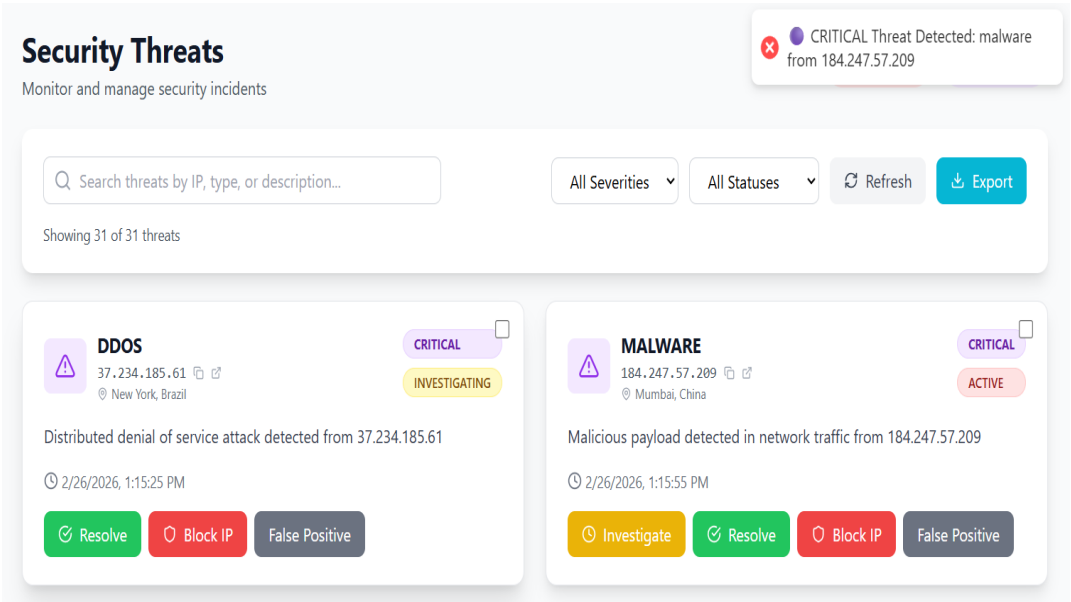
3.1 Behavioral Monitoring Module

This module is responsible for monitoring network traffic in real-time and extracting statistical features. Rather than relying on packet payload signatures alone, it also analyzes distribution features such as connection rate, port rate, and protocol variety [8].



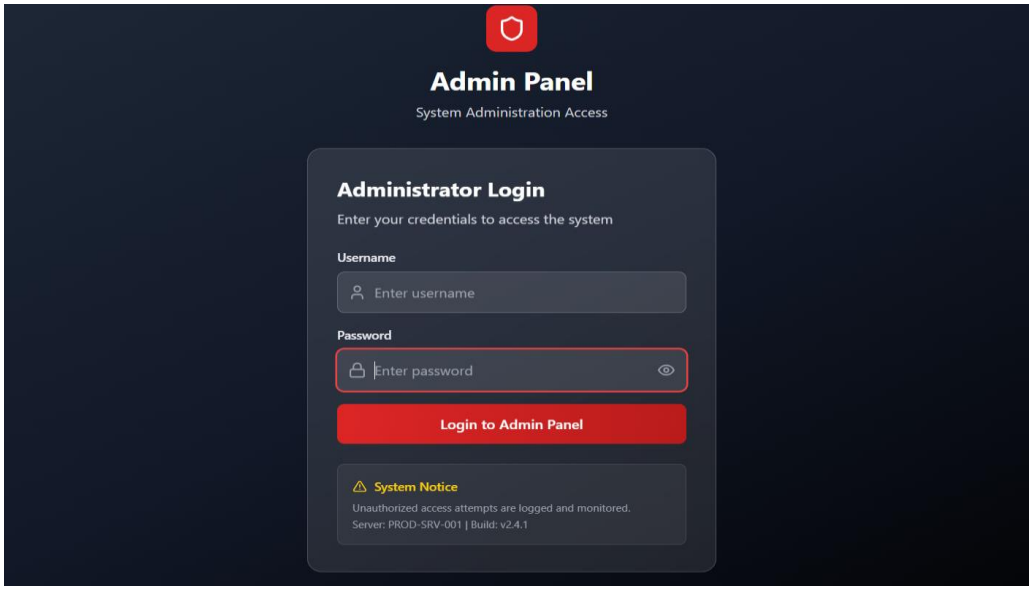
3.2 Entropy-Based Anomaly Engine

Entropy is employed as a measure of uncertainty in network properties. Large variations in the values of entropy point to irregular network traffic distribution patterns [15]. Machine learning classifiers are employed to determine whether anomalies are benign or malicious based on features extracted from entropy values [10], [22]. Optimization classifiers and attention classifiers can be employed to improve detection accuracy in IoT networks [20].



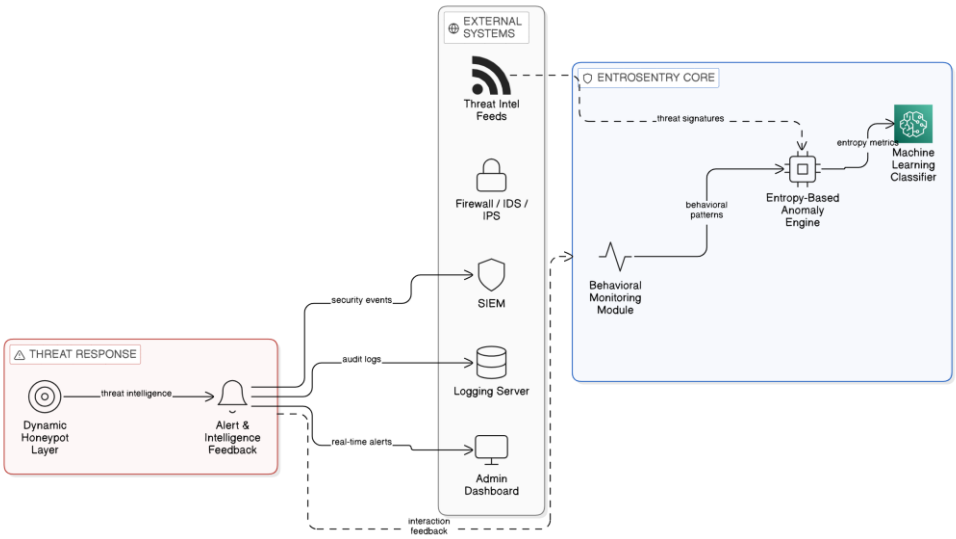
3.3 Dynamic Decoy Layer

The deception layer employs interactive SSH and web-based honeypots that mimic legitimate services [18], [19]. These decoys trap attackers while monitoring login attempts, command execution patterns, payload delivery attempts, and lateral movement simulations. Interaction data is analyzed using AI-powered honeypot intelligence models [21], which improve awareness of behavioral context.



4. METHODOLOGY

The functional methodology involves continuous packet capture, feature extraction and aggregation, entropy calculation, machine learning-based anomaly classification, dynamic decoy activation, and behavioral feedback integration. Unsupervised learning algorithms are employed to identify anomalies in baseline behavior without relying on labeled data [7]. Semi-supervised learning algorithms can be employed to improve classification accuracy when labeled data is limited [24]. The decoy system provides insight into attacker behavior and contextual validation of alerts triggered by entropy changes [6], [16]. This two-tier validation system is more effective in reducing false positives than anomaly detection systems [22].



5. EXPERIMENTAL EVALUATION

The proposed framework was evaluated using standard datasets and simulated environments with both benign traffic and zero-day attacks. The evaluation criteria included detection accuracy, false positives, and adaptability to novel attack patterns. High detection accuracy has been reported by hybrid AI-based intrusion detection systems in recent studies [11], and GAN-based models show enhanced anomaly detection abilities [14]. EntroSentry showed high detection accuracy for novel attack behaviors, lowered false positives compared to static IDS models, and enhanced attacker behavior profiling using decoy interaction insights. The system also showed robustness against obfuscation attacks in malware, which is consistent with findings from deep learning-based malware detection studies [25].

6. RESULTS AND DISCUSSION

The experimental outcome shows that entropy-based monitoring provides early warnings of potential attacks, but deception system-based reinforcement enhances detection accuracy. AI-based IDS frameworks have been shown to outperform rule-based systems in zero-day attack detection in previous studies [4], [22]. Honeypot intelligence provides attackers' tactic insights that are not possible with passive monitoring approaches [6], [16].

Future work can be extended to include federated learning-based distributed detection frameworks for large-scale networks [13] and novelty detection frameworks to maintain adaptability against evolving threats [12]. Insider threat detection methods can also be integrated into the proposed framework for enterprise-wide protection [23].

7. CONCLUSION

EntroSentry proposes an integrated cybersecurity framework that combines entropy-based anomaly detection with adaptive deception. The proposed framework enhances zero-day attack detection accuracy with reduced false positives by correlating statistical uncertainty with attacker interaction intelligence. The combination of AI-based anomaly classification and dynamic honeypot intelligence offers a scalable and adaptive defense paradigm that is appropriate for today’s enterprise networks. Future research will investigate federated intelligence sharing [13] and learning-based intrusion detection [12] to improve defenses against future cyber threats.

8. REFERENCES

1. E. Alatawi and U. Albalawi, "Harnessing AI for Cyber Defense: Honeypot-Driven Intrusion Detection Systems," *Symmetry*, vol. 17, no. 5, Art. no. 628, 2025, doi: 10.3390/sym17050628.
2. A. Jain and R. Bagoria, "An Intelligent Zero-Day Attack Detection System Using Unsupervised Machine Learning," *Knowledge-Based Systems*, vol. 324, Art. no. 113833, 2025, doi: 10.1016/j.knosys.2025.113833.
3. S. Soltani, M. Asghari, and H. Takabi, "An Adaptable Deep Learning-Based Intrusion Detection System Against Zero-Day Attacks," *Journal of Information Security and Applications*, vol. 76, Art. no. 103516, 2023, doi: 10.1016/j.jisa.2023.103516.
4. A. Hozouri, A. Mirzaei, and M. Effatparvar, "A Comprehensive Survey on Intrusion Detection Systems with Machine Learning and Deep Learning Approaches," *Discover Artificial Intelligence*, vol. 5, Art. no. 314, 2025, doi: 10.1007/s44163-025-00578-1.
5. V. S. Devi Priya and S. Sibi Chakkaravarthy, "Containerized Cloud-Based Honeypot Deception for Tracking Attackers," *Scientific Reports*, vol. 13, Art. no. 1437, 2023, doi: 10.1038/s41598-023-28613-0.
6. Z. Morić, V. Dakić, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," *Informatics*, vol. 12, no. 1, Art. no. 14, 2025, doi: 10.3390/informatics12010014.
7. S. Oluwadare and Z. ElSayed, "A Survey of Unsupervised Learning Algorithms for Zero-Day Attacks in Intrusion Detection Systems," in *Proc. 36th FLAIRS Conf.*, 2023, doi: 10.32473/flairs.36.133182.
8. A. Pinto, L.-C. Herrera, and J. A. Gutierrez, "Enhancing Critical Infrastructure Security Through Unsupervised Anomaly Detection," *International Journal of Computational Intelligence Systems*, vol. 17, Art. no. 236, 2024, doi: 10.1007/s44196-024-00644-z.
9. W. Ahmad, M. A. Raza, S. Nawaz, and F. Waqas, "Detection and Analysis of Active Attacks Using Honeypot," *International Journal of Computer Applications*, vol. 184, no. 50, pp. 27–31, 2023, doi: 10.5120/ijca2023922624.
10. M. Sridharan, S. Patil, T. Shobha, and P. Pai, "Hybrid Machine Learning-Based Intrusion Detection for Zero-Day Prevention," *International Journal of Safety and Security Engineering*, vol. 15, no. 8, pp. 1703–1713, 2025, doi: 10.18280/ijsse.150815.
11. S. Muhammad Rabiu, B. Khalid Aminu, and D. Aminu Zubairu, "AI-Driven Network Intrusion Detection Systems: Hybrid Models and Zero-Day Mitigation," *International*

Journal of Computer Applications, vol. 187, no. 8, pp. 27–33, 2025, doi: 10.5120/ijca2025925016.

12. S. Fuhrman, O. Gungor, and T. Rosing, "CND-IDS: Continual Novelty Detection for Intrusion Detection Systems," *arXiv preprint arXiv:2502.14094*, 2025.
13. L. Huang and Y. Wang, "Federated Learning for Zero-Day Attack Detection in 5G and V2X Networks," *arXiv preprint arXiv:2407.03070*, 2024.
14. D. Araujo-Filho, M. Naili, G. Kaddoum, and Z. Zhu, "Unsupervised GAN-Based Intrusion Detection System Using Temporal Convolutional Networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 1850–1863, 2023, doi: 10.1109/TNSM.2023.3241215.
15. Z. Dai, X. Li, and Y. Chen, "Zero-Day Attack Detection Using Machine Learning in Unseen Data Environments," *PLoS ONE*, vol. 19, no. 9, 2024, doi: 10.1371/journal.pone.0308469.
16. H. C. Altunay, "Analysis of Cyber Attacks Using Honeypot Systems," *Black Sea Journal of Engineering and Science*, vol. 7, no. 5, pp. 954–959, 2024, doi: 10.34248/bsengineering.1531420.
17. N. Gaddam, "AI-Enhanced Honeypots for Advanced Cyber Deception Strategies," *International Journal of Cyber Security Research and Development*, vol. 5, no. 1, pp. 9–19, 2025.
18. Y. T. Abewa and S. Z. Melese, "Dynamic Interactive Honeypot for Web Application Security," *International Journal of Wireless and Microwave Technologies*, vol. 14, no. 6, pp. 1–14, 2024, doi: 10.5815/ijwmt.2024.06.01.
19. A. Satpute, S. Nikam, V. Gaikwad, Y. Kakade, and C. Mhaske, "AI-Driven Intrusion Detection Using SSH Honeypots," *ICCK Transactions on Cybersecurity*, vol. 1, no. 1, pp. 3–12, 2025, doi: 10.62762/TC.2025.521799.
20. A. S. Almuflih et al., "Securing IoT Devices with Zero-Day Intrusion Detection Using Optimization and Attention-Based Classifiers," *Scientific Reports*, vol. 14, Art. no. 29238, 2024, doi: 10.1038/s41598-024-80255-y.
21. P. Lanka, K. Gupta, and C. Varol, "Intelligent Threat Detection Through AI-Driven Honeypot Data Analysis," *Electronics*, vol. 13, no. 13, Art. no. 2465, 2024, doi: 10.3390/electronics13132465.
22. Z. Azam, M. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems Using Machine Learning Models," *IEEE Access*, vol. 11, pp. 117812–117834, 2023, doi: 10.1109/ACCESS.2023.3326164.

23. F. R. Alzaabi and A. Mehmood, "Recent Advances in Insider Threat Detection Using Machine Learning Techniques," *IEEE Access*, vol. 12, pp. 43210–43225, 2024, doi: 10.1109/ACCESS.2024.3378901.
24. Y. Hou et al., "Semi-Supervised Learning with Mixup Decision Tree for Attack Traffic Classification," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2500–2513, 2022, doi: 10.1109/TDSC.2021.3060382.
25. D. Mezina and R. Burget, "Obfuscated Malware Detection Using Deep Convolutional Neural Networks," in *Proc. 14th Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2022, pp. 110–115, doi: 10.1109/ICUMT57764.2022.9943461.