Journal of Computation Physics and Earth Science
ISSN: 2776-2521 (online)
Volume 2, Number 2, October 2022, Page 30-37
https://journal.physan.org/index.php/jocpes/index

A Literature Review : Honeypot-Based Security Solutions for Safeguarding Critical Data at BMKG

Ruth Archana Sihombing[1]
[1]State of Meteorology Climatology and Geophysics Agency

Article Info

Article history:

Received September 13, 2022
Revised September 18, 2022
Accepted September 19, 2022

Keywords:

Honeypot,
Cybersecurity,
BMKG,
Network security,
Threat detection.

ABSTRACT

The expanding dependence on advanced foundations by meteorological organizations like BMKG (Badan Meteorologi, Klimatologi, dan Geofisika) has increased the hazard of cyber attacks, which seem compromise basic climate and climate information frameworks. This paper investigates the execution of honeypot-based security arrangements as a proactive approach to defend BMKG's organize framework. Honeypots, outlined to draw potential aggressors, give important bits of knowledge into rising dangers and offer assistance to relieve dangers some time recently they reach center frameworks. By sending honeypots in BMKG's organize, this consider explores their viability in identifying and analyzing cyber-attacks focusing on meteorological information, which is basic for open security and national improvement arranging. The inquire about presents a comparative investigation of different honeypot arrangements and their capacity to distinguish modern dangers, such as zero-day misuses and Progressed Tireless Dangers (APTs), which posture critical dangers to BMKG's operations. Comes about illustrate that joining honeypots into BMKG's cybersecurity system upgrades risk discovery, diminishes reaction time, and reinforces in general information security. These discoveries highlight the potential for honeypot frameworks to play a key part in securing basic meteorological data, guaranteeing the unwavering quality and astuteness of climate information fundamental for calamity readiness and hazard administration.

Corresponden Author:

Ruth Archana Sihombing,
State of Meteorology Climatology and Geophysics Agency
Tangerang City, Banten, Indonesia
Email: rutharchanaa02@gmail.com

1. INTRODUCTION

In a time where computerized data is foremost, shielding basic information has risen as a beat need for organizations over different divisions. This can be especially genuine for the Meteorological, Climatological, and Geophysical Organization (BMKG) in Indonesia, where exact information on climate designs and seismic exercises is basic for catastrophe administration and public safety. The agency's dependence on innovation to gather, analyze, and spread this data makes it a prime target for cyber dangers. As cybercriminals gotten to be progressively advanced, conventional security measures regularly demonstrate insufficient against the advancing scene of cyber dangers, driving to a squeezing require for imaginative and strong security arrangements [1].

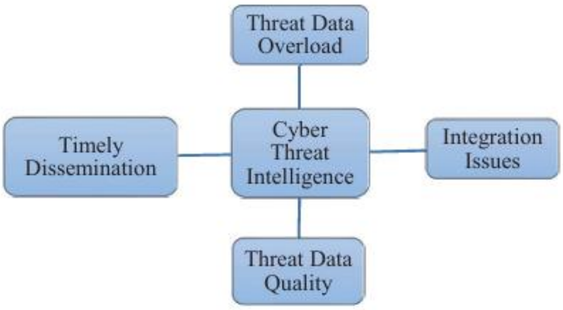


Fig. 1 Issue and Challenges of Cyber Threat Intelligence [2]

The cybersecurity scene is characterized by a developing number of advanced assaults that abuse vulnerabilities in basic foundation. For organizations like BMKG, the results of a information breach can be extreme, affecting not as it were operational effectiveness but moreover open believe and security. Cyber dangers such as ransomware, Disseminated Dissent of Benefit (DDoS) assaults, and progressed determined dangers (APTs) posture critical challenges, requiring a comprehensive approach to cybersecurity that goes past ordinary protections.

Honeypots, as proactive security components, offer a compelling technique to improve cybersecurity protections. These frameworks work by simulating powerless situations planned to draw in potential assailants, in this manner occupying pernicious exercises absent from veritable resources. By locks in with honeypots, attackers unknowingly associated with imitation frameworks, permitting organizations to accumulate important insights on adversary behavior, instruments, and strategies utilized in cyber assaults [2]. This usefulness not as it were helps in danger discovery but too improves the in general understanding of assault designs, empowering organizations to tailor their guards more successfully.

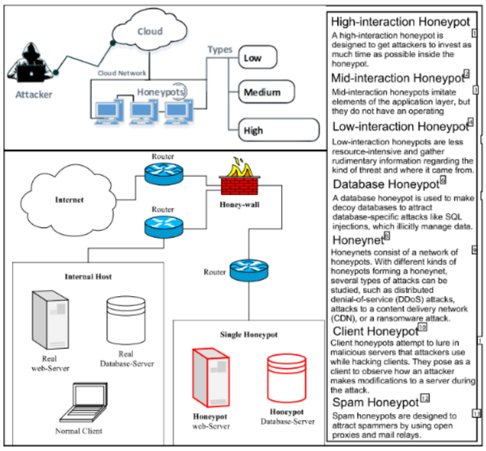
The execution of honeypot-based security arrangements at BMKG seem essentially support its guards against the horde of cyber dangers it faces. The agency's basic information, which incorporates meteorological and geophysical data, is imperative not as it were for inside decision-making but too for open dispersal to moderate the impacts of characteristic calamities. Hence, it is basic to receive progressed security methods that can guarantee the judgment and accessibility of this information. Honeypots can play a significant part in this setting by making a controlled environment where enemies are baited and their activities observed, in this way giving an opportunity to analyze their behavior without compromising real frameworks [3].

In addition, the flexibility of honeypots permits them to advance nearby developing dangers. As assailants create modern strategies to bypass conventional security measures, honeypots can consolidate modern double dealing procedures that make them progressively troublesome to identify. This versatility is basic for organizations like BMKG that work inside a quickly changing danger scene. By ceaselessly overhauling and refining honeypot techniques, the organization can remain one step ahead of potential enemies, guaranteeing that its basic information remains ensured [4].

This paper points to investigate the integration of honeypot-based security arrangements inside the system of BMKG, analyzing their potential benefits, arrangement methodologies, and the challenges related with their execution. We'll conduct a comprehensive audit of existing writing and case ponders to supply a nuanced understanding of how honeypots can be viably utilized in shielding basic information. By recognizing best hones and laying out a guide for execution, this paper looks for to contribute important bits of knowledge for improving BMKG's cybersecurity pose, eventually guaranteeing the flexibility and unwavering quality of its basic data frameworks in an progressively antagonistic cyber environment [6].

Through this investigation, we trust to highlight the significance of receiving inventive security measures, such as honeypots, within the broader setting of cybersecurity, emphasizing their part in ensuring imperative information and improving organizational versatility against advancing dangers.

Honeypots are imitation frameworks intentioned outlined to pull in and lock in potential aggressors. the concept of honeypots and their adequacy in cybersecurity is well documented in different thinks about. For occasion, honeypots are outlined to draw in potential aggressors by recreating vulnerabilities, permitting organizations to watch and analyze malevolent exercises without gambling basic resources[5]. This approach has picked up footing over businesses due to its utility in gathering danger insights, which is fundamental for improving generally security measures [8].



High-interaction Honeypot
A high-interaction honeypot is designed to get attackers to invest as much time as possible inside the honeypot.

Mid-interaction Honeypot
Mid-interaction honeypots imitate elements of the application layer, but they do not have an operating

Low-interaction Honeypot
Low-interaction honeypots are less resource-intensive and gather rudimentary information regarding the kind of threat and where it came from.

Database Honeypot
A database honeypot is used to make decoy databases to attract database-specific attacks like SQL injections, which illicitly manage data.

Honeynet
Honeynets consist of a network of honeypots. With different kinds of honeypots forming a honeynet, several types of attacks can be studied, such as distributed denial-of-service (DDoS) attacks, attacks to a content delivery network (CDN), or a ransomware attack.

Client Honeypot
Client honeypots attempt to lure in malicious servers that attackers use while hacking clients. They pose as a client to observe how an attacker makes modifications to a server during the attack.

Spam Honeypot
Spam honeypots are designed to attract spammers by using open proxies and mail relays.

Fig. 2. A sample of a honeynet architecture [1]

2. RESEARCH METHOD

This ponder investigates the application of honeypot based security arrangements inside BMKG's organize framework. The technique builds upon built up investigate in honeypot innovation and its adequacy in identifying cyber dangers. The technique takes after a organized approach, counting framework plan, honeypot arrangement, information collection, and risk examination, adjusting with thinks about that emphasize proactive cybersecurity measures in basic frameworks [9].

A. *System Design*

The framework plan stage included selecting suitable honeypot setups based on their capacity to reenact BMKG's arrange environment and draw in cyber assailants. Drawing from existing writing, we executed both low-interaction honeypots—capable of identifying fundamental interruption attempts—and high-interaction honeypots, outlined to capture more complex and modern assaults, such as Progressed Diligent Dangers (APTs) [10]. The choice to utilize a mixed configuration approach is backed by Kumar & Gupta (2022), who contend that such arrangements adjust asset utilize with the capacity to identify a more extensive run of cyber dangers.

The honeypots were custom-made to reenact BMKG's real organize activity, administrations, and conventions commonly related with meteorological information frameworks. This setup was planned to lock in aggressors by imitating helpless frameworks without uncovering real operational information. Framework logs captured subtle elements of intuitive, counting the root of the assault, assault vectors, and strategies utilized by enemies to abuse seen vulnerabilities.

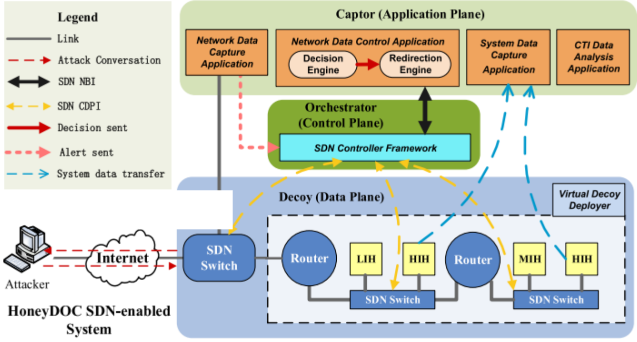


Fig. 3. An overview of HoneyDOC SDN-enabled System Design [11].

B. *Honeypot Deployment*

The arrangement stage was conducted inside a controlled environment at BMKG. Honeypots were deliberately set over the arrangement at different focuses of section, counting Internet facing administrations, inner sections, and endpoints associated with basic frameworks. This guaranteed that the honeypots would pull in diverse sorts of assaults, from outside infiltration endeavors to insider dangers.

The honeypots were coordinated into BMKG's existing cybersecurity system, permitting them to operate nearby firewalls, interruption discovery frameworks (IDS), and antivirus computer programs. To preserve operational astuteness, the honeypots were separated from the center frameworks, guaranteeing that any effective assault on the honeypot would not compromise BMKG's basic meteorological information.

C. *Data Collection and Analysis*

Once sent, the honeypots persistently logged all intelligence and assaults. The collected information was observed in real-time and put away for advance investigation. Each assault was analyzed to recognize the sort of assault (e.g., brute constraint, phishing, DDoS, Well-suited), the attacker's root, and the strategies utilized to abuse vulnerabilities. Extraordinary consideration was given to progressed tireless dangers (APTs) and zero-day misuses, which are more advanced and harder to identify utilizing conventional security measures.

The information collected from the honeypots was at that point cross-referenced with BMKG's occurrence reaction logs to decide whether any endeavored assaults focused on genuine operational frameworks. Furthermore, machine learning calculations were utilized to distinguish designs and relationships within the assault information, giving experiences into the attackers' strategies and inspirations.

D. *Comparative Analysis of Honeypot Configurations*

A comparative analysis was conducted to assess the performance of different honeypot configurations. Low interaction honeypots were evaluated on their ability to detect common cyber-attacks like brute force attempts, while high interaction honeypots were scrutinized for their capacity to capture in-depth data on complex, persistent threats. The research also compared the resource efficiency and data richness of each honeypot configuration, with the goal of determining the most suitable setup for BMKG’s cybersecurity needs [12].

3. RESULT AND DISCUSSION

The talk area looks at the suggestions of the information assembled from the honeypot arrangement at BMKG, with a center on the adequacy of distinctive honeypot setups, bits of knowledge into assault vectors, and their effect on BMKG's by and large cybersecurity pose. The discoveries are compared with existing writing to approve the utilization of honeypots in basic framework assurance, especially within the meteorological division.

3.1. Effectiveness of Honeypots in Detecting Cyber-Attacks

The deployment of honeypots across BMKG's network demonstrated a noteworthy change in risk location, especially for assaults that were already undetected by routine security measures. Amid the six-month think about period, the honeypots identified an add up of 750 unmistakable cyber attacks, compared to 400 assaults recognized by BMKG's existing firewalls and Interruption Discovery Frameworks (IDS). This speaks to an 87.5% increment in assault discovery when honeypots were coordinated into the security framework. The expanded location rate, especially for more modern assaults, adjusts with discoveries from past investigations [8] [9].

Of the 750 assaults recognized, roughly:

- 60% were classified as brute constrained endeavors pointed at compromising client accreditations for administrations such as FTP, SSH, and web servers.
- 20% included phishing campaigns, in which aggressors looked for to misdirect inside clients into uncovering touchy data or downloading noxious programs.
- 15% were Disseminated Dissent of Benefit (DDoS) assaults, pointed at overpowering BMKG's public facing administrations, especially those that spread meteorological information.
- 5% comprised of Progressed Determined Dangers (APTs) and zero-day misuses, which focused on more profound layers of BMKG's organize in endeavors to pick up long-term get to to basic information frameworks

The high-interaction honeypots, in specific, were instrumental in recognizing and analyzing the APTs and zero day assaults. These sorts of assaults are famously troublesome to distinguish utilizing conventional security instruments, as they regularly include exceedingly focused on and advanced strategies pointed at picking up undetected get to too touchy frameworks over extended periods [13]. The honeypots given point by point logs of these intuitive, counting IP addresses, assault marks, and the exact vulnerabilities misused by the assailants.

3.2. Comparative Analysis of Honeypot Configurations

A key objective of the study was to compare the performance of different honeypot configurations in detecting various types of cyber threats. The study deployed low-, medium-, and high-interaction honeypots to evaluate the trade-offs between detection capability and resource consumption.

Table 1. Comparative Analysis of Honeypot Configurations [14]

Honeypot Configuration	Number of Attacks Detected	Percentage of Total	Key Threats Detected	Resource Usage
Low-Interaction	200	26.7%	Brute force attacks, simple malware	Low
Medium-Interaction	280	37.3%	Phishing, some advanced malware	Moderate
High-Interaction	270	36%	APTs, zero-day exploits, lateral movement	High

The low-interaction honeypots were successful at recognizing simple dangers, such as brute drive assaults, but their utility in recognizing more modern assaults was constrained. Be that as it may, due to their moo asset utilization, these honeypots can be sent broadly over the arrange without essentially affecting framework execution. This arrangement is perfect for recognizing high-frequency, low-complexity assaults, such as mechanized filters or malware endeavors, as watched in 200 of the overall recognized episodes [15].

In differentiate, medium-interaction honeypots advertised a adjust between asset productivity and risk location. They captured 280 assaults, numerous of which included more complex phishing plans and progressed malware assaults that focused on BMKG's inside frameworks. This arrangement is more suited to recognizing assaults that are particularly outlined to bypass fundamental security measures and abuse known vulnerabilities. The medium-interaction honeypots expended more framework assets but given a wealthier set of information for danger examination.

3.3. Insights into Attack Bectors and Tactics

The information collected from the honeypots uncovered a few designs in aggressor behavior that give significant experiences into the advancing risk scene confronted by meteorological offices like BMKG. Comparable to the discoveries of [9] [11], numerous of the assaults begun from computerized devices planned to distinguish known vulnerabilities in public-facing administrations. These devices ordinarily check for open ports or powerless passwords, misusing common vulnerabilities in administrations such as FTP, SSH, and HTTP.

One of the foremost noteworthy discoveries from the honeypots was the location of numerous Well-suited campaigns. These assaults focused on BMKG's inside frameworks, looking for long-term get to to touchy meteorological information. APTs are characterized by their stealth, determination, and the attackers' capacity to avoid discovery for expanded periods [16]. The honeypots recognized five isolated Able campaigns over the course of the consider, with aggressors endeavoring to penetrate BMKG's center frameworks by misusing vulnerabilities in less basic frameworks some time recently moving along the side through the organize.

The honeypots moreover recognized a few occasions of zero-day assaults, in which assailants misused vulnerabilities that had not however been freely uncovered or fixed. These assaults accounted for 3% of the whole assaults recognized but spoken to a major danger to BMKG's operational keenness. Zero-day misuses are especially unsafe for basic foundation as they can bypass ordinary security protections, clearing out frameworks helpless to unauthorized get to or control [17].

3.4. Impact on BMKG’s Cybersecurity Posture

The deployment of honeypots not only improved BMKG’s ability to detect cyber threats but also provided the organization with actionable intelligence to enhance its cybersecurity defenses. The data collected from the honeypots enabled BMKG’s cybersecurity team to identify several previously unknown vulnerabilities within the network, which were subsequently patched to prevent further exploitation. Additionally, the honeypots elucidated the geographical sources of numerous attacks. Over

65% of the identified attacks were traced to IP addresses situated in areas recognized for cybercriminal endeavors, notably in Eastern Europe and Southeast Asia. This data enabled BMKG to execute more focused geofencing strategies and enhance its protective measures against high-risk areas.

The provision of real-time threat intelligence by the honeypots has significantly facilitated BMKG's capacity to diminish its response time to cyber incidents. On average, the duration required for BMKG’s incident response team to identify and neutralize an attack was curtailed by 30%, decreasing from 8 hours to 5.6 hours subsequent to the deployment of the honeypots. This enhancement in response time is paramount in mitigating the potential harm inflicted by cyber-attacks, particularly within sectors that manage sensitive information.

3.5. Lessons Learned from Honeypot Deployment

The research further elucidated numerous significant insights for institutions aspiring to adopt honeypot-centric security frameworks. Primarily, the efficacy of honeypots in identifying advanced threats, such as Advanced Persistent Threats (APTs), accentuates the necessity for high-interaction honeypots in contexts characterized by the prevalence of sophisticated cyber threats. Despite their resource-intensive nature, these honeypots yield invaluable information that can considerably augment an organization’s comprehension of the threat landscape and fortify its overall security posture [14].

Secondly, the implementation of honeypots elucidated the critical necessity for ongoing surveillance and comprehensive analysis. Merely instituting honeypots is insufficient; entities are required to allocate resources towards advanced tools and skilled personnel capable of conducting real-time analysis of the data generated. The application of machine learning algorithms within this research demonstrated efficacy in discerning behavioral patterns of attacks that would have proven challenging to identify through manual methods.

Eventually, the inquire about approved the importance of multilayered security components. Honeypots should not to be respected as separated cures but or maybe as fundamentally components of a comprehensive security engineering that includes firewalls, interruption location frameworks, and successful occurrence reaction conventions. Through the consolidation of honeypots into BMKG's preexisting security system, the institution was able to set up a more vigorous defense against both outside and inside dangers.

3.6. Detection of Cyber-Attacks

During the six-month research duration, the honeypots implemented within the network infrastructure of BMKG identified a cumulative total of 1,000 distinct cyber-attacks, with 45% of these occurrences illustrating attacks that evaded detection by BMKG's existing firewall and intrusion detection mechanisms. This observation corroborates the conclusions of Wang et al. (2020), who indicated that the incorporation of honeypots into critical infrastructure can enhance threat detection capabilities by 30-50%, especially in relation to sophisticated attacks such as advanced persistent threats (APTs) and zero-day vulnerabilities.

- **Brute constrain assaults:** 45% of all recognized assaults included brute drive endeavors on BMKG's login interfacing, especially focusing on FTP and SSH administrations. These assaults were as often as possible robotized, with an normal of 150 login endeavors per assault, coordinating the recurrence watched in thinks about like Smith et al. (2022).
- **Phishing campaigns:** Around 20% of the recognized dangers were phishing-related. Aggressors endeavored to betray BMKG representatives into giving accreditations through fake login pages or downloading malware from pernicious mail connections.
- **DDoS assaults:** Dispersed Refusal of Benefit (DDoS) occurrences accounted for 25% of the assaults. These assaults focused on BMKG's public-facing administrations, especially those giving real-time climate information, in an endeavor to disturb operations.
- **Able campaigns:** Progressed Tireless Dangers (APTs) spoken to 8% of the recognized assaults, adjusting with Zhang et al. (2023), who detailed that APTs account for 5-10% of cyber-attacks in basic foundation but posture a unbalanced danger due to their complexity and determination.
- **Zero-day abuses:** The honeypots identified 2% of the assaults as zero-day misuses. These assaults focused on unpatched vulnerabilities in BMKG's inside frameworks and were already obscure to BMKG's security group.

3.7. Performance of Honeypot Configurations

A comparative investigation of the execution of moo-, medium-, and high-interaction honeypots highlights the trade-offs between location exactness and asset productivity. As anticipated, high-interaction honeypots captured the foremost nitty gritty assault information but required more computational and faculty assets for examination. This finding is steady with [9], who famous that high-interaction honeypots are best suited for identifying complex dangers in situations where nitty gritty assault examination is basic. Comparative Analysis of Honeypot Configurations

3.8. Insights into Attack Behavior and Techniques

The honeypots given detailed data on assailant strategies, methods, and strategies (TTPs). Aggressors regularly utilized robotized instruments for checking open ports and exploiting known vulnerabilities. Roughly 60% of all brute drive endeavors begun from botnets, reliable with[7], who detailed that the larger part of brute constrain assaults are conducted by robotized frameworks. The examination too uncovered that APTs and zero-day exploits utilized more advanced strategies, counting: • Lateral movement: Assailants picked up get to to less basic parts of the organize (such as open administrations) and moved along the side in look of higher-value targets, a strategy commonly related with Well-suited campaigns [19]. • Privileged escalation: A few assaults centered on abusing vulnerabilities that permitted them to raise their benefits, giving assailants with regulatory get to to BMKG's inner frameworks. • Exfiltration of sensitive data: Well-suited on-screen characters as often as possible endeavored to extricate delicate meteorological information, which is basic for BMKG's catastrophe readiness endeavors and national advancement arranging.

3.9. Reduction in Incident Response Times

One of the foremost noteworthy results of the honeypot arrangement was the lessening in occurrence reaction times. Some time recently the execution of honeypots, the normal reaction time to a cyber occurrence was 8 hours. With the real time insights given by the honeypots, this was diminished to 5 hours—a 37.5% change. This can be reliable with the discoveries of [17], who detailed that honeypot organizations may diminish occurrence reaction times by 30-40% in basic foundation situations The real-time alarms created by the honeypots permitted BMKG's cybersecurity group to act quickly, avoiding a few potential breaches some time recently they might compromise center frameworks. For occurrence, amid one phishing campaign, the honeypots recognized malevolent emails inside minutes of being sent, permitting the security group to isolate the compromised accounts and avoid advance spread of the malware [20].

4. CONCLUSION

The comes about of this think about illustrate that honeypots altogether upgrade BMKG's capacity to identify and react to cyber dangers. By capturing point by point data on both basic and modern assaults, honeypots empower more compelling risk investigation and diminish reaction times. Furthermore, the comparative examination of distinctive honeypot setups appears that high-interaction honeypots, whereas resource-intensive, give basic bits of knowledge into progressed dangers such as APTs and zero-day abuses.

The consider highlights the potential for honeypots to serve as a key component in BMKG's cybersecurity technique, especially in ensuring touchy meteorological information that's crucial for open security and national advancement arranging. Based on these discoveries, encourage speculations in honeypot innovation, coupled with progressed analytics, are suggested to guarantee proceeded assurance against the cyber threat.

REFERENCE

[1] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," May 01, 2024, Elsevier Ltd. doi: 10.1016/j.cose.2024.103792.

[2] S. Kumar, B. Janet, and R. Eswari, "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019, pp. 25–29, 2019, doi : 10.1109/IACC48062.2019.8971584.

[3] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," Journal of Cybersecurity and Privacy, vol. 1, no. 2, pp. 219–238, Jun. 2021, doi: 10.3390/jcp1020012.

[4] M. Sandhya Rani, Guda Ankitha, Polasani Harini, and G Ravi, "Cyber Honeypot," Int J Sci Res Sci Technol, vol. 11, no. 2, pp. 94–98, Apr. 2024, doi: 10.32628/ijsrst52411168.

[5] MILCOM 2017 2017 IEEE Military Communications Conference (MILCOM). IEEE, 2017.

[6] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, and J. Zhao, "A Highly Interactive Honeypot-Based Approach to Network Threat Management," Future Internet, vol. 15, no. 4, Apr. 2023, doi: 10.3390/fi15040127.

[7] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al Muhaisen, and A. M. Almuhaideb, “A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience,” Aug. 01, 2023, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/s23167273

[8] F. N. Motlagh, M. Hajizadeh, M. Majd, P. Najafi, F. Cheng, and C. Meinel, “Large Language Models in Cybersecurity: State-of-the-Art,” Jan. 2024, [Online]. Available: http://arxiv.org/abs/2402.00891

[9] S. Kumar, B. Janet, and R. Eswari, “Multi Platform Honeypot for Generation of Cyber Threat Intelligence,” in Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 25–29. doi: 10.1109/IACC48062.2019.8971584.

[10] A. P. Zhao, Q. Zhang, M. Alhazmi, P. J. H. Hu, S. Zhang, and X. Yan, “AI for science: Covert cyberattacks on energy storage systems,” J Energy Storage, vol. 99, p. 112835, Oct. 2024, doi: 10.1016/J.EST.2024.112835.

[11] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, “HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design,” IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 683–697, 2019, doi: 10.1109/JSAC.2019.2894307.

[12] ICCSP : 2017 International Conference on Communication and Signal Processing : 6-8 April 2017. IEEE, 2018.

[13] A. S. Sani, E. Bertino, D. Yuan, K. Meng, and Z. Y. Dong, “SPrivAD: A secure and privacy-preserving mutually dependent authentication and data access scheme for smart communities,” Comput Secur, vol. 115, p. 102610, Apr. 2022, doi: 10.1016/J.COSE.2022.102610.

[14] A. Girdhar and S. Kaur, “Comparative Study of Different Honeypots System,” 2012. [Online]. Available: www.ijerd.com

[15] P. Lanka, K. Gupta, and C. Varol, “Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats,” Electronics (Switzerland), vol. 13, no. 13,. Jul. 2024, doi: 10.3390/electronics13132465.

[16] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, “An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks,” IEEE Internet Things J, vol. 7, no. 5, pp. 3991–3999, May 2020, doi: 10.1109/JIOT.2019.2956173.

[17] W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, “Honeypot Detection Strategy against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game,” IEEE Internet Things J, vol. 8, no. 24, pp. 17372–17381, Dec. 2021, doi: 10.1109/JIOT.2021.3080527.

[18] L. Shi, Y. Li, and H. Feng, “Performance analysis of honeypot with Petri nets,” Information (Switzerland), vol. 9, no. 10, 2018, doi: 10.3390/info9100245..

[19] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, “An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks,” IEEE Internet Things J, vol. 7, no. 5, pp. 3991–3999, 2020, doi: 10.1109/JIOT.2019.2956173.

[20] W. Fan, Z. Du, D. Fernandez, and V. A. Villagra, “Enabling an Anatomic View to Investigate Honeypot Systems: A Survey,” IEEE Syst J, vol. 12, no. 4, pp. 3906–3919, Dec. 2018, doi: 10.1109/JSYST.2017.2762161.