International Journal of
Human Computations & Intelligence
Vol. 03, Issue. 06, 2024

RESEARCH ARTICLE OPEN ACCESS

Emerging Trends in Honeypot Research: A Review of Applications and Techniques

Vishal Kumar . Sawan Bhardwaj . Pradeep Chouksey . Praveen Sadotra . Mayank Chopra

Department of Computer Science and Informatics, Central University of Himachal Pradesh

DOI: **10.5281/zenodo.14811718**
Received: 12 January 2025 / Revised: 26 January 2025 / Accepted: 01 February 2025
©Milestone Research Publications, Part of CLOCKSS archiving

Abstract — Honeypots are decoys in cybersecurity, where a system is set up to attract and monitor cyber intruders. These systems appear vulnerable but are isolated and monitored, emulating the entire real world, for example, databases or IOT devices. To gain insight into their tactics, attackers interact with these decoys. Security teams can fortify their defences by learning about these emerging threats. Honeypots are classified on the basis of interaction offered. A low-interaction honeypot will only record the most basic attacks. High-interaction honeypots, in contrast, allow attackers to be interacted with on a higher level, yielding more insight as to how they operate. By adopting this approach early, organizations can better understand how they might be targeted by potential attackers. Besides enabling the early detection of threats, they publish decoys that honeypots distract attackers away from actual systems. But they fail to catch all attacks, particularly those that do not engage the decoy. Honeypots must be kept current to remain effective against rapidly evolving threats.

Index Terms — Attacks, Cyber-security, Data Collection, Honeypots, Honey, Threat Detection

I. INTRODUCTION

Cyber threats are ever evolving and if we want to stay ahead in the competition then our cybersecurity defences should evolve too. There has been an increasing number of studies, both academic and practical, thereby highlighting the significance of honeypots. Decoy Systems are used to mislead the attacker on a network and help in detecting, deflecting, or analyzing malicious activity. [1] By luring attackers to a phony, vulnerable target, a honeypot offers valuable insight into the actions and tactics of cybercriminals. Honeypots establish a protected environment for malicious activities, serve as a diversion away from key systems and magnetize attackers to themselves. These details provide attackers with the opportunity to expose their tactics and motivation by simulating realistic systems, applications, or data. This data can enable a more effective incident response, make emergent threats visible, and help secure networks. [2] They help organizations anticipate and prepare for attacks before it happens. Organizations can minimize the damage of an ongoing cyber-attack by simulating/real time tracking of attacker behaviour.

This cyber-security approach involves continuously improving practices as well as pinpointing potential weaknesses. [3]Broadly, honeypots are classified into two types having low interaction and high interaction. Low-interaction honeypots provide automatic logging of the basic environment without providing attackers much control. As they are easy to deploy and maintain, these systems are appropriate for organizations with fewer resources. [4] Deep behaviour and good understanding of attacker gain can be provided with a high interaction honeypot where you are providing a complete environment to the attackers. This thus makes them mor risky, because any hackers could also use these as a jumping pad for further attacks. [5] This type of selection is necessary to keep honeypot deployments unnoticed by attackers. In addition to the data itself, an extensive examination of aggregated data — often supported by complex analytics platforms and machine-learning tools — is also required in order to identify valuable insights. However, a honeypot might also gather sensitive information - which introduces additional privacy and legal risks. With the rise of IoT and complex network layers, a honeypot is slowly becoming relevant in cyber security. In the modern world of business, using new technologies have become a necessity, be it for operational purposes or other complementary functions, and cybercriminals are adept at turning these towards their advantage. Honeypots allow to change security strategies dynamically when threats appear. Finally, it promotes knowledge sharing among cyber experts, with individual organizations benefiting from shared insights and experiences. [6]

II. KEY ASPECTS

a. Understanding Honeypots in Cybersecurity

A honeypot is a decoy system that does exactly that, it will lure, analyse and neutralise potential threats cybersecurity. By providing information on types and methods of attack, they may also draw attackers away from genuine targets. A honeypot is more appropriately classified into two categories: low-interaction or high-interaction. Low-interaction honeypots emulate basic services and are easier to deploy, but provide less granular information about involving attack methodologies than a high-interaction honeypot. Conversely, high-interaction honeypots offer greater insight into attacker behaviour, but require much higher resource requirements for operation. [7]

b. Honeypot Architecture

Honeypots are designed to intercept malignant activity, and well after that dissect it during various layers of the diagram. Low-interaction honeypots collect at a preliminary attack data easier and faster than high interaction honeypots, and they are suitable for organizations with limited resources. High interaction honeypots, on the other hand, let attackers work in depth and provide knowledge about exploitation tactics and persistence. However, it is important to exercise caution with these types of systems so that they neither become hijacked, nor misused. [8]

c. Honeypot Deployment

Deploying honeypots will require consideration of placement, visibility, and integration into existing security tools. Depending on the organization's threat model, a honeypot can be placed either inside of an organization's network segment or at the perimeter. This process of deploying honeypots involves faking the real systems that are being used (often fake account are created to attract attackers) and isolating other critical assets at the same time. In addition, honeypots are complementary to other security systems (IDS and SIEM) making them more effective in detecting malicious activity and responding to incidents. [9]

d. Honeypot Techniques and Technologies

Honeypots are decoys that help detect unauthorized access attempts and also identifying the tactics, techniques, and procedures of attackers. [4] Broadly, there are two categories of honeypots: these that save an organization's assets by misleading attackers and those that help monitor attacks with detailed information on how they conduct the attacks. Tools like Honeyed, Dionaea & Blastoff which could be used for the purpose of understanding the new threats by capturing malware samples

e. Deployment and Management

Before deploying and maintaining a honeypot, an organization will need to set the purpose of it gathering intelligence or redirecting attacks amongst others. To ensure that a honeypot is not compromising critical systems, it should be isolated and monitored continuously to provide actionable intelligence [6]. It is also important that legal considerations (alongside ethical ones) to manage compliance with privacy laws and avoid unintentional harm to non-malicious actors.

f. Purpose and Benefits

When an attack is performed, honeypots allow you to gain intelligence by analysing what the attackers do [6]With this information, it is possible to make more proactive defences as well as response protocols. For example, honeypots can act as a deterrence to attackers since the resources spent on tracing malignant behaviour makes it less lucrative target real systems.

III. METHODOLOGY

This review paper employs a systematic literature review methodology to provide summaries and analyses of honeypots, their usage as well as their efficacy in cybersecurity, especially concerning résumé ransomware and industrial control systems. This allows to get an overview over the current state of research, what gaps are still not covered and gives ideas on where to go next.

a. Literature Search and Selection criteria

The first stage of the review involves literature searching based on several academic databases which includes IEEE Xplore, Scopus and Google Scholar. Several search terms were used in this query, including "honeypots," "cybersecurity" and "ransomware," as well as phrases such as "industrial control systems" and "anomaly detection" and "AI in cybersecurity". All studies referred to in the review were published from 2018 to up to 2024, so as to keep relevance and contemporized. An inclusion criterion was formulated, as described in the following section, to identify the significant papers for review. These criteria included: ***Relevance:*** The topic of the paper must be honeypots, which if used with respect to cybersecurity, especially ransomware and industrial control systems. ***Peer-Reviewed:*** Only research explored in peer reviewed articles, conference papers and reputable journals. ***Methodological***

Rigor: Empirical methods, theoretical method, or a literature review Abstracts that focus solely on the value or need for further research.

b. Data Extraction and Analysis

We assessed each paper about its findings, conclusions and suggestions for further research. To ensure consistency of data extraction between reviews, we developed a standardized form as part of the review process.

- The extracted data included: Title and authors of study Authors conclusions or key finding Recommendations for future research Collected data was analysed using thematic analysis to find key themes, trends, and gaps in the literature. Studies were then classified according to thematic areas, including honeypots for ransomware detection or prevention measures; artificial intelligence and machine learning; and the integration of blockchain technology as a means of bolstering cybersecurity, among others
- Limitations: Although providing novel insights, this review should also be interpreted in the light of some limitations. Relying solely on published literature may mean missing out on relevant findings from industry reports and unpublished studies. Research on cybersecurity has become a very dynamic discipline which might render the findings less relevant in the future as more technologies and methods are developed, this is another possible justification. In summary, this systematic review has provided a comprehensive state of the art on honeypot research in cybersecurity, and can be used for further investigation.

IV. OBJECTIVE AND SIGNIFICANCE OF THIS REVIEW

a. Objectives

We review honeypots as part of the improvement of cybersecurity environments. Honeypots tightly monitored in terms of their behaviours can be used as the bait for cyber-attacks into confined, non-threatening systems to provide information on malicious intent and action to better plan detection processes or defences against future breaches. In this paper, we take a closer look at honeypots (including low- and high-interaction) and their usage in practical security environments [10] Finally, the honeypots abstraction can be investigated for its capacity to detect advanced persistent threats (e.g. zero-day vulnerabilities) based on specific case studies and their overall role in enhancing organizations security. Abstract: Honeypot has been a popular area of research in computer and network security for more than two decades, with an impressive number of diverse types used successfully by practitioners in the field as well. [4] [2]

b. Significance

In cybersecurity, the growing sophistication of cyber threats lays the demand for innovative defences like honeypots. Review of honeypots' efficiency and scope. By studying how attackers engage with these decoys, organizations gain invaluable insights into the changing threat landscape and can adapt their defences accordingly. Honeypots serve a dual purpose: they can proactively deter would-be intruders and reactively assist in incident response by providing a controlled environment for studying breaches [2]This will also provide insights into ethical and legal issues that are critical to an ongoing debate as to how, in fact, better cybersecurity practices can risk migration out of the shadowy Internet black market. [10]

V. LITERATURE REVIEW

A honeypot is a thing that attracts hackers, which gives team members up to steal data for example about bad behaviour and use it to improve the security against threats. [11] These honeypots have low interaction, which means that they provide only a little bit of engagement and therefore can collect some basic attack data. Although higher detail than low-interaction honeypots, these also consume more resources. Proactive action of cybersecurity can be done by placing a honeypot at any area in public or internal network and receiving threats from both external and internal hackers. [12]. How AI and ML are being used to improve analysis of data and identification of threats: klassischen Honeypot-Forschung. AI-driven honeypots help in speedier and accurate detection; they quickly identify attack patterns. High-Interaction Honeypots with Machine Learning It is possible to study a wide variety of details in attacks without putting production systems at risk by using high-interaction honeypots combined with machine learning. Honeypots simulate vulnerable services to lure attackers, and thus, can provide information on intrusion techniques, so they contribute to higher security protection of IT systems. [8]

TABLE 1: Summaries Review of Papers

Title	Key Findings	Conclusion	Future Work
“Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations” [10]	Ransomware causes financial/reputational harm; proactive defenses needed.	Urgent need for resilient strategies against ransomware	Focus on critical infrastructure and detection methods.
“IoT Honeypot Review” [2]	Types of honeypots, data collection, research benefits	Honeypots improve IoT security	Develop intelligent honeypot, further research, deploy in SCADA testbed.
“Enhanced honeypot security for intrusion detection and prevention systems using blockchain” [8]	Blockchain improves IDPS accuracy and response time, facilitates threat intelligence sharing.	Blockchain integration enhances cybersecurity, providing a strong framework for threat management.	Develop dynamic honeypots, integrate with incident response systems.
“How do honeypots fit within industrial control system security.” [4]	Honeypots are effective for detecting and mitigating ICS threats.	Honeypots are important for ICS security, need comprehensive surveys, integration with standards, and analysis of historical attacks	Data analysis, interactivity levels, mapping to Purdue model, legal implications research
“Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats”	AI-driven analysis of honeypot data is valuable, honeypots gather critical data, machine learning can	AI-driven analysis is valuable, improves detection speed and accuracy, integrates AI and machine	Model refinement, dataset expansion, real-time testing, organizational collaboration, integration of emerging

[6]	analyze data, and the proposed framework is scalable.	learning, need for ongoing research.	technologies, user behavior analysis, longitudinal studies.
“Observation of Human-Operated Accesses Using Remote Management Device Honeypot” [13]	Honeypot attracted human visitors, observed various manual operations, identified persistent visitors, challenges in determining visitor intentions, mixed visitor composition, limited impact of IoT search engines	Honeypot effective, visitors engaged in various operations, persistent visitors, challenges in distinguishing intentions, significant cyber attack risks	Clarifying visitor discovery, enhancing interaction mechanisms, longitudinal studies, expanding deployment, collaboration with security researchers
“Encountering Social Engineering Activities with a Novel Honeypot Mechanism” [5]	Proposes a novel honeypot mechanism to combat social engineering, integrates AI for better recognition and blocking, emphasizes user awareness and research gap in automated security mechanisms	Organizations are investing in anti-social engineering, current detection systems have limitations, proposed honeypot mechanism offers a promising solution, need for further research and testing	Testing and refining the honeypot in a production network, ongoing research to improve automated security measures, innovative strategies for adapting to new techniques
“Comparison of Strategies for Honeypot Deployment” [11]	Adaptive strategies, particularly LLR, were most effective. Static strategies less effective. Human adversaries adapt over time. Randomization makes attacks harder	Honeypots are essential in cybersecurity. Strategic deployment and adaptive defences are effective. Human adversaries adapt. Further research needed to understand long-term effectiveness and attacker adaptation.	Improving existing strategies, attack distribution for FTRL, introducing new strategies, evaluating against experienced adversaries, real-world testing.
“Exploring Honeypot as a Deception and Trigger Mechanism for Real-Time Attack Detection in Software-Defined Networking” [12]	Proposes a lightweight detection mechanism for probe attacks in SDN, integrates a honeypot and machine learning for detection, experimental results show high accuracy and low CPU load	Probe attacks are threatening in SDN, proposed mechanism is effective, future research needed for fingerprinting and traffic monitoring	Preventing honeypot fingerprinting, improving traffic monitoring, expanding dataset, integrating with other security mechanisms, and real-world testing.
“A Comparative Study of Unsupervised Anomaly Detection Techniques Using Honeypot Data” [3]	Emphasizes importance of unsupervised anomaly detection, criticizes past research, compares various unsupervised techniques, evaluation criteria include similarity measurements, training data size, overall performance, and time complexity	Underscores significance of unsupervised anomaly detection, criticizes past research, compares methods, offers practical guidelines	Expanding dataset, developing hybrid models, improving similarity measurements, addressing time complexity, adapting to emerging threats, incorporating user feedback, integrating with other security measures
“Honeyboost: Boosting Honeypot Performance with Data Fusion and Anomaly Detection” [1]	Effectively identifies anomalous nodes, uses horizontal and vertical anomaly detection, lower false positive rate, data	Emphasizes significance of Honeyboost, highlights innovative data fusion techniques, practical applications, and potential	exploring network science and graph theory, refining anomaly detection techniques, real-world testing, integration with

	fusion for improved accuracy, focuses on internal LAN traffic, unsupervised operation	for future advancements	other security solutions, analyzing user behavior
“DecoyPot: A Large Language Model-Driven Web API Honeypot for Realistic Attacker Engagement” [14]	Dynamic Honeypots: Shift to adaptive, high-interaction systems using AI and NLP for realistic threat engagement. Data Challenges: Large datasets complicate analysis; require robust logging.	AI-driven honeypots improve attacker detection and engagement but face data management issues. NLP enhances realism, aiding threat analysis. Ongoing research is key for adaptability.	Advanced Honeypots: Real-time, interactive systems for complex threats. Improved AI & NLP: For better detection and engagement. Future Research: Focus on scalable datasets and adaptability.
“Utilizing Virtualized Honeypots for Threat Hunting, Malware Analysis, and Reporting” [15]	Real-Time Threat Detection: Captures ransomware and attacker tactics using virtualized honeypots and SIEM. Education: Enhances student engagement in cybersecurity.	Virtualized honeypots with SIEM improve threat detection and offer educational benefits, supporting proactive cybersecurity.	Data Sharing: CSV datasets and VirusTotal uploads. Infrastructure: Patches, firewall updates, and containerization for scalability
“Honeypot Deployment: A Blockchain-Based Distributed Approach” [9]	Blockchain Security: Enhances resilience with secure storage, tamper-proof logging, and smart contracts. Effective Detection: Validated for threat mitigation	Blockchain honeypots improve cyber defense by ensuring data integrity and secure threat detection.	Automation: Expand smart contracts. Scalability: Optimize consensus. AI: Integrate for better detection. Compliance: Address regulatory needs.
“A comprehensive survey on cyber deception techniques to improve honeypot performance” [3]	Highlights effectiveness of deception in cybersecurity, proposes a honeynet model, identifies gaps for future honeypot advancements.	Surveys honeypot research, emphasizes deception for performance, offers insights for stronger network defenses.	Advanced techniques, real-time metrics, psychological impact on attackers, AI-driven automation, interdisciplinary collaboration, ethical guidelines.

VI. CONCLUSION

The honeypot has evolved to be an essential instrument of improving cyber defences throughout numerous fields including industrial control system and Internet of Things. With the help of these systems, you can track risks and thwart them — and defend against cyber attacks before they happen as well. Blockchain technology has come in handy to strengthen sectors like threat management and firm up integrity and security in honeypot frameworks. Its effectiveness regarding ICS security is more pronounced because detailed surveys on a honeypot and its standard compliance are critical. Honeypots allow organizations to analyse historical attack data, which can help reinforce defences against emerging threats. Moreover, artificial intelligence and machine learning featured honeypot systems help in increasing the speed and precision of detection but further research is needed to improve these technologies against ever-evolving technical cyber threat landscape. Although honeypots provide numerous advantages, they also come with a number of issues regarding their deployment. Cyber-attacks are one of the easiest modes of attack for organizations to conduct as they cannot determine between actual problems and persistent visitors in this new digital world. To fill in this gap found in conventional detection methods, requires a honeypot mechanism that is able to truly combat social engineering. With the evolution of human adversary strategies, we must remain judicious in our deployment of these systems but not at the cost of develop adaptive defences. A probe attacks against Software-Defined Networking with an emphasis on specialized instrumentation more focused around fingerprinting and traffic analysis. We additionally highlight the need of unsupervised anomaly detection and suggest a reconsideration of past research approaches towards actionable recommendations for deployment. Advanced concepts such as Honey boost, based on state of the art data fusion methods, show us how far can honeypot technology evolve.

REFERENCES

1. Kandanaarachchi, S., Ochiai, H., & Rao, A. (2022). Honeyboost: Boosting honeypot performance with data fusion and anomaly detection. *Expert Systems with Applications, 201*, 117073. https://doi.org/10.1016/j.eswa.2022.117073
2. Razali, M. F., Razali, M. N., Mansor, F. Z., Muruti, G., & Jamil, N. (2018). IoT honeypot: A review from researcher's perspective. *2018 IEEE Conference on Application, Information and Network Security (AINS)*. https://doi.org/10.1109/AINS.2018.8631457
3. Song, J., Takakura, H., Okabe, Y., Inoue, D., Eto, M., & Nakao, K. (2010). A comparative study of unsupervised anomaly detection techniques using honeypot data. *IEICE Transactions on Information and Systems, 93*, 2544–2554. https://doi.org/10.1587/transinf.E93.D.2544
4. Maesschalck, S., Giotsas, V., Green, B., & Race, N. (2022). Don't get stung, cover your ICS in honey: How do honeypots fit within industrial control system security? *Computers & Security, 114*, 102598. https://doi.org/10.1016/j.cose.2022.102598
5. Abualhija, M., Al-Shaf'i, N., Turab, N. M., & Hussein, A. (2023). Encountering social engineering activities with a novel honeypot mechanism. *International Journal of Electrical & Computer Engineering, 13*. https://doi.org/10.11591/ijece.v13i1
6. Lanka, P., Gupta, K., & Varol, C. (2024). Intelligent threat detection—AI-driven analysis of honeypot data to counter cyber threats. *Electronics, 13*, 2465. https://doi.org/10.3390/electronics13022465
7. 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*. https://doi.org/10.1016/j.cose.2024.103792
8. Maranco, M., et al. (2024). Enhanced honeypot security for intrusion detection and prevention systems using blockchain. *World Journal of Advanced Research and Reviews, 22*, 751–758.
9. Nishad, N., & Singh, R. (2024). Honeypot deployment: A blockchain-based distributed approach.
10. Muniandy, M., Ismail, N. A., Yahya, A., Al-Nahari, Y., & Yao, D. N. L. (2022). Evolution and impact of ransomware: Patterns, prevention, and recommendations for organizational resilience. *International Journal of Neural Computing and Applications, 34*, 12077–12096. https://doi.org/10.1007/s00521-021-06578-6
11. Brynielsson, J., Cohen, M., Hansen, P., Lavebrink, S., Lindström, M., & Tjörnhammar, E. (2023). Comparison of strategies for honeypot deployment. *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining.*
12. Khalid, H. Y., & Aldabagh, N. B. (2024). Exploring honeypot as a deception and trigger mechanism for real-time attack detection in software-defined networking. *International Journal of Computing and Digital Systems, 16*, 951–960. https://doi.org/10.12785/ijcds/1604951
13. Sasaki, T., Kawaguchi, M., Kumagai, T., Yoshioka, K., & Matsumoto, T. (2024). Observation of human-operated accesses using remote management device honeypot. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 107*, 291–305. https://doi.org/10.1587/transfun.107.291
14. Sezgin, A., & Boyacı, A. (2024). Decoypot: A large language model-driven web API honeypot for realistic attacker engagement. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5009535
15. Holbel, R., Yerby, J., & Smith, W. (2024). Utilizing virtualized honeypots for threat hunting, malware analysis, and reporting. *Issues in Information Systems, 25*, 265–278.