Anusandhanvallari
Vol 2025, No.1
December 2025
ISSN 2229-3388

C3RBERUS – An AI Based Incident Response Agent for Cybersecurity

Dr. Usha G R[1], Umme Kulsum[2], Adarsh Kumar[2], Tejas M Banakar[2]
ushagr85@gmail.com, kulsum9237@gmail.com, kumaradarshh5@gmail.com, krshtejas@gmail.com
Associate Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India [1]

U.G Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India [2]

ABSTRACT

C3RBERUS-Cybersecurity 3-layered Response-Based Enhanced Resilient Unified Shield is a new generation AI-based incident response system tailored to enhance the security posture of Linux-based servers against sophisticated and evolving cyber threats. Traditional security tools often rely on reactive measures, detecting threats only after damage has begun. C3RBERUS addresses this gap by implementing a proactive, autonomous framework capable of identifying, analyzing, and responding to threats in real time. The system intelligently monitors SSH activity to detect brute-force attacks, verifies new IP addresses through automated email workflows, and redirects unverified access attempts to a controlled honeypot environment. It also continuously scans for ransomware-like behavior by analyzing process patterns and file system activities, instantly terminating malicious actions before data can be compromised. Additionally, C3RBERUS enforces strict access controls for sensitive files and logs every critical event, ensuring accountability and traceability.

KEYWORDS
Cybersecurity, SSH, brute-force attacks, ransomware, honeypot environment

1. Introduction

In today's world, as our dependence on interconnected systems grows, so does the sophistication and frequency of cyber threats. Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage. From ransomware and phishing to zero-day vulnerabilities and advanced persistent threats (APTs), modern attacks target not only infrastructure but also the integrity and availability of data. Traditional security methods, which largely rely on static rules and signature-based detection, are no longer sufficient to address these dynamic and evolving threats [1].

In this rapidly changing landscape, artificial intelligence and machine learning have emerged as powerful tools to enhance cybersecurity. These technologies enable the development of intelligent systems that can analyze vast amounts of data in real time, identify suspicious behavior, and make autonomous decisions [2]. The integration of AI into cybersecurity operations has significantly improved threat detection capabilities, with 58% of security professionals identifying improved threat detection as a key advantage of incorporating AI [3]. Modern AI-powered systems can process extensive data, recognize patterns and irregularities, and provide scalable and efficient means for early threat detection and automated incident responses [4].
The C3RBERUS project builds on this concept by combining real-time monitoring, threat detection, and automated response in a unified platform. It leverages AI to adapt to new threat patterns, while integrating additional security layers such as honeypots, Geo-IP mapping, and ransomware detection, providing a comprehensive approach to protecting digital environments. C3RBERUS-Cybersecurity 3-layered Response-

Based Enhanced Resilient Unified Shield is a new-generation, AI-driven incident response and server protection system engineered to safeguard Linux environments from the ground up.

At its core, C3RBERUS introduces an intelligent SSH access gateway fortified with an IP verification system. When an unknown IP attempts to connect via SSH, instead of being granted direct access, it is rerouted to a simulated honeypot—a fake shell environment designed to observe and contain potential threats [5]. Honeypots are computer security mechanisms set to detect, deflect, or counteract attempts at unauthorized use of information systems, providing a way to prevent and observe vulnerabilities in specific network systems [6]. Only upon verification via email does the IP gain access to the actual server, creating a highly effective first layer of defense against brute-force and unauthorized attempts.

By combining the precision of automation with the vigilance of artificial intelligence, C3RBERUS doesn't just respond to threats—it prevents them, contains them, and learns from them. It is not just a tool—it's a guardian engineered for the modern cyber battlefield.

2. Objectives

- To detect and respond to brute-force SSH attack patterns using IP behavior analysis and implement automated email verification as part of the incident handling process.
- To implement a honeypot environment for isolating unverified access attempts.
- To detect and terminate ransomware processes and unauthorized file access in real time.
- To generate and email PDF reports summarizing threat incidents for accountability and auditing.

3. Scope and Methodology

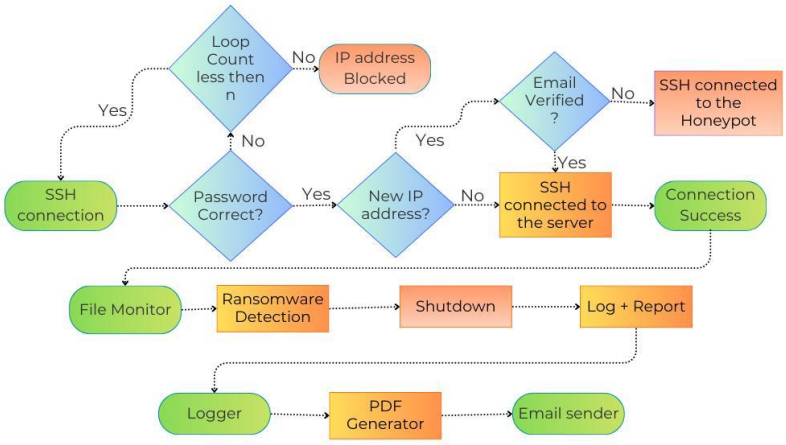

Fig 3.1:Flowchart diagram

The flowchart diagram of the C3RBERUS system visually represents the operational workflow of the cybersecurity framework, illustrating how different components interact to detect, analyze, and respond to security incidents. It provides a high-level overview of the entire system architecture—from initial log collection to final incident reporting—highlighting the logical progression of actions taken by the AI agents in real-time.

The flow begins with the real-time log aggregation module, where data is collected from various endpoints such as servers, network devices, and user activity logs. This data is passed through a log normalization and storage

layer to ensure consistency and accessibility for analysis. The core of the system, the threat detection engine, uses machine learning models to evaluate this data for anomalies, intrusion attempts, and ransomware behaviors. If a threat is identified, the system activates the SOAR (Security Orchestration, Automation, and Response) mechanism. SOAR technology helps coordinate, execute, and automate tasks between various security tools within a single platform, enabling organizations to quickly respond to cybersecurity attacks and observe, understand, and prevent future incidents [7]. The system executes predefined actions such as blocking IPs, locking user accounts, or notifying administrators, significantly reducing the time between detection and response [8].

4. Literature Review

Artificial Intelligence (AI) is revolutionizing the landscape of cybersecurity and emergency response by automating incident detection, response, and mitigation. The integration of AI-powered incident response transforms cybersecurity by enabling automated threat detection, improving incident response services, and streamlining incident response automation [9]. AI-driven systems can analyze vast amounts of data in real-time, detect anomalies, and respond to incidents with unmatched speed and accuracy—significantly reducing the impact of cyberattacks [10].

4.1. SSH Brute-Force Attack Detection

SSH brute-force attacks remain one of the predominant network attacks that pose distressing threats to network security. Hynek et al. (2020) presented a novel approach to detect SSH brute-force attacks in high-speed networks using machine learning, achieving high accuracy with low false-positive rates through specially extended IP flows [11]. Their work demonstrated that network-level detection approaches can overcome limitations of host-based methods that rely on system logs.

Wanjau et al. (2021) proposed an efficient mechanism for SSH brute-force network attack detection based on a supervised deep learning algorithm using Convolutional Neural Networks, achieving 94.3% accuracy with superior performance compared to traditional machine learning methods [12]. The study confirmed that deep learning algorithms, particularly CNNs, are effective alternatives to traditional firewall techniques for detecting and preventing these attacks.

Recent research by Satpute et al. (2025) proposed an intelligent intrusion detection system powered by SSH honeypots combined with machine learning, demonstrating robust detection rates across multiple attack vectors and offering dynamic adaptability to evolving threats [13]. The system bridges the gap between traditional signature-based systems and modern AI-driven security solutions.

4.2 Honeypot Technology and Deception

Honeypot technologies have become increasingly popular in cybersecurity as they offer valuable insights into adversary behavior with low rates of false detections [14]. By diverting the attention of potential attackers and siphoning off their resources, honeypots serve as powerful tools for protecting critical assets within networks.

Recent advances include AI-generated honeypots that learn and adapt in real-time. These systems use large language models to process attacker commands and generate realistic system responses, creating dynamic defense mechanisms that continuously evolve [15]. The integration of generative models, reinforcement learning, and advanced natural language processing enables these honeypots to simulate not only superficial characteristics but also nuanced behaviors and vulnerabilities of real systems [16].

Javadpari et al. (2024) provided a comprehensive survey on cyber deception techniques to improve honeypot performance, exploring various methods designed specifically to enhance deception while making honeypots

impervious to detection [17]. Their research highlighted the importance of maintaining high levels of deception as professional attackers continually work to uncover and bypass honeypots.

4.3 Ransomware Detection Using AI and Machine Learning

Ransomware attacks pose significant security threats to personal and corporate data. Al-Rimy et al. (2023) conducted a comprehensive survey on ransomware detection using machine learning, emphasizing that real-time behavioral analysis is the preferred approach for detecting and responding to attacks [18]. Their research demonstrated that machine learning-based detection methods can achieve high detection rates with low false-positive rates.

Ahmed et al. (2022) proposed a ransomware detection system using deep learning-based unsupervised feature extraction with a cost-sensitive Pareto Ensemble classifier, addressing the limitation of signature-based methods that are ineffective against zero-day attacks [19]. The system achieved superior performance by training weighted average ensembles on different features rather than relying on single classifiers.

Manavi and Hamzeh (2024) presented XRan, an explainable deep learning-based ransomware detector using dynamic analysis, demonstrating that low-level memory access patterns improved detection performance compared to detectors using only storage access patterns [20]. Recent studies confirm that dynamic analysis combined with machine learning enables detection of ransomware during execution, allowing for real-time intervention before encryption completes [21].

4.4 Security Orchestration, Automation, and Response (SOAR)

SOAR platforms have emerged as essential technologies for mature security functions, enabling organizations to collect inputs monitored by security operations teams and perform incident analysis and triage through a combination of human and machine intelligence [22]. These platforms help define, prioritize, and drive standardized incident response activities by integrating various security tools and automating repetitive tasks [23].

By automating routine tasks and orchestrating responses, SOAR helps organizations reduce mean time to detect (MTTD) and mean time to respond (MTTR), improving overall security posture [24]. AI-powered risk analysis within SOAR platforms can produce incident summaries for high-fidelity alerts and automate incident responses, accelerating alert investigations and triage by an average of 55% [25].

4.5 AI-Driven Cybersecurity and Incident Response

Hassan and Ibrahim (2023) illustrated AI's dual role in cybersecurity and incident response, demonstrating how AI not only detects threats but also autonomously orchestrates countermeasures [26]. Their work emphasized the importance of AI-driven automation in handling the overwhelming number of security alerts that modern security teams face daily.

Al-Mohannadi et al. (2025) presented research on enhancing cybersecurity incident response through AI-driven optimization for strengthened advanced persistent threat detection, proposing solutions to automate the incident response process and reduce manual intervention in post-alert decisions [27]. Their framework addressed two significant challenges: the generation of large amounts of alerts with huge rates of false positives and time-consuming manual expert engagement.

Collectively, these works illustrate a rapidly advancing field where AI not only augments human capabilities but often supersedes them in speed, accuracy, and scalability—making intelligent automation an indispensable pillar of modern cybersecurity and emergency response.

5. Result and Discussion

C3RBERUS-Cybersecurity 3-layered Response-Based Enhanced Resilient Unified Shield is an AI-powered cybersecurity platform designed to provide a comprehensive, real-time response to cyber threats. The system integrates multiple intelligent modules that work cohesively to detect, analyze, and mitigate attacks proactively.

Key components include a real-time log aggregation engine, which collects data from various sources, and a log normalization module that structures this data for efficient analysis. At the core lies a threat detection engine powered by machine learning algorithms trained to recognize suspicious patterns, anomalous behaviors, and known signatures of malware, including ransomware.
Upon detecting a threat, the system activates a dynamic alert and SOAR mechanism that can isolate affected systems, block malicious IPs, or disable compromised accounts without human intervention. Additionally, the system generates detailed incident reports and visualizes attack origins using Geo-IP mapping. Integration with honeypots enables the system to lure and study attackers, feeding valuable threat intelligence back into the AI engine. Together, these components make C3RBERUS a self-learning, adaptive defense framework capable of real-time threat prevention and response.

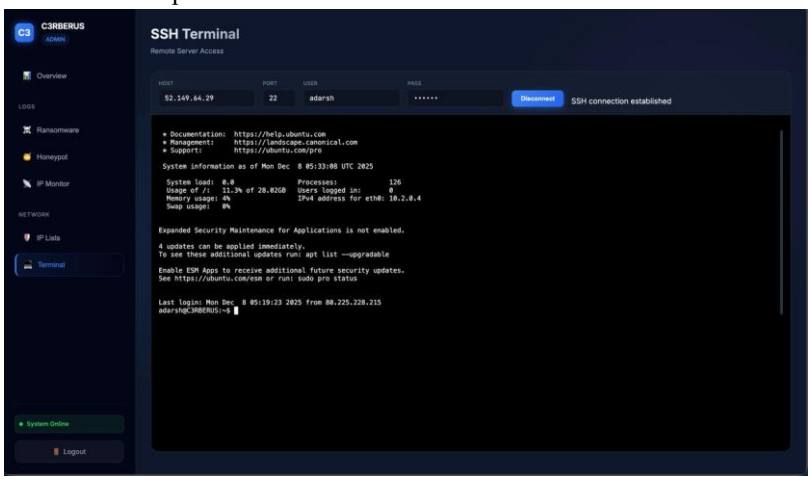

Fig 5.1:SSH web-terminal

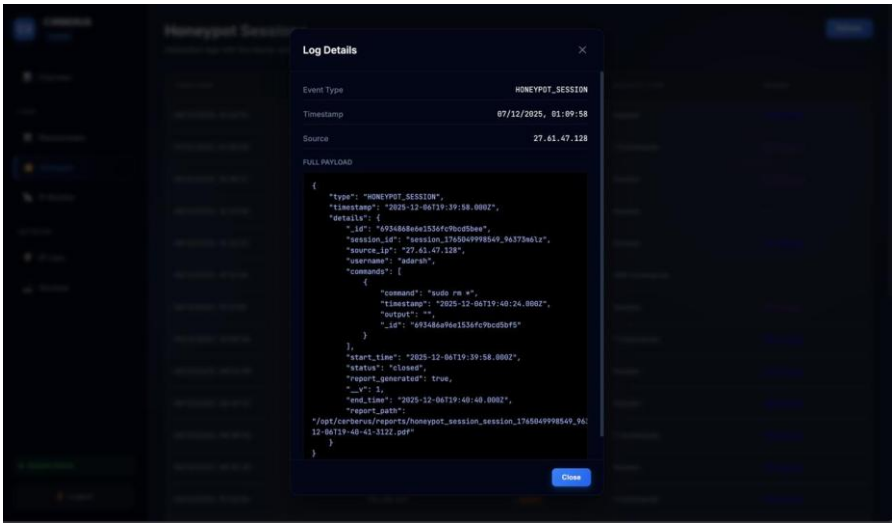

Fig 5.2 : HoneyPot Log

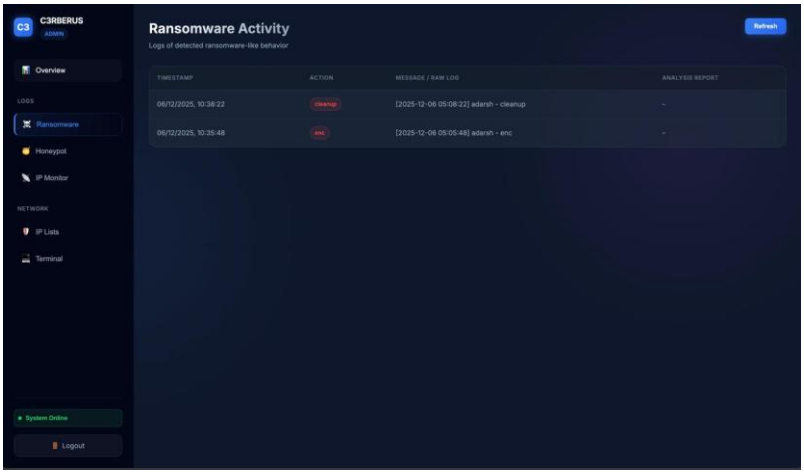

Fig 5.3:Ransomware Logs

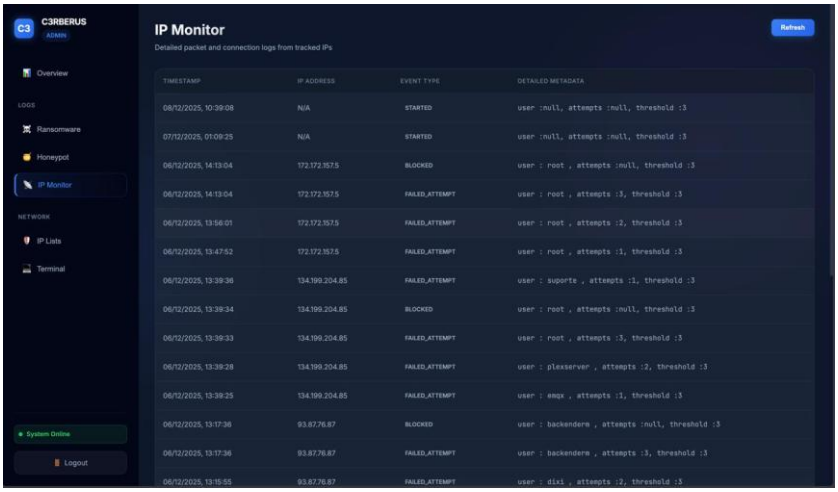

Fig 5.4 :IP Monitor

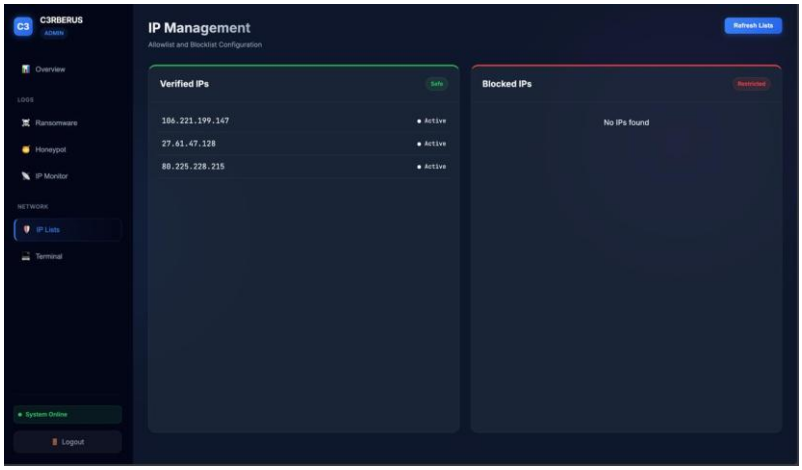

Fig 5.5: IP Lists

Fig 5.6: Dashboard

6. Findings

- The system effectively identified and blocked brute-force SSH attempts by monitoring failed logins and permanently banning malicious IPs.
- The honeypot mechanism successfully diverted unverified users, preventing direct access to the real server during initial connections.
- AI-generated command responses in the honeypot created a realistic fake SSH environment, making attacker detection highly accurate.
- The IP verification workflow ensured that only legitimate users bypassed the honeypot and gained access to the real server.
- The ransomware protection module reliably detected unauthorized file changes and initiated immediate system shutdown for damage control.
- Process and file monitoring components were able to identify unusual or malicious behaviors in real time.
- All security events—including blocked IPs, honeypot sessions, and ransomware alerts—were logged efficiently for auditing.
- AI-generated incident reports provided clear, automated summaries of suspicious activities, improving administrative response time.
- The dashboard maintained a clean record of verified and blocked IPs, enhancing visibility of system security status.
- Overall, the combined system provided layered security and significantly improved detection, analysis, and response to cyber threats.

7. Limitations and Research Gaps

The C3RBERUS system, while effective, has several limitations and research gaps that offer scope for further improvement. The IP-based blocking mechanism cannot fully prevent attacks originating from VPNs, proxies, or frequently changing IP addresses. The honeypot's dependency on AI-generated responses also introduces the possibility of inaccurate or incomplete command emulation in complex scenarios.

Additionally, the first-time user verification process may cause delays, and the ransomware protection module's immediate shutdown response, though safe, can disrupt ongoing services. The file-based tripwire detects tampering only in monitored files, leaving room for advanced ransomware techniques to bypass detection.
The system also lacks full filesystem monitoring, multi-server scalability, and automated threat correlation or long-term trend analysis. Furthermore, email-based alerting may not always ensure timely notifications during critical events. These gaps highlight the need for adaptive learning capabilities, broader monitoring coverage, and more advanced threat intelligence integration in future versions of the system.

8. Conclusion

C3RBERUS is a robust, modular, and proactive Linux incident response system designed to defend critical infrastructure against modern cyber threats. By combining behavioral monitoring, IP-level access control, honeypot deception techniques, and intelligent response automation, it offers a powerful line of defense—especially for cloud-based and remote Linux servers that are often exposed to brute-force attacks, unauthorized access, and ransomware payloads.

The system does not rely solely on traditional reactive methods but instead takes an intelligent and preventive approach. It ensures that only verified devices can access the real SSH environment, neutralizes ransomware threats in real-time before damage occurs, and restricts unauthorized attempts to access sensitive files.
In addition, detailed logs and auto-generated PDF incident reports provide transparency, accountability, and traceability of every event, empowering administrators and users to stay informed and alert. Overall, C3RBERUS brings together system security, automation, and observability under a single, extensible framework—offering a practical and customizable solution for modern-day Linux server protection.

References

[1] A. George, "Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis," *Partners Universal Innovative Research Publication*, vol. 2, no. 4, pp. 15-28, 2024.

[2] M. A. M. Farzaan et al., "AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments," *IEEE Transactions on Machine Learning in Communications and Networking*, 2025.
[3] Radiant Security, "What is AI-Driven Threat Detection and Response?" [Online]. Available: https://radiantsecurity.ai/learn/ai-driven-threat-detection-and-reponse/
[4] Palo Alto Networks, "What Is the Role of AI in Threat Detection?" [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection
[5] A. Satpute, S. Nikam, V. Gaikwad, Y. Kakade, and C. Mhaske, "AI-Driven Intrusion Detection System Using SSH Honeypots," *ICCK Transactions on Cybersecurity*, vol. 1, no. 1, pp. 3-12, 2025.
[6] Wikipedia, "Honeypot (computing)," [Online]. Available: https://en.wikipedia.org/wiki/Honeypot_(computing)
[7] Palo Alto Networks, "What Is SOAR?" [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-soar
[8] IBM, "What is SOAR (security orchestration, automation and response)," *IBM Think Topics*, 2024. [Online]. Available: https://www.ibm.com/think/topics/security-orchestration-automation-response
[9] Cyble, "AI-Powered Incident Response: Transforming Cybersecurity," May 2025. [Online]. Available: https://cyble.com/knowledge-hub/ai-powered-incident-response/
[10] Payoda Technology Inc., "AI for Cybersecurity: Threat Detection & Automated Incident Response,"

Medium, Apr. 2025.
[11] K. Hynek, T. Beneš, T. Čejka, and H. Kubátová, "Refined Detection of SSH Brute-Force Attackers Using Machine Learning," in *ICT Systems Security and Privacy Protection*, IFIP SEC 2020, vol. 580, Springer, Cham, 2020, pp. 63-77.
[12] K. Wanjau, D. Mbuvi, and P. Waiganjo, "SSH-Brute Force Attack Detection Model based on Deep Learning," *International Journal of Computer Applications Technology and Research*, vol. 10, no. 1, pp. 42-50, 2021.
[13] A. Satpute, S. Nikam, V. Gaikwad, Y. Kakade, and C. Mhaske, "AI-Driven Intrusion Detection System Using SSH Honeypots," *ICCK Transactions on Cybersecurity*, vol. 1, no. 1, pp. 3-12, 2025.
[14] A. Javadpari, F. Ja'fari, and T. Taleb, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, vol. 140, 2024.
[15] Cybersecurity Tribe, "AI-Generated Honeypots that Learn and Adapt," June 2025. [Online]. Available: https://www.cybersecuritytribe.com/articles/ai-generated-honeypots-that-learn-and-adapt
[16] Z. Morić, V. Dakić, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," *Informatics*, vol. 12, no. 1, p. 14, MDPI, 2025.
[17] A. Javadpari, F. Ja'fari, and T. Taleb, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, vol. 140, Mar. 2024.
[18] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware Detection Using Machine Learning: A Survey," *Applied Sciences*, vol. 7, no. 3, p. 143, Aug. 2023.
[19] Y. A. Ahmed, B. Koçer, S. Huda, B. A. S. Al-rimy, and T. Hassan, "Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier," *Scientific Reports*, vol. 12, Sep. 2022.
[20] F. Manavi and A. Hamzeh, "XRan: Explainable deep learning-based ransomware detection using dynamic analysis," *Computers & Security*, vol. 139, Jan. 2024.
[21] M. Al-Hawawreh, F. Den Hartog, and F. Sitnikova, "Ransomware Detection Using Dynamic Analysis and Machine Learning: A Survey and Research Directions," *Applied Sciences*, vol. 12, no. 1, p. 172, Dec. 2021.
[22] Gartner, "Definition of Security Orchestration, Automation and Response (SOAR)," *Gartner Information Technology Glossary*, 2024.
[23] Fortinet, "What Is SOAR? Security Orchestration, Automation, and Response," *Fortinet Cyberglossary*, 2024.
[24] IBM, "What is SOAR (security orchestration, automation and response)," *IBM Think Topics*, 2024.
[25] IBM Security, "Artificial Intelligence (AI) Cybersecurity," [Online]. Available: https://www.ibm.com/ai-cybersecurity
[26] S. K. Hassan and A. Ibrahim, "The role of artificial intelligence in cyber security and incident response," *International Journal for Electronic Crime Investigation*, vol. 7, no. 2, 2023.
[27] H. Al-Mohannadi et al., "Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection," *ScienceDirect*, Jan. 2025.