Using AI to Generate Dynamic Honeypots and Fake Data Trails to Confuse Attackers

Author Name: Gaurang Deshpande
Role: Software Developer
Affiliation: IBM, USA
Email: gaurangdeshpande89@gmail.com

Name: Deepak Singh
Role: Advisory Solution Architect
Affiliation: Gainwell Technologies, USA
Email: deepaksingh1981@gmail.com

Author Name: Sushant Suresh Jadhav
Role: Lead Product Software Engineer
Affiliation: WoltersKluwer, USA
Email: sushantjadhav21@gmail.com

***Abstract*- This study highlights how artificial intelligence, or AI, can be applied to cybersecurity using dynamic honeypots and auto-generating fake data trails. This seeks to decrease threat detection, misdirection of attackers, and collection of active action intelligence. Along with the concepts of machine learning, reinforcement learning, and secondary data collection and analysis techniques, the study establishes how AI can behave realistically in a system and respond in real time to the attacker's strategies. The outcome revealed that capturing rates and threat analysis cases have shown great improvement, as displayed in case studies, literature reviews, and experimental evaluations. The study also discusses applicability issues and suggests a scalable design along with recommendations such as collaboration between institutions. Moreover, it indicates the disruptive power of AI towards proactive, smart, and deception-based approaches to cybersecurity defence.**

***Index Terms*- AI, fake data trails, ML, dynamic honeypots, Cybersecurity**

I. INTRODUCTION

A. Background to the Study

A honeypot has been identified as a network-attached method set up as a decoy to lure cyberattacks and to help companies highlight, deflect, and investigate hacking attempts. Security risks in the cyber world are becoming increasingly advanced, demanding more active security measures. Fake data mimics the illusion of real data to an attacker [1]. Advanced persistent threats or APTs, and targeted attacks are often difficult to address with traditional security measures. On the other hand, static honeypots are proactively highlighted by professional adversaries. The use of Artificial Intelligence or AI offers a radical direction, the use of dynamic honeypots, constantly changing and leaving false and believable data traces. This not only deceives an attacker but also improves intelligence collection and makes AI a critical component of contemporary cybersecurity landscapes.

Doi:10.48047/ijiee.2023.13.4.15

B. Overview

This paper investigates AI algorithms based on which realistic system behaviours and user activities are simulated, which are challenging to track by opponents. In this paper, the concepts of incorporating AI into dynamic honeypots and the creation of deceptive data trails to trap operators of cyberattacks and analyse them are discussed. Additionally, honeypots are hosts masquerading as major systems in a subnet intended to deceive attackers [2]. This paper also assessed the degree to which these AI-driven mechanisms lead to better incident responses, threat attribution, and resilience of the system. The practical implementation strategies and the limitations, as well as the possible avenues in future research, are also mentioned to provide enough guidance to cybersecurity practitioners on the implementation of effective systems based on deception.

C. Problem Statement

The use of static honeypots and predefined fake data patterns was increasingly becoming obsolete as attackers have developed tools in order to detect them quickly and bypass them. On the other hand, Vollmer and Manic can be applied to develop dynamic virtual honeypots for observing and attracting network intruder activities [3]. The essence of the threat is that traditional deception systems are not flexible and realistic. The study fills that gap as it applies AI to develop dynamically intelligent honeypots and produce continuously changing simulated data trails. AI-based systems can learn about attacks, adapt, and imitate legitimate user sessions and data movements. Therefore, the paper introduces a new, adaptive defence layer that makes the reconnaissance of attacker's complex and prolongs the process of engagement and threat intelligence gathering.

D. Objectives

The primary goals of this study are: 1. To highlight AI-enabled dynamic honeypots that incorporate in real-time to reflect the behaviour of an authentic system and interactions from the users. 2. To identify automated fake data trail manufacturing processes that simulate practical data usage and system actions to create an illusion for the attackers. 3. To identify the impact of AI-oriented deception processes in highlighting, interpreting, and delaying cyber-oriented threats. 4. To highlight threats in applying AI-based deception processes and recommend models for incorporating AI-based honeypots in threat defence. These objectives aim to cultivate AI-based dynamic honeypots as well as fake data trail generation processes to improve defences in cybersecurity measures by increasing threat detection, misleading attackers, and collecting actionable intelligence.

E. Scope and Significance

This paper prioritises the creation and integration of AI-based dynamic honeypots and fake data trails as proactive cybersecurity deception equipment. This mitigates the algorithm design, behavioural simulation, system integration, and performance assessment throughout various attack scenarios. Additionally, AI-oriented methodology identifies phases of a host-level cyber-attack seamlessly from system call logs [4]. Thus, the significance of this paper lies in threat detection by being proactive in dealing with the attackers, keeping intrusions at bay, and capturing real intelligence. In solving these existing shortcomings of the static deception methods, the study provides a scalable, adaptive, and intelligent spoofing solution that strengthens organisational immunity against emergent cyber threats and offers its contribution to the wider body of knowledge in the area of AI-based cyber defence.

II. LITERATURE REVIEW

A. AI-enabled dynamic honeypots

Doi:10.48047/ijiee.2023.13.4.15

AI algorithms create practical and adaptive honeypots by highlighting natural language processing, machine learning, as well as generative AI to demonstrate real systems and communication, making them proactive in analysing and engaging attacks. Honeypots that dynamically simulate the actual behaviour of the system can be created with the help of AI in order to simulate the actual behaviour of the system based on the live traffic on the network or on the interactions with a human user. Additionally, "AI-augmented honeypots" act as a proactive threat deception strategy in cloud environments [5]. For example, ML models can be trained to simulate a normal operating system operation, any application logs, and user activity, thus adding to the plausibility of the honeypot.

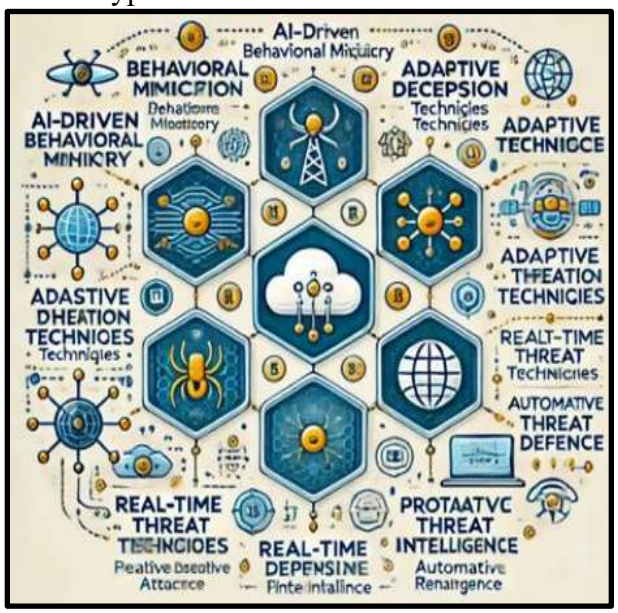

Figure 1: AI-Augmented Honeypot Framework

[5]

The adaptive systems can adjust their responses according to the behaviour of the attackers, making it much harder to detect and evade. The above figure has highlighted an overview of the "Augmented Honeypot Framework" for the cloud environment with attributes such as adaptive technology, automatic threat defence, and others [5]. Additionally, reinforcement learning has been suggested to keep on enhancing the honeypot approach to universalising the maximisation of involvement and miscommunication.

B. Detect automated fake data trail manufacturing processes

Fake data trail generation has become a highly relevant method in deception strategies in the cybersecurity domain that would mislead and perplex attackers in the system reconnaissance and exploitation stages. The customary fake data systems are based upon a fixed script or a dataset that can be quickly recognised by contemporary threats. With the advent of recent trends in the application of AI and machine learning, these data trails became more dynamic and realistic in that they could be automated and personalised. Honeypots uncover attack behaviour with longitudinal deployments in systems [6]. The generation of synthetic logs of user activity and access patterns using generative models such as GANs or "Generative Adversarial Networks" is capable of creating user activity logs and access patterns similar to legitimate user activity. This strives to the deployment of AI-powered fake data trail resolution systems to actively deceive the attacker and improve the overall cybersecurity status.

C. Effectiveness of AI-based deception systems

Cultivating the effect of AI-oriented deception processes is crucial to identifying integration in the real world to the defence system of cybersecurity measures. Most of the research has focused on the performance of such systems in identifying, analysing, and impending cyber threats. As an example, ML-based dynamic honeypots caused a drastic increase in the duration of engagement that attackers spent and better detection of early-stage intrusions. On the other hand, most of the dynamic honeypots can simulate the real system in time [7].

Doi:10.48047/ijiee.2023.13.4.15

Additionally, AI-enriched deception strategies can be in a position to investigate attacker behaviour profiles and extrapolate alerts that are more accurate than those of conventional systems. The incorporation of game theory in this regard describes the role of AI deception processes in transforming attacker initiatives by creating uncertainties in perceived threats and incentives, hence improving the potential of the system to decrease risk and enhance the results of the detection [8]. Furthermore, models based on reinforcement learning have been proven to achieve optimal response strategies so that the advance of the attackers is delayed, giving the defenders a greater duration to respond in time.

D. Challenges and Corrective Measures

There are various obstacles to implementing AI deception technologies, particularly in terms of obtaining scalability, reliability, and realism in different IT environments. This is quite computation-intensive, integration is challenging, and the deception mechanisms can be detected by adversaries. On the other hand, it is difficult to identify and anticipate an attempted fingerprinting attack due to the challenge of implementation [9]. The requirement to collect and train models to retain high levels of realism often impedes the scalability of large or heterogeneous networks. Moreover, it is essential to specify that the created behaviours and data cannot be distinguished from the lawful activity, which is technically challenging. The threat is finding the balance between system performance lightness, and flexibility, especially in the case of cloud-based or hybrid infrastructures. In their mitigation to manage such threats, experts can structure a method that assists in the modular and adaptive deployment of AI-driven honeypots. As an example, a layered architecture that embeds machine learning modules with currently available intrusion detection and response systems.

III. METHODOLOGY

A. Research Design

Research design refers to the overall initiative and framework applied to conduct research and collect data to answer research questions and hypotheses. Thus, to cultivate AI-based dynamic honeypots as well as fake data trail generation processes to improve defences in cybersecurity measures, "***explanatory research design***" has been taken into consideration. Explanatory design is a two-stage which includes quantitative data being used as the basis on which to create and describe qualitative data [10]. This type of design assists in achieving the research aim and objectives by identifying cause-and-effect relationships amid AI-driven deception technologies and effectiveness in cybersecurity. This leads to a structured assessment of the effect of dynamic honeypots and synthetic data trails on the behaviour of attackers, the certainty of detection, and the delay of threats.

B. Data Collection

This study employs a multi-methods research approach, incorporating both ***secondary quantitative and qualitative data collection and analysis techniques.*** Secondary data is used as supporting data to complete the interpretations in research [11]. Data sources used for the secondary qualitative research are journal articles, case study examples, and industry reports. On the other hand, statistical charts, graphs, and metrics are collected and further interpreted in a secondary quantitative method. These data collection and analysis methods improve study reliability and validity by creating extensive and cross-verified outcomes, specifying a balanced explanation with the help of trustworthy sources of data.

C. Case Studies/Examples

Case Study 1: Splunk's DECEIVE Proof-of-Concept

Splunk developed and released DECEIVE, an AI-based honeypot capable of modelling a

Doi:10.48047/ijiee.2023.13.4.15

realistic luxury SSH Linux environment with the help of a language model [12]. This is a dynamic generator of the system behaviour and summarises the commands of attackers, which improves detection processes.

Case Study 2: Forescout's AI-Crafted Ransomware Trap

Forescout brought online an AI-created corporate personality, including a website and network infrastructure that were designed to entice bad actors [13]. Successful deception was demonstrated as the honeypot had managed to attract Phobos ransomware operators through the open RDP.

Case Study 3: Trend Micro's Smart Factory Honeypot

Trend Micro set up a smart factory industrial control system honeypot, which captured real-world attacks several months them, such as ransomware. After that, they created a "cover company" for a faux factory and a client base for large anonymous companies from major sectors [14].

D. Evaluation Metrics

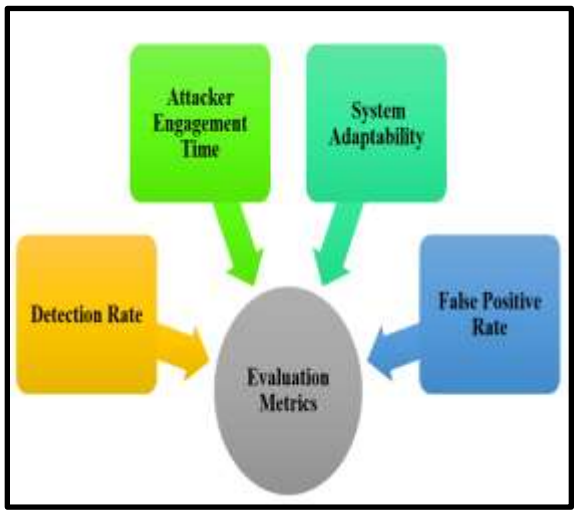

Figure 2: Evaluation Metrics

[Source: Self-Created]

As per the above figure, detection rate, attacker engagement time, system adaptability, and false positive rate have been identified as evaluation metrics of this paper. These research-based evaluation metrics have been assessing the efficacy of AI-based deception in a practical context, encouraging the findings by supporting its success factors in decreasing threats, enhancing accuracy, and highlighting applicability in cybersecurity landscapes.

IV. RESULTS

A. Data Presentation

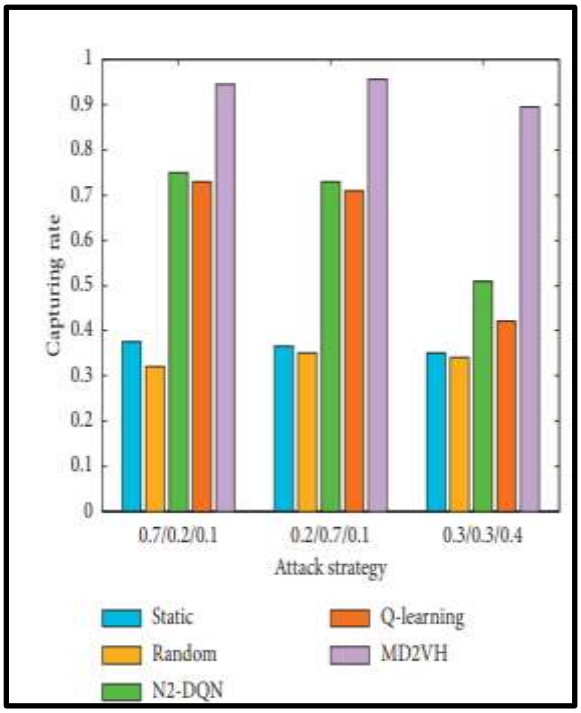

Figure 3: Probability of attacks being captured

[15]

The bar graph illustrates how each of the honeypot deployment strategies captures the different honeypots at different attack strategies: Static, Random, Q-learning, N2-DQN, and MD2VH. MD2VH always produces the most significant capture rate (around 0.9), which shows improved efficiency [15]. The Static and Random strategies fail to work, and this shows that the strategies fail to address dynamic threats.

Doi:10.48047/ijiee.2023.13.4.15

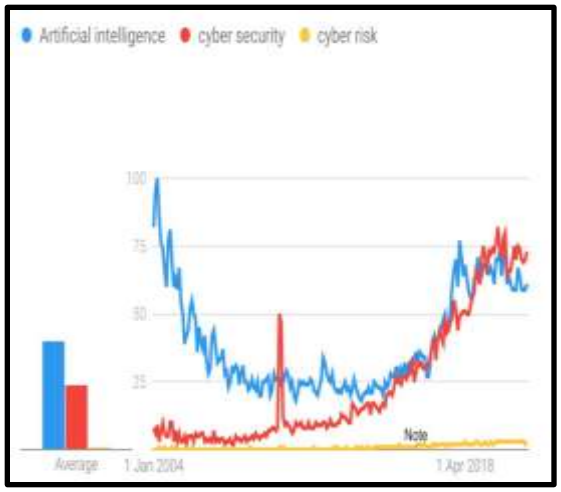

Figure 4: AI, Cybersecurity, and Cyber risk

[16]

Figure 4 shows how Artificial Intelligence, Cybersecurity, and Cyber Risk have evolved and looked since 2004. This indicates that people started to show a significant interest in AI and Cybersecurity after 2015, which shows global awareness and concern [16]. Cyber Risk stays in the lower range, indicating that it is not covered much in the public domain, although its importance in security planning has been increasing.

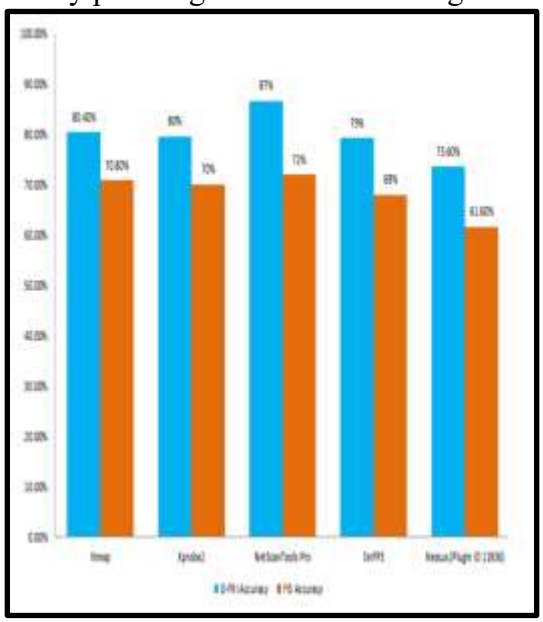

Figure 5: Prediction Accuracy of D-FRI-Honeypot

[9]

Figure 5 shows the accuracy of the prediction of the D-FRI Honeypot and that of FIS-only in a range of five scanning tools. D-FRI has always shown a better result than FIS, with the best accuracy of 87% when it uses NetScanTools Pro [9]. Additionally, D-FRI is extended to build a cognizant honeypot for detecting active fingerprinting attacks [17]. This shows the better level of threat detection and classification of D-FRI.

B. Findings

Figure 3 shows the high competency of "AI-supported dynamic deployment" (MD2VH) in terms of being more adaptive and effective in efficiency regarding capturing the attacker as compared to its traditional counterparts [15]. This establishes that intelligent learning-based schemes, especially reinforcement-based strategies such as MD2VH, fare better in being adaptable to the behavior of attackers and enhancing cybersecurity protection in general. As per Figure 4, the recent upsurge in interest in both AI and Cybersecurity shows them as a growing area in online safety [16]. The tendency verifies the necessity of AI-based cybersecurity innovations such as dynamic honeypots and data deception. Lastly, the detection accuracy of D-FRI-enhanced honeypots is superior to that of a FIS alone, which proves that AI can be effective in enhancing the analysis of threats [9].

C. Case Study Outcomes

Case Study Name	Company	Case Study Outcome	Relevance to Current Study
DECEIVE AI Honeypot	Splunk	Created SSH honeypots with the help of AI to highlight	This case study example has highlighted the role of AI in

Doi:10.48047/ijiee.2023.13.4.15

		real systems and interpret the inputs of the attacks [12].	improving realism in honeypots for higher detection and behavioural interpretation.
Ransomware Trap with Fake Identity	Forescout	Actors of "lured real ransomware" used AI-based infrastructure and monitored their actions [13].	Highlights the impact of fake data trails in attacks and the collection of intelligence.
Smart Factory Honeypot	Trend Micro	Accounted for several attacks in a real-world context with the help of a "fabricated ICS environment" [14].	This case study example supports detection through AI in major infrastructures and leads to scalability in various circumstances.

Table 1: Case Study Outcome
[Source: Self-Created]

The above case study instances highlighted the impact of AI-based deception in extensive circumstances, from SSH servers to industrial standards.

D. Comparative Analysis

Author	Aim	Findings	Gaps identified
[5]	This paper aims to identify the contribution of AI-based Honeypots to the cloud environment.	AI-augmented honeypots create a proactive defence, adapting to new attack vectors and generating actionable intelligence to improve cloud security [5].	Lack of primary and in-depth research
[6]	This article aims to propose a "new framework for the development and deployment of honeypots for evolving malware threats."	A "honeypot for automated and repetitive malware" (HARM) can be adaptive so that the best responses may be learned during its interaction with attack sequences [6].	Lack of mitigations discussed for certain limitations of Honeypots.

Doi:10.48047/ijiee.2023.13.4.15

[7]	This paper aims to explore the nature of a "Dynamic Distributed Honeypot."	Honeypot technology can be integrated to attract attackers efficiently and exhaust their resources [7].	Lack of theoretical discussion.
[9]	This paper aims to identify the role of "D-FRI-Honeypot."	Honeypots are commonly used as a decoy to inspect attackers and their attack tactics to improve the cybersecurity infrastructure [9].	Theoretical gap

Table 2: Comparative Analysis of Literature Review Sources

[Source: Self-Created]

This comparative analysis helps to fulfil research aims and objectives by identifying gaps, trends, and strategies, specifying refined knowledge of the future of AI to generate dynamic honeypots and fake data trails.

V. DISCUSSION

A. Interpretation of Results

Both qualitative and quantitative research have been conducted to fulfil the parameters of the research objectives. The first objective is achieved by the high capture rates of MD2VH, which justifies the honeypots based on real-time and AI. The second RO is fulfilled with case studies such as Forescout, where a fake data trail was successfully implemented in order to deceive the attackers. The context in which D-FRI improves the accuracy of prediction literature presents delayed and analysed threats referred to as objective 3. The last objective deals with deployment obstacles observed in literature and deployment of the system in practice, such as Splunk DECEIVE. Cumulatively, these aspects show that AI-based deception increases the number of detected initiatives, delays the time of attacks, and offers practical knowledge, as suggested in the research overall of what cybersecurity defence is to achieve.

B. Practical Implications

This paper creates a "forward-looking cybersecurity" context by applying AI to create major honeypots as well as fake data trails, improving delays, threat detection, and the capabilities of analysis. This allows companies to actively mislead and analyse attackers and acquire meaningful threat intelligence, all the time securing the most important resources. These AI-enabled systems highlighted in this paper could be customised in diverse IT environments and therefore could be of value in industrial networks, enterprises, and even government systems [18]. Additionally, the outcome is compatible with the prevailing security tools and thus helps to create smarter, stronger, and more proactive defense responses in the current era of fast-evolving cyber threats.

C. Challenges and Limitations

The study includes certain limitations, including limited processing resources that are required to accommodate real-time AI processing and the need to sustain believability in dynamically changing deception. The presence of heterogeneity also makes scalability more complex, and the integration of legacy systems can be associated with compatibility problems [19]. There is also a scope of eloquent attackers identifying and evading honeypots of the AI.

Doi:10.48047/ijiee.2023.13.4.15

Additionally, real-world information to train the model might not be available with the incorporation of secondary research only, and with some privacy and legal issues with using real datasets, which impaired the quality and performance of the suggested system.

D. Recommendations

Companies ought to use AI-based honeypots in the form of a layered defensive approach, with the adaptive goal of being a real-time requirement and integrating with the existing SIEM and threat intelligence portals. Training the models regularly using new attack data is critical in order to continually keep the quality and the relevance of the deceptions [20]. Research institutions in cybersecurity can collaborate to make available anonymised datasets to improve the model. Additionally, it is necessary to be able to set clear ethical and legal frameworks on how to use data and to implement AI to correlate ethics and transparency. User training regarding deception technologies will help with consistency in technical tools and general security policies in the organisations.

VI. CONCLUSION AND FUTURE WORK

Moreover, honeypots are decoy computing processes that replicate real circumstances to mislead attackers into revealing their equipment. Further, this study will look into making the framework more efficient, seeking federated learning solutions to decentralise the training, and generating more context-agnostic deception approaches. A combination of AI deception and blockchain holds the potential to create better data integrity and traceability. Cultivating experimentation on differing infrastructures, will assist in corroborating the framework's efficiency and flexibility under tricky and real circumstances.

VII. REFERENCE LIST

[1] Ojugo, A.A. and Yoro, R.E., 2020. Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. *Technology Report of Kansai University*, *62*(08), pp.5933-5947.

[2] AbuOdeh, M., Adkins, C., Setayeshfar, O., Doshi, P. and Lee, K.H., 2021, May. A novel AI-based methodology for identifying cyber attacks in honey pots. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 35, No. 17, pp. 15224-15231).

[3] Mohamed, N., Al-Jaroodi, J. and Jawhar, I., 2020. Cyber–physical systems forensics: Today and tomorrow. *Journal of Sensor and Actuator Networks*, *9*(3), p.37.

[4] Setianto, F., Tsani, E., Sadiq, F., Domalis, G., Tsakalidis, D. and Kostakos, P., 2021, November. GPT-2C: A parser for honeypot logs using large pre-trained language models. In *Proceedings of the 2021 IEEE/ACM international conference on advances in social networks analysis and mining* (pp. 649-653).

[5] Gopireddy, S.R., 2019. AI-Augmented Honeypots for Cloud Environments: Proactive Threat Deception. *European Journal of Advances in Engineering and Technology*, *6*(12), pp.85-89.

[6] Dowling, S., Schukat, M. and Barrett, E., 2020. New framework for adaptive and agile honeypots. *Etri Journal*, *42*(6), pp.965-975.

[7] Shi, L., Li, Y., Liu, T., Liu, J., Shan, B. and Chen, H., 2019. Dynamic distributed honeypot based on blockchain. *IEEE Access*, *7*, pp.72234-72246.

[8] Newton, J., 2018. Evolutionary game theory: A renaissance. *Games*, *9*(2), p.31.

[9] Naik, N., Shang, C., Jenkins, P. and Shen, Q., 2020. D-FRI-Honeypot: A secure sting operation for hacking the hackers using dynamic fuzzy rule interpolation. *IEEE Transactions on Emerging Topics in*

Doi:10.48047/ijiee.2023.13.4.15

Computational Intelligence, *5*(6), pp.893-907.
[10] Asenahabi, B.M., 2019. Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, *6*(5), pp.76-89.
[11] Mahendra, M.Y.I. and Amelia, D., 2020. Moral values analysis in the fault in our stars novel by John Green. *Linguist. Lit. J*, *1*(2), pp.55-61.
[12] Splunk.com, 2022. *Overview of the Company*, Available at: https://www.splunk.com/en_us/cisco-splunk-better-together.html [Accessed on: 3rd December, 2022]
[13] Forescout.com, 2022. *Overview of the Company*, https://www.forescout.com/company/ [Accessed on: 5th December, 2022]
[14] Trendmicro.com, 2020. *Fake Company, Real Threats*, https://www.trendmicro.com/vinfo/in/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot [Accessed on: 11th December, 2022]
[15] Gao, Y., Zhang, G. and Xing, C., 2021. A multiphase dynamic deployment mechanism of virtualized honeypots based on intelligent attack path prediction. *Security and Communication Networks*, *2021*(1), p.6378218.
[16] Radanliev, P., De Roure, D., Maple, C. and Ani, U., 2022. Super-forecasting the 'technological singularity'risks from artificial intelligence. *Evolving Systems*, *13*(5), pp.747-757.
[17] Naik, N., Shang, C., Jenkins, P. and Shen, Q., 2021. Building a cognizant honeypot for detecting active fingerprinting attacks using dynamic fuzzy rule interpolation. *Expert Systems*, *38*(5), p.e12557.
[18] Srinivasan, V., 2021. Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ingénierie des Systèmes d Inf.*, *26*(6), pp.549-557.
[19] Gemlau, K.B., Köhler, L. and Ernst, R., 2020. A platform programming paradigm for heterogeneous systems integration. *Proceedings of the IEEE*, *109*(4), pp.582-603.
[20] Steingartner, W., Galinec, D. and Kozina, A., 2021. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), p.597.
[21] Chintale P: Optimizing data governance and privacy in Fintech: leveraging Microsoft Azure hybrid cloud solutions. Int J Innov Eng Res. 2022, 11:
[22] Goli, S. R., & Goli, A. K. R. (2022). Strengthening Data Governance and Privacy: Utilizing Amazon AWS Cloud Solutions for Optimal Results. Available at SSRN 5317148.
[23] Goli, Arun Kumar Reddy. "DEVOPS METRICS THAT MATTER: BUSINESS IMPACT OF DORA AND SRE RELIABILITY INDICATORS."
[24] Konda, R. End-to-End Observability in API-Driven Architecture using MuleSoft and Prometheus.

Doi:10.48047/ijiee.2023.13.4.15