Innovative Security Practices Using Double Honeypots in Cyber Defence

Dr. Avijit Mondal
Assistant Professor, CSE,
Narula Institute of Technology, Kolkata
avijitmondaltmsl@gmail.com

Abstract

As cyber threats continue to evolve, traditional defense mechanisms often fail to provide necessary protection. This chapter explores the innovative concept of double honeypots, which is a layered approach to honeypot technology designed to enhance cybersecurity. By employing two honeypots—one for monitoring and the other for luring attackers—this method offers improved threat intelligence, better attacker diversion, and more proactive defense. This chapter examines the evolution of honeypot technology, architecture and principles of double honeypots, and their implementation in real-world systems. Case studies, including research by Palo Alto Networks, were presented to highlight the practical benefits and challenges of double honeypots. Additionally, the chapter discusses the integration of double honeypots with emerging technologies, such as AI and machine learning, offering a glimpse into the future of scalable and automated cybersecurity solutions. Despite challenges including complexity and false positives, double honeypots represent a promising advancement in defense strategies against increasingly sophisticated cyber threats.

Keywords: - Double Honeypots; Cybersecurity Threats; Advanced Honeypot Technology; Proactive Defense Strategies; Threat Intelligence and Analysis

1. Introduction

Double honeypots represent a significant advancement in cybersecurity practices, addressing the critical challenges posed by the increasing sophistication of cyberattack. Building on the foundational principles of honeypots introduced by Spitzner (2003), these systems employ a dual-layered approach to enhance the deception and data collection. Honeypots, in their traditional form, are decoy systems designed to mimic legitimate environments, luring attackers and allowing for the analysis of their methods. Over time, attackers have developed strategies for detecting and bypassing such systems, thereby diminishing their effectiveness. To counteract this, double honeypots integrate two layers of interaction: a primary honeypot to attract attackers, and a secondary layer to analyze more advanced techniques. This layered design not only increases engagement with attackers but also reduces the likelihood of the honeypot being identified as a decoy, thereby improving its efficacy (Provos and Holz 2007). The current cybersecurity landscape presents numerous challenges including zero-day vulnerabilities, advanced persistent threats, and increasingly sophisticated malware. These threats exploit the weaknesses of traditional security measures, necessitating innovative and adaptive solutions. Single honeypots, which are effective in capturing data on straightforward attacks, often fail to address complex and evasive threats. According to Javadpour et al. (2024), attackers leveraging modern tools and strategies can bypass single-layer honeypots, thereby reducing their utility. Double honeypots address these limitations by introducing a second layer of deception, allowing organizations to monitor advanced attacks in greater detail. This approach enhances threat intelligence and provides valuable insights into attacker behavior, tactics, and techniques. The evolution of honeypot technology has been marked by significant advancements from low-interaction systems designed for minimal engagement with high-interaction honeypots that provide attackers with fully functional environments. Low-interaction honeypots are effective at detecting and deterring basic attacks with minimal risk, whereas high-interaction systems allow for an in-depth analysis of complex threats, but require greater resources and management (Moric et al., 2024). By combining these approaches, the double honeypots strike a balance between resource efficiency and the ability to capture detailed threat data. The primary honeypot serves as the first line of engagement, distracting attackers and minimizing risk to critical systems, while the secondary honeypot offers a more sophisticated environment for studying advanced techniques. The importance of double honeypots in modern cybersecurity is underscored by their ability to address the limitations of the traditional systems. Paradise et al. (2017) emphasize that layered deception strategies improve the resilience of cybersecurity defenses by complicating the attacker’s efforts to detect and evade decoy systems. The dual-layer structure not only enhances detection capabilities, but also reduces false positives, as attackers engaging with the secondary honeypot are more likely to demonstrate malicious intent. This approach is particularly valuable in complex environments, such as industrial control systems, IoT networks, and critical infrastructures, where traditional security measures often fall short (Franco et al., 2021). Wang et al. (2020) further highlight the effectiveness of double honeypots in reducing detection risks and improving the overall security posture of organizations. By employing a dual-layered strategy, double honeypots offer a proactive and dynamic solution to the evolving cybersecurity challenges. Their ability to adapt to sophisticated threats, coupled with the insights they provide into attacker behavior, positions them as vital components of modern security frameworks. As cyber threats continue to evolve, the adoption of innovative approaches, such as double honeypots, is essential for maintaining robust and effective defenses.

2. Literature Review

The development of honeypot technology has played a pivotal role in advancing cybersecurity by providing detailed insights into the methods and behaviors of cyber attackers. Provos and Holz (2007) provided foundational knowledge on virtual honeypots, emphasizing their capability to mimic vulnerable systems and attract malicious actors. Spitzner (2003) classified honeypots into low- and high-interaction types, with low-interaction honeypots offering limited engagement to attackers, whereas high-interaction honeypots provide deeper interactions, thereby collecting more comprehensive data about attack strategies. This dual classification reflects the balance between the depth of interaction and operational complexity when designing effective honeypot systems.

Recent research has extended these concepts to specialized applications. For example, Franco et al. (2021) examined honeypots in the context of IoT, industrial IoT, and cyber-physical systems, identifying their effectiveness in capturing unique threat behaviors in these environments. Wang et al. (2020) highlighted the utility of honeypots tailored for IPv6 networks, addressing the specific vulnerabilities associated with newer network protocols. Javadpour et al. (2024) explored advancements in cyber deception techniques, showing how dynamic and adaptive honeypots enhance threat detection capabilities by responding to the evolving tactics of attackers. One notable evolution in this domain is the development of double honeypot frameworks that deploy multiple layers of honeypots to enhance deception and detection. Paradise et al. (2017) introduced social network honeypots as a novel approach for detecting targeted attacks in digital communication platforms. Moric et al. (2024) emphasized the importance of integrating layered honeypot systems, noting their ability to engage attackers at multiple stages, thereby increasing the likelihood of capturing sophisticated attack patterns.

Specific techniques, such as the shadow honeypots described by Anagnostakis et al. (2005), have demonstrated how dynamic environments can detect and analyze targeted attacks more effectively. Similarly, Zhu et al. (2024) proposed HoneyJudge, a framework focused on programmable logic controller (PLC) environments, underscoring the role of honeypots in securing industrial systems. Casey (2011) discussed the forensic applications of honeypots, highlighting their use in reconstructing attack sequences and providing critical evidence for cybercrime investigations. The integration of machine learning and behavioral analysis further enhances the effectiveness of honeypots.

Martínez Santander (2024) combined honeypot data with psychological surveys to detect attackers' personality traits, providing insights into their motivations and strategies. Paul and Mishra (2014) focused on the generation of signatures for polymorphic worms, demonstrating how honeypots can adapt to detect rapidly evolving malware. Yahyaoui and Rowe (2015) tested deceptive honeypot tools and illustrated how simple deception techniques can outmaneuver attackers and collect valuable intelligence.

Despite these advancements, several challenges remain to be overcome. Scalability and automation remain key issues because deploying large-scale honeypot networks requires significant resources. Ethical and legal concerns also present barriers to its broader adoption. Moric et al. (2024) and Paradise et al. (2017) highlighted the risks of inadvertently collecting sensitive data, necessitating careful design and compliance with data protection laws.

3. Honeypots and Double Honeypots in Cybersecurity

Honeypots are cybersecurity mechanisms designed to attract and deceive attackers by creating decoy systems that appear vulnerable or valuable, encouraging malicious activity. The primary goal of a honeypot is to study attack methodologies, gather intelligence, and improve network defense systems. Honeypots can be broadly classified into two types: low-interaction and high-interaction. Low-interaction honeypots simulate a limited set of vulnerabilities and functionalities, offering minimal risk but limited data on attack techniques. In contrast, high-interaction honeypots create a fully functional system with real operating systems and applications, posing a higher risk of compromise but providing detailed insights into attacker behavior and tactics (Provos & Holz, 2007; Spitzner, 2003).

Traditional honeypots have been widely used in cybersecurity to detect, track, and mitigate malicious activities such as botnets, DDoS attacks, and malware propagation. They function by acting as decoy systems that attract attackers, allowing security professionals to monitor and log malicious activities. While effective, traditional honeypots face limitations, such as scalability and resource demands. Deploying and maintaining a large number of honeypots across different environments is resource-intensive, and there is also the inherent risk that if a honeypot is compromised, it could provide attackers with valuable intelligence or a false sense of success, potentially making the system more vulnerable to future exploits (Moric et al., 2024). Furthermore, traditional honeypots often have limited capacity to capture and analyze the breadth of attack activities.

To overcome these limitations, the concept of double honeypots was introduced. Double honeypots use a layered defense approach, where two honeypots are deployed in sequence: one as a decoy to attract attackers and another to engage them further. This architecture is designed to enhance the ability to analyze attack methods and reduce the risk to real systems. The first honeypot serves as an exposed entry point to lure attackers, while the second honeypot is more isolated, designed to monitor attacker behavior in greater detail once they are engaged. This layered approach provides a more comprehensive view of attacker tactics, techniques, and procedures (TTPs) and helps to improve overall security posture (Javadpour et al., 2024).

Double honeypots offer several key advantages over traditional single honeypots. The enhanced threat analysis is one of the most significant benefits. With two honeypots in place, security teams can observe the full scope of an attack from the initial breach through to the deeper exploitation of the system, allowing for more detailed analysis and a better understanding of attacker motivations and tools. Moreover, the second honeypot can be designed to isolate attackers from critical systems, minimizing the potential impact of a compromised honeypot. By diverting attackers' attention from real systems to honeypots, this strategy helps to reduce the likelihood of a successful attack on actual valuable systems (Yahyaoui & Rowe, 2015). Additionally, double honeypots help mitigate the risk of a compromised system by ensuring that if one honeypot is breached, the second layer continues to track and engage the attacker without exposing the underlying infrastructure.

Furthermore, the deployment of double honeypots allows for a better diversion of attackers, which is crucial in environments where protecting sensitive data is paramount. As attackers focus their efforts on the decoy systems, the actual network infrastructure remains secure, with attackers unaware that they are interacting with controlled, isolated systems designed specifically for observation and analysis. This diversionary tactic improves the security of critical systems by providing security teams with valuable time to respond and mitigate any threats that may arise (Franco et al., 2021; Moric et al., 2024).

The architecture and deployment of double honeypots also offer significant advantages in terms of scalability and adaptability. While traditional honeypots may struggle to scale across large networks, double honeypots can be deployed in a more targeted and efficient manner. By layering the systems and directing attackers to specific points in the network, defenders can control and monitor malicious activity more effectively. This strategy also helps mitigate the computational load by reducing the resources needed to maintain multiple fully functional honeypots, making it more feasible to deploy on a larger scale (Zhu et al., 2024).

Despite these advantages, the use of double honeypots comes with its own challenges. One of the main concerns is the complexity involved in setting up and maintaining these systems. Double honeypots require careful configuration and constant monitoring to ensure they function as intended without introducing additional vulnerabilities. Furthermore, ethical and legal concerns arise when deploying honeypots, particularly regarding data collection and privacy. Organizations must ensure that their use of honeypots complies with legal Honeypots are cybersecurity mechanisms designed to attract and deceive attackers by creating decoy systems that appear vulnerable or valuable, thereby encouraging malicious activity. The primary goal of a honeypot is to study attack methodologies, gather intelligence, and improve network-defense systems. Honeypots can be broadly classified into two types: low and high interaction. Low-interaction honeypots simulate a limited set of vulnerabilities and functionalities, offering minimal risk but limited data on attack techniques. In contrast, high-interaction honeypots create a fully functional system with real operating systems and applications, posing a higher risk of compromise but providing detailed insights into attacker behavior and tactics (Provos & Holz, 2007; Spitzner, 2003). Traditional honeypots have been widely used in cybersecurity to detect, track, and mitigate malicious activities, such as botnets, DDoS attacks, and malware propagation. They function as decoy systems that attract attackers, allowing security professionals to monitor and log malicious activities. Traditional honeypots face limitations, such as scalability and resource demands. Deploying and maintaining a large number of honeypots across different environments is resource intensive, and there is also the inherent risk that if a honeypot is compromised, it could provide attackers with valuable intelligence or a false sense of success, potentially making the system more vulnerable to future exploits (Moric et al., 2024). Furthermore, traditional honeypots often have a limited capacity to capture and analyze the breadth of attack activities. To overcome these limitations, the concept of double honeypots has been introduced. Double honeypots use a layered defense approach, in which two honeypots are deployed in sequence: one as a decoy to attract attackers and the other to engage them further. This architecture was designed to enhance the ability to analyze attack methods and reduce the risk to real systems. The first honeypot serves as an exposed entry point to lure attackers, whereas the second honeypot is more isolated and designed to monitor attacker behavior in greater detail once they are engaged. This layered approach provides a more comprehensive view of attacker tactics, techniques, and procedures (TTPs) and helps improve the overall security posture (Javadpour et al., 2024). Double honeypots offer several advantages over traditional single honeypots. Enhanced threat analysis is one of the most significant benefits. With two honeypots in place, security teams can observe the full scope of an attack from the initial breach through to the deeper exploitation of the system, allowing for a more detailed analysis and better understanding of attacker motivations and tools. Moreover, the second honeypot can be designed to isolate attackers from critical systems, thereby minimizing the potential impact of a compromised honeypot. By diverting attackers' attention from real systems to honeypots, this strategy helps reduce the likelihood of a successful attack on actual valuable systems (Yahyaoui & Rowe, 2015). Additionally, double honeypots help mitigate the risk of a compromised system by ensuring that, if one honeypot is breached, the second layer continues to track and engage the attacker without exposing the underlying infrastructure. Furthermore, the deployment of double honeypots allows for better diversion of attackers, which is crucial in environments where protecting sensitive data is paramount. Because attackers focus their efforts on decoy systems, the actual network infrastructure remains secure, with attackers unaware that they are interacting with controlled, isolated systems designed specifically for observation and analysis. This diversionary tactic improves the security of critical systems by providing security teams with valuable time to respond and mitigate threats that may arise (Franco et al., 2021; Moric et al., 2024). The architecture and deployment of double honeypots offer significant advantages in terms of scalability and adaptability. Although traditional honeypots may struggle to scale across large networks, double honeypots can be deployed in a more targeted and efficient manner. By layering the systems and directing attackers to specific points in the network, defenders can control and monitor malicious activities more effectively. This strategy also helps mitigate the computational load by reducing the resources required to maintain multiple fully functional honeypots, making it more feasible to deploy on a larger scale (Zhu et al., 2024). Despite these advantages, the use of double honeypots remains challenging. One of the main concerns is the complexity involved in establishing and maintaining these systems. Double honeypots require careful configuration and constant monitoring to ensure that they function as intended, without introducing additional vulnerabilities. Furthermore, ethical and legal concerns arise when deploying honeypots, particularly with regard to data collection and privacy. Organizations must ensure that their use of honeypots complies with legal regulations, and that attackers' data are handled responsibly (Casey, 2011; Paul & Mishra, 2014). In summary, while traditional honeypots remain a valuable tool in cybersecurity, the deployment of double honeypots offers significant advantages, particularly in terms of enhancing threat analysis and diversions, and reducing the risk to critical systems. By employing a layered approach, double honeypots allow for a more nuanced understanding of attack methods, while providing additional layers of security to mitigate potential damage. However, challenges related to scalability, complexity, and legal concerns remain, necessitating careful consideration and planning when implementing such systems in real-world environments (Franco et al., 2024; Franco et al., 2021). regulations and that attackers' data is handled responsibly (Casey, 2011; Paul & Mishra, 2014).

In summary, while traditional honeypots remain a valuable tool in cybersecurity, the deployment of double honeypots offers significant advantages, particularly in terms of enhancing threat analysis, diversions, and reducing the risk to critical systems. By employing a layered approach, double honeypots allow for a more nuanced understanding of attack methods while providing additional layers of security to mitigate potential damage. However, challenges related to scalability, complexity, and legal concerns remain, necessitating careful consideration and planning when implementing such systems in real-world environments (Javadpour et al., 2024; Franco et al., 2021).

4. Implementation of Double Honeypots

The deployment of double honeypots introduces a layered approach to cybersecurity, enhancing threat detection and attacker diversion. Here is a concise breakdown of the design, integration, and configuration of double honeypots. System Design: Architecture for Deploying Double Honeypots Double honeypots consist of two layers: the decoy honeypot, which mimics vulnerable systems to attract attackers, and the trap honeypot, which captures detailed insights into the attacker's methods. The decoy honeypot is exposed to external networks, while the trap honeypot is isolated behind the decoy, ensuring that attackers are monitored without risking the actual systems. Network segmentation and real-time monitoring ensure that the system remains secure even if one honeypot is compromised (Franco et al., 2021). Integration with Existing Systems Double honeypots complement traditional security tools such as firewalls, IDS/IPS, and SIEM systems. Firewalls can control access to decoy honeypots, whereas IDS/IPS tools, such as Snort and Suricata, detect malicious traffic. When integrated with endpoint detection systems, double honeypots enhance overall threat visibility and response (Wang et al., 2020). They also help to identify new attack vectors and guide vulnerability management processes. Technology Stack: Tools, Frameworks, and Platforms · Snort/Suricata: Detects malicious traffic to and from honeypots. Docker: Facilitates isolated honeypot environments for easy scaling and deployment. · AWS: Provides scalable infrastructure for cloud-based honeypots. Honeyd/Dionaea: Simulated networks and captured exploit-targeting services. · Kippo: Emulates SSH servers to attract attackers that target weak credentials. Key Considerations for Effective Deployment · Decoy Honeypot Configuration: Simulate common vulnerabilities while filtering legitimate traffic. · Trap Honeypot Isolation: Place it behind strict isolation barriers (e.g., VLANs) to protect actual systems. · Monitoring and Response: Continuously monitor attack activity and respond to automated alerts. · Periodic Updates: Keep honeypots updated to reflect current attack trends. Ethical Considerations: Ensure compliance with privacy regulations and avoid unintended harm. By carefully designing, integrating, and configuring double honeypots, organizations can significantly improve their cybersecurity posture.

5. Case Study: Palo Alto Networks' Honeypot Research in Cybersecurity

Founded in 2005, the Palo Alto Network is a global leader in cybersecurity, specializing in next-generation firewall solutions, advanced threat prevention, and secure cloud services. The company is known for its innovative approach to network security and its commitment to providing cutting-edge tools that help organizations defend themselves against evolving cyber threats. With a focus on automation, AI-driven security, and real-time threat intelligence, Palo Alto Networks serve enterprises worldwide across multiple industries, including healthcare, finance, government, and critical infrastructure. A key element of the cybersecurity strategy of Palo Alto Networks is the use of honeypot —decoy systems to lure cybercriminals and gather intelligence on attack techniques. Honeypots are particularly valuable for detecting new and sophisticated threats that might evade traditional defenses. Palo Alto Networks deployed IoT honeynets to simulate vulnerable devices within military systems, enabling early detection and strategic defense mechanisms. According to Hanson et al. (2018), this IoT honeynet serves as both a deception tool and an early warning system, helping military organizations monitor and respond to cyber threats in real-time. The company also implemented scalable VPN-forwarded honeypots to track potential vulnerabilities in remote access systems, which are often targeted by cybercriminals. Aung et al. (2020) demonstrated that these honeypots, deployed in industrial control systems, provide critical insights into advanced persistent threats (APTs) targeting remote management platforms in sectors like energy, utilities, and healthcare. This study contributes to improving security by detecting and analyzing suspicious activities before they can cause damage. Palo Alto Networks' work with honeypots exemplifies its broader strategy of using innovative technologies to stay ahead of cyber threats. By using honeypots in various contexts, the company not only gathers threat intelligence, but also strengthens the security posture of organizations operating in critical sectors, such as banking, healthcare, and government.

6. Benefits and Challenges of Double Honeypot Implementation

Double honeypots, which utilize two decoy systems or services to mislead and track attackers, offer significant benefits in cybersecurity, but have several challenges. One of the key advantages is an increase in threat intelligence. By monitoring interactions with both honeypots, security teams can gain a better understanding of an attacker's tactics, techniques, and procedures (TTPs). This allows for a more refined approach to securing the systems. In addition, improved system deception is achieved because attackers are more likely to engage with decoy systems designed to mimic real operational environments. This misdirection helps identify and mitigate potential threats before they can affect actual systems (Franco et Holz, 2007; Franco et al., 2021). Double honeypots also contribute to a proactive defense strategy, providing cybersecurity teams with early warnings and insights into evolving threats. Rather than waiting for an attack to occur in a real system, defenders can simulate attack scenarios, evaluate the effectiveness of their defenses, enhance response strategies, and prevent potential breaches (Franco et al., 2021; Javadpour et al., 2024). This proactive stance is a key feature of modern cybersecurity systems, which rely on deception. However, deployment of double honeypots is challenging. However, complex implementation is one of the most significant hurdles. Establishing and managing multiple honeypots that interact seamlessly while maintaining the illusion of vulnerability can be technically demanding. Integration with existing security infrastructure requires careful planning and resources, particularly when considering real-time monitoring and incident response (Spitzner, 2003; Moric et al., 2024). Another challenge is the risk of false positive results. Legitimate traffic or non-malicious behavior can sometimes trigger alerts, leading to unnecessary investigations or even system disruptions. Managing these false positives is essential to ensure that resources are not wasted on irrelevant events (Yahyaoui and Rowe, 2015). Finally, legal and ethical considerations arise from the use of honeypots, especially when engaging with malicious actors. Although honeypots are designed to attract attackers, there are concerns regarding the ethical implications of allowing attackers to interact with fake systems. These concerns are heightened when dealing with sensitive data or potentially unlawful activities (Anagnostakis et al., 2017; Anagnostakis et al., 2005). In conclusion, while double honeypots offer valuable tools for enhancing cybersecurity through improved deception and threat intelligence, their complex implementation and associated risks must be carefully managed to avoid legal, ethical, and operational pitfalls.

7. Future Perspectives

The future of double honeypots in cybersecurity is closely linked to emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, which can greatly enhance the effectiveness and adaptability of these systems. Double honeypots have already been recognized for their ability to lure attackers into simulated environments in order to study their methods and techniques. Integrating AI and ML can take this step further by enabling real-time threat detection and automatic adaptation to evolving attack strategies. For instance, AI can analyze the behavior of attackers within honeypots, allowing the system to learn and adjust its responses accordingly. This proactive approach can significantly enhance the ability to identify and neutralize new types of threats before they escalate (Franco et al., 2021; Sangui & Ghosh, 2021). The scalability of double honeypots is also an important consideration for future development, particularly in the context of the Internet of Things (IoT) and cloud environments. As IoT networks continue to expand, they introduce new security challenges owing to the sheer volume and diversity of the connected devices. Double honeypots can be deployed to secure these networks by emulating different devices and tricking attackers to engage with decoy systems rather than a critical infrastructure (Franco et al., 2021). Similarly, cloud environments, which are highly dynamic and often involve complex infrastructure, would benefit from the scalability and flexibility of double honeypots. These systems can be designed to function in multi-cloud and hybrid environments, thereby providing enhanced security across diverse platforms (Alyas et al., 2022; Alkadi et al., 2020). Another promising avenue for the future is the automation of response mechanisms, based on data from double honeypots. Automation can help streamline the detection and response processes by instantly triggering alerts, isolating compromised systems, and deploying defensive measures when a suspicious activity is detected. By integrating AI-driven threat intelligence, automated systems can react more efficiently to emerging threats, reducing the time required to mitigate risks (Bartwal et al., 2022; Tabari & Ou, 2020). Moreover, automated systems can adapt to new attack techniques by analyzing behavioral patterns and modifying their tactics accordingly, making them more effective at countering advanced persistent threats (Lanka et al., 2024). In conclusion, the future of double honeypots is bright, with innovations in AI, scalability for IoT and cloud environments, and automation paving the way for more sophisticated and effective cyber-security solutions. These advancements will not only improve detection and response times, but also create more resilient systems capable of defending against increasingly complex cyber threats (Ng et al., 2018; Rabzelj et al., 2023).

8. Conclusion

Double honeypots offer promising advancements in cybersecurity by addressing the limitations of traditional honeypots. Using a layered approach, where one honeypot monitors while the other diverts attackers, double honeypots provide enhanced threat intelligence, improved deception, and a proactive defense strategy. Despite challenges such as complexity and potential false positives, their integration with emerging technologies such as AI and machine learning presents an exciting future for scalable and automated cybersecurity solutions. As cyber threats evolve, double honeypots can play a crucial role in strengthening defenses across diverse environments.

References

1. Alkadi, O., Moustafa, N., & Turnbull, B. (2020). A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. *IEEE Access*, *8*, 104893-104917.
2. Alyas, T., Alissa, K., Alqahtani, M., Faiz, T., Alsaif, S. A., Tabassum, N., & Naqvi, H. H. (2022). Multi-Cloud Integration Security Framework Using Honeypots. *Mobile Information Systems*, *2022*(1), 2600712.
3. Anagnostakis, K. G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E., & Keromytis, A. D. (2005). Detecting targeted attacks using shadow honeypots.
4. Aung, Y. L., Tiang, H. H., Wijaya, H., Ochoa, M., & Zhou, J. (2020). Scalable VPN-forwarded honeypots: Dataset and threat intelligence insights. Sixth Annual Industrial Control System Security Workshop, 21-30.
5. Bartwal, U., Mukhopadhyay, S., Negi, R., & Shukla, S. (2022, June). Security orchestration, automation, and response engine for deployment of behavioural honeypots. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (pp. 1-8). IEEE.
6. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.
7. Franco, J., Aris, A., Canberk, B., & Uluagac, A. S. (2021). A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. *IEEE Communications Surveys & Tutorials*, *23*(4), 2351-2383.
8. Hanson, P. J., Truax, L., & Saranchak, D. D. (2018). IoT honeynet for military deception and indications and warnings. Autonomous Systems: Sensors, Vehicles, Security, and the Internet of Everything, 10643, 296-306.
9. Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., & Benzaïd, C. (2024). A comprehensive survey on cyber deception techniques to improve honeypot performance. *Computers & Security*, 103792.
10. Lanka, P., Gupta, K., & Varol, C. (2024). Intelligent threat detection—AI-driven analysis of honeypot data to counter cyber threats. *Electronics*, *13*(13), 2465.
11. Malik, V., Khanna, A., & Sharma, N. (2024). Trends in Ransomware Attacks: Analysis and Future Predictions. *International Journal of Global Innovations and Solutions (IJGIS)*.
12. Martínez Santander, C. J. (2024). Learning models to detect personality traits of cyber attackers:

a combined approach using honeypot and surveys.

13. Moric, Z., Mršić, L., Kunić, Z., & Đambić, G. (2024). Honeypots in cybersecurity: their analysis, evaluation and importance.
14. Ng, C. K., Pan, L., & Xiang, Y. (2018). *Honeypot frameworks and their applications: a new framework*. Springer Singapore.
15. Paradise, A., Shabtai, A., Puzis, R., Elyashar, A., Elovici, Y., Roshandel, M., & Peylo, C. (2017). Creation and management of social network honeypots for detecting targeted cyber attacks. *IEEE transactions on computational social systems*, *4*(3), 65-79.
16. Paul, S., & Mishra, B. K. (2014). Honeypot-based signature generation for polymorphic worms. *International Journal of Security and Its Applications*, *8*(6), 101-114.
17. Piens, T. (2020). Mastering Palo Alto Networks: Deploy and manage industry-leading PAN-OS 10.x solutions to secure your users and infrastructure. Packt Publishing Ltd.
18. Provos, N., & Holz, T. (2007). *Virtual honeypots: from botnet tracking to intrusion detection*. Pearson Education.
19. Rabzelj, M., Južnič, L. Š., Volk, M., Kos, A., Kren, M., & Sedlar, U. (2023). Designing and evaluating a flexible and scalable HTTP honeypot platform: architecture, implementation, and applications. *Electronics*, *12*(16), 3480.
20. Sangui, S., & Ghosh, S. K. (2021). Cloud Security Using Honeypot Network and Blockchain: A Review. *Machine Learning Techniques and Analytics for Cloud Security*, 213-237.
21. Spitzner, L. (2003). Honeypots: tracking hackers [CD].
22. Wang, K., Tong, M., Yang, D., & Liu, Y. (2020). A web-based honeypot in IPv6 to enhance security. *Information*, *11*(9), 440.
23. Yahyaoui, A., & Rowe, N. C. (2015, May). Testing simple deceptive honeypot tools. In *Cyber Sensing 2015* (Vol. 9458, pp. 9-23). SPIE.
24. Zhu, H., Liu, M., Chen, B., Che, X., Cheng, P., & Deng, R. (2024). HoneyJudge: A PLC Honeypot Identification Framework Based on Device Memory Testing. *IEEE Transactions on Information Forensics and Security*.
25. Ziaie Tabari, A., & Ou, X. (2020, October). A multi-phased multi-faceted iot honeypot ecosystem. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2121-2123).