iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78940

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Cloud-Based Honeypot for Cyber Threat Intelligence and Incident Response

Gadhe Vijayendar Reddy[1], Varun Jangam[2], Md. Baber Yaseen[3], Dr. Mahammad Rafi D[4]
[1, 2, 3]*CSE Department, Institute Of Aeronautical Engineering* Hyderabad, India
[4]*Assistant Professor in the Department of CSE. Institute Of Aeronautical Engineering* Hyderabad, India

Abstract: ***This paper introduces an advanced honeypot frame- work deployed in a cloud environment to improve cyber threat detection and facilitate efficient incident response. Leveraging Microsoft Azure technologies such as Artillery, Azure Monitor Agent, Log Analytics Workspace, and Microsoft Sentinel, the system is architected to monitor and analyze malicious behaviors in real-time. It enhances situational awareness through threat intelligence integration, behavioral analysis, and automated work-flows. By isolating suspicious activity and delivering actionable insights via detailed telemetry and visual dashboards, the system enables informed security operations. The effectiveness of the architecture is demonstrated through practical implementation, with discussions on performance, encountered challenges, and potential avenues for future development.***
Index Terms: Honeypot, Cybersecurity, Threat Intelligence, Incident Response, Cloud Infrastructure, Microsoft Azure, SIEM

I. INTRODUCTION

The landscape of cybersecurity is undergoing rapid transformation, marked by increasingly advanced and evasive threats. Malicious actors are constantly refining their methods to bypass traditional security controls, making it necessary for organizations to implement smarter and more adaptive defense mechanisms. One such proactive approach involves the use of honeypots—specially crafted decoy systems designed to mimic legitimate assets and attract unauthorized access at- tempts.

These decoys serve as bait for attackers, presenting them- selves as vulnerable systems while being safely isolated and closely monitored. When threat actors interact with these honeypots, their behavior—including attack techniques and tools—is captured, providing crucial insights into real-world threats without exposing critical infrastructure. This threat intelligence can be leveraged to enhance the effectiveness of overall security measures.



Fig. 1. Illustration of Honeypot-based Cloud Cyber Defense

The adoption of cloud computing has further enhanced the capabilities and flexibility of honeypot systems. Cloud platforms offer rapid scalability, broad geographic deployment, and simplified configuration, making it easier to implement decoy environments that are harder for attackers to distinguish from actual assets. These features increase engagement rates and result in more meaningful data collection. Deploying honeypots across diverse cloud regions allows organizations to observe cyberattack trends from a global perspective. This contributes to early threat identification and the development of strategic defenses. Additionally, real-time data collection enables the monitoring of attacker behavior, analysis of net- work activity, and capture of malware samples.

©IJRASET: All Rights are Reserved

The intelligence gathered from honeypot interactions can also be shared with cybersecurity communities, government agencies, and law enforcement bodies. Such collaboration strengthens the collective response to cyber threats and sup- ports broader incident mitigation efforts. Moreover, honeypots assist in identifying internal system vulnerabilities, allowing organizations to fortify their defenses before exploitation oc- curs.

When integrated with advanced platforms like Microsoft Sentinel, honeypots become even more powerful. Real-time detection, automation through predefined response playbooks, and enriched analytics using tools such as Kusto Query Language (KQL) allow for efficient and intelligent threat mitigation. Unlike traditional security tools that often react after a breach, honeypots enable proactive threat hunting and early intervention. Their continuous data generation also supports ongoing research in anomaly detection and machine learning-driven security solutions.

II. LITERATURE REVIEW

1) Hamad AL-Mohannadi et al. investigated how to im- prove cyber threat intelligence by using data from honeypots. The ELK Stack (Elasticsearch, Logstash, and Kibana) was used in their study to process the incident logs that were gathered from a honeypot that was set up on AWS. This platform made it easier to analyze and visualize attack activity in real time, which helped identify sophisticated attacks like Advanced Persistent attacks (APTs). The study identified certain drawbacks, such as the possibility of false positives and the requirement for exact honeypot installations, despite its effectiveness in data analytics and visualization.

2) Sokol, Pekarcik, and Bajtos (2015) explored how hon- eypots and honeynets contribute to cybersecurity through data collection and behavioral analysis. Honeynets, which consist of multiple interconnected honeypots, provide deeper visibility into coordinated attack strategies. The authors emphasized challenges related to managing large volumes of data and the importance of robust analytical techniques to derive actionable insights.

3) A broader perspective on cyber-attack simulations was provided by Al-Mohannadi et al. (2016), who reviewed various modeling techniques aimed at replicating attacker behavior in digital environments. These techniques are useful for testing defense mechanisms and evaluating potential vulnerabilities within secure systems.

4) A structured threat hunting methodology was proposed by SQRRL (2016). This framework adopts a data-driven approach combining anomaly detection, pattern recognition, and expert investigation. It outlines sequential stages including data collection, hypothesis generation, threat investigation, and remediation. Continuous learning and adaptive response are key components of this model.

5) Ovelgonne et al. (2017) conducted a data-driven analysis to examine the link between human behavior and cyber-attack susceptibility. By applying machine learning to behavioral datasets, the study identified common risk patterns such as poor password management, phishing susceptibility, and non- adherence to security protocols, underlining the role of user behavior in organizational cybersecurity.

6) Kandanaarachchi, Ochiai, and Rao introduced the Hon- eyboost framework, which aims to optimize honeypot effec- tiveness using anomaly detection and data fusion techniques. The system uses extreme value theory and dual-dimensional analysis (vertical and horizontal) to detect malicious behavior with high precision, even before direct attacker interaction occurs.

7) A Security Orchestration, Automation, and Response (SOAR) engine was proposed by Bartwal, Mukhopadhyay, Negi, and Shukla. This engine allows behavioral honeypots to be deployed dynamically. By integrating with current security infrastructure, such as SIEM, EDR, and IDS/IPS systems, this engine automates detection workflows and improves threat response speed and accuracy.

III. EXISTING SYSTEM

Current systems leverage the integration of honeypots with Elasticsearch to enhance the collection and analysis of cy- ber threat intelligence. Honeypots are deployed as deceptive systems that mimic vulnerable services or devices to attract malicious actors. Once attackers interact with these decoys, their activities are closely tracked, providing valuable insights into their behavior, techniques, and attack patterns. A central feature of such systems is their data handling and analysis architecture. Data captured by distributed honeypot sensors is transmitted to a centralized Elasticsearch repository. Elasticsearch, known for its distributed and scalable search capabilities, indexes and stores large volumes of structured and unstructured data, enabling extensive analysis of the captured telemetry. To facilitate real-time threat monitoring and visualization, Kibana is employed. This tool, integrated with Elasticsearch, transforms raw data into dynamic, visual dashboards that allow security analysts to detect anomalies, monitor trends, and investigate suspicious behavior through a user-friendly graphical interface.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

One of the core advantages of this setup is its ability to provide continuous threat visibility. By maintaining real- time indexing of logs, security teams can monitor attack attempts as they occur and respond proactively to mitigate potential impacts. This improves organizational response time and helps in containing threats before they escalate.In terms of scalability and performance, the system is well-suited for environments with high data volume requirements. Elastic- search's distributed design ensures efficient handling of large datasets without latency issues, making it applicable for use in enterprise-grade or research-intensive environments.

Additionally, this setup supports advanced threat attribution and cyber forensic analysis. By examining interaction logs from honeypots, analysts can trace the origins of attacks, uncover frequently exploited vulnerabilities, and correlate behaviors with known threat actors. Such in-depth analysis not only strengthens immediate response capabilities but also contributes to long-term threat modeling and prediction.

IV. PROBLEM STATEMENT

Traditional security measures can no longer keep up with the increasing complexity of cyber threats. Advanced technologies like automation, machine learning, and artificial intelligence are being used by modern attackers to go around traditional security measures and more precisely exploit weaknesses. As organizations increasingly embrace cloud platforms and digital transformation, the expansion of the attack surface introduces more endpoints, applications, and remote access vectors that require constant protection.

Conventional security measures, like as intrusion detec- tion systems (IDS) and firewalls, rely heavily on signature- based reasoning, which renders them inadequate in the face of emerging threats like zero-day assaults. Usually reactive, these techniques provide little information about the context or nature of the threat. Furthermore, they frequently result in an excessive number of false positives, which reduces overall operational efficiency and burdens security analysts with redundant notifications.

Manual workflows for identifying and responding to inci- dents introduce delays that adversaries can exploit. Inconsis- tent procedures and human error further compromise security posture, making systems more susceptible to breaches. As a result, there is a critical need for a more dynamic and proactive security framework.

To effectively counter today's cyber threats, organizations must implement intelligent solutions that combine real-time analytics, automated detection, contextual awareness, and behavior-based monitoring. By integrating threat intelligence feeds and automated playbooks, such systems can rapidly iden- tify and mitigate malicious activities, reducing detection time and improving accuracy. This approach not only strengthens defense capabilities but also allows security teams to shift their focus from reactive firefighting to strategic planning and resilience enhancement.

V. PROPOSED SYSTEM

Developed on Microsoft Azure, the suggested system is a cloud-native honeypot architecture intended for automated incident response, behavioral analysis, and real-time threat detection. It makes use of virtual computers set up to mimic vulnerable ports or exposed or poorly secured services using Artillery, a portable honeypot tool. The purpose of these fake assets is to entice cyber attackers and record their attack behaviors, such as exploitation attempts, scanning probes, and brute-force login attempts.

Through the Azure Monitor Agent (AMA), captured telemetry from these interactions is gathered and sent to the central Log Analytics Workspace. This data is enhanced with information from outside databases such as VirusTotal and AbuseIPDB to improve the accuracy of threat detection. These resources assist in confirming whether detected file hashes, URLs, or IP addresses have known associations with malicious activity. Microsoft Sentinel, Azure's integrated Security Information and Event Management (SIEM) platform, is then used to analyze the threat data. Sentinel uses Kusto Query Language (KQL) to apply custom rules and analytics in order to identify suspicious activity, including activity from flagged IPs, brute- force attacks, and repeated scanning. To accelerate mitigation, the system leverages automated workflows built with Azure Logic Apps. These playbooks enable rapid response actions, such as isolating affected virtual machines, blocking attacker IPs, and notifying system administrators in real-time. This automation minimizes the need for manual intervention, thereby reducing reaction time and limiting potential damage. Sentinel also provides real- time dashboards that offer visibility into system health, attack trends, geographical distribution of threats, and alert statuses. This enables security teams to actively monitor the evolving threat landscape and adapt their defenses accordingly. The architecture is modular and highly scalable, allowing for the deployment of multiple honeypot instances across various Azure regions. This multi-region design supports simulation of a wide range of services and broadens visibility across different attack vectors. Furthermore, detection rules and response playbooks are continuously updated to stay aligned with the latest attack techniques, ensuring the system's resilience and adaptability in a dynamic cloud environment.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

VI. SYSTEM MODEL

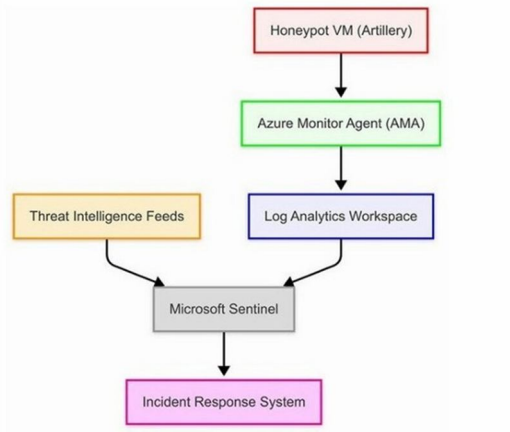


Fig. 2. Architecture Design

The system architecture for the cloud-based honeypot lever- ages the capabilities of Microsoft Azure to provide scalable and automated cyber threat detection and response. At the core of this model is a virtual machine (VM) configured with Artillery, a lightweight honeypot tool that emulates open ports and vulnerable services to attract malicious actors. Once deployed, this decoy system monitors and records various attacker behaviors, including brute-force attempts and port scanning.

Azure's cloud architecture allows for quick deployment and scalability while maintaining this honeypot setup's isolation from production systems. The Azure Monitor Agent (AMA) gathers security and system activity logs from the honeypot virtual machine (VM) and sends them to the Log Analytics Workspace. This workspace provides near real-time awareness into environmental concerns by acting as a central repository for data analysis using Kusto Query Language (KQL).

Threat detection and automated incident handling are driven by Microsoft Sentinel, Azure's integrated SIEM solution. Sentinel continuously ingests and analyzes logs, applies rule- based and heuristic detection logic, and correlates events with data from global threat intelligence feeds. Additionally, features like User Behavior Analytics (UBA) and anomaly detection powered by machine learning enhance the accuracy of identifying sophisticated threats.

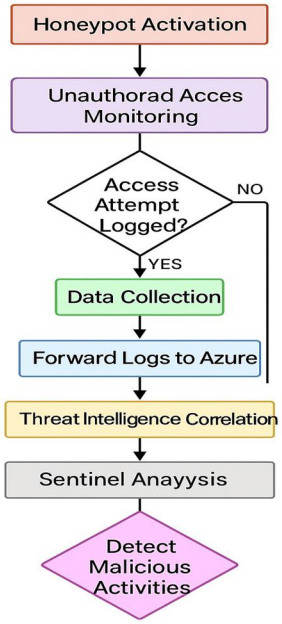


Fig. 3. Honeypot Detection and Response Workflow

©IJRASET: All Rights are Reserved

Automated responses are orchestrated using Azure Logic Apps, which execute pre-defined playbooks when threats are confirmed. These actions may include isolating affected virtual machines, blocking IP addresses, generating alerts, or initiating ticketing workflows for incident management. This automa- tion reduces human intervention, decreases reaction time, and improves the overall efficiency of threat mitigation. The honeypot detection and response process begins with system deployment and initialization. During normal operation, the system passively monitors activity. Upon detecting an attack, detailed telemetry—including attacker IPs, techniques used, and targeted ports—is captured and analyzed in real time. Sentinel evaluates this data against known threat indicators and behavioral patterns. If a threat is validated, corresponding playbooks are automatically triggered to contain and respond to the incident. This architecture establishes a closed-loop defense model where detection, analysis, and mitigation are seamlessly integrated. The modular design ensures continuous monitoring and proactive defense, enabling organizations to move beyond reactive strategies and adopt a more resilient and adaptive cybersecurity posture.

VII. METHODOLOGY

The system follows a modular, cloud-native design that supports continuous threat detection, real-time intelligence collection, and automated response. It is composed of several integrated modules, each fulfilling a distinct function in the overall security architecture:

1) Honeypot Module: This component is responsible for de- ploying decoy virtual machines within the Azure cloud. These VMs emulate exploitable systems by simulating open ports and services, with the goal of attracting and recording unauthorized interactions such as brute-force login attempts, reconnaissance scans, and exploitation behavior.

2) Data Collection Module: Utilizing the Azure Monitor Agent (AMA), this module captures system logs and telemetry data from both the honeypots and surrounding resources. The col- lected data is sent to the centralized Log Analytics Workspace, which serves as the primary data store and query platform for subsequent analysis.

3) Threat Intelligence Module: To enhance detection accuracy, this module integrates external threat intelligence feeds such as VirusTotal and AbuseIPDB. These sources are used to verify whether specific IP addresses, domains, or file hashes have been flagged as malicious, helping to distinguish genuine threats from benign anomalies.

4) SIEM Module: The Security Information and Event Man- agement layer is powered by Microsoft Sentinel. It aggregates log data and applies detection logic using AI-enhanced rules, correlation engines, and behavior-based analytics. Sentinel correlates internal data with external intelligence to identify suspicious patterns or attack signatures in near real time.

5) Incident Response and Automation Module: When a threat is confirmed, this module automatically initiates mitigation workflows using Sentinel Playbooks and Azure Logic Apps. Response actions include IP address blocking, VM isolation, alert generation, and escalation to security personnel. These automated processes significantly reduce the time to respond and limit the window of attacker activity.

6) Visualization and Reporting Module: Real-time dashboards and alerting interfaces are provided to visualize threat data, system status, and attack trends. These insights help security teams monitor incidents, assess threat severity, and refine defense strategies effectively.

7) User Management Module: This module uses Multi- Factor Authentication (MFA) and Role-Based Access Control (RBAC) to secure system access. Critical security components can only be managed or interacted with by authorized persons thanks to these characteristics.

VIII. IMPLEMENTATION

The honeypot solution is implemented using Microsoft Azure, enabling a scalable, cloud-based deployment capable of real-time threat monitoring and automated response. The ar- chitecture integrates continuous data collection, external threat intelligence enrichment, and incident response automation to strengthen an organization's security framework.

Step 1: Deployment and Configuration of the Honeypot A virtual machine (VM) running Ubuntu OS is provisioned in the Azure environment to serve as the honeypot. To attract potential attackers, specific inbound ports—such as 22 (SSH), 80 (HTTP), and 1433 (SQL)—are intentionally exposed. A lightweight honeypot tool, Artillery, is installed on the VM to simulate insecure services and monitor incoming connec- tions. Artillery captures key interaction details, including IP addresses, timestamps, and targeted ports. This decoy setup diverts attackers from critical assets while recording their behavior for further analysis.

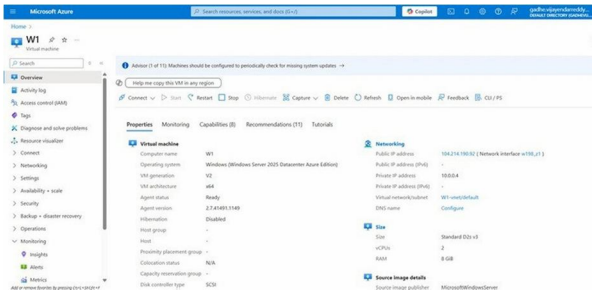


Fig. 4. Virtual Machine Configuration for Honeypot Deployment in Azure

Step 2: Log Collection, Enrichment, and Monitoring To enable log management, the Azure Monitor Agent (AMA) is configured on the VM. It collects system and network activity logs from the honeypot and forwards them to the Log Analytics Workspace, which functions as a centralized storage and analysis hub. To improve detection precision, the collected data is enriched using third-party threat intelligence platforms such as AbuseIPDB and VirusTotal, which help verify the reputation of IPs and detect known malicious signatures. Analysts use Kusto Query Language (KQL) within Azure to investigate attacker behaviors, trace targeted ports, and identify patterns such as brute-force attacks and scanning activities.

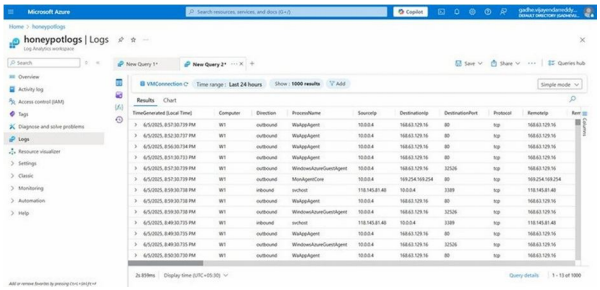


Fig. 5. VM Connection Logs from Azure Log Analytics Workspace showing inbound and outbound traffic details

Step 3: Threat Detection, Automation, and Visualization Microsoft Sentinel is integrated with the Log Analytics Workspace to handle threat detection. Sentinel leverages built- in detection rules and analytics templates to raise alerts when suspicious activity is detected. Playbooks carry out pre- configured tasks like blocking malicious IP addresses, isolating compromised virtual machines, or notifying the security oper- ations team in order to conduct automated incident response with Azure Logic Apps. Additionally, Sentinel's visualization capabilities and Azure Workbooks are used to create unique dashboards. These dashboards display up-to-date information on the origins of attacks, the kinds of activities that were noticed, and the threats' geographic origins. The solution facil- itates quick decision-making and improves the organization's overall cybersecurity posture by converting honeypot data into actionable insight.

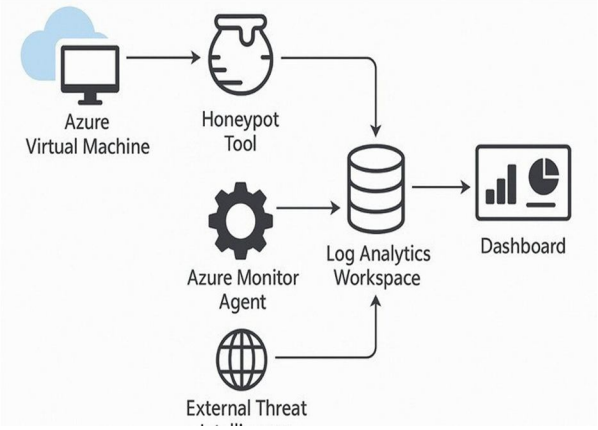


Fig. 6. Honeypot Data Flow in Azure Environment

IX. RESULTS

The deployment of the cloud-based honeypot solution was successfully completed within the Microsoft Azure environ- ment. An Azure Resource Group was created to manage and logically organize all components involved in the deployment. A virtual machine (VM) running Ubuntu was provisioned within this group to emulate vulnerable systems. The VM was configured with a public IP and intentionally exposed inbound ports, such as SSH (22) and HTTP (80), to attract unauthorized connection attempts.

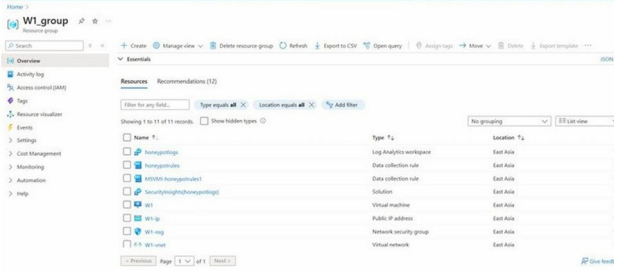


Fig. 7. Azure Resource Group Showing Honeypot-Related Deployments

To facilitate log aggregation and centralized monitoring, Azure Monitor Agent (AMA) was configured on the honeypot VM. It ensured that all network activity and system events were directed to the Log Analytics Workspace. This workspace served as a secure repository for telemetry and supported structured analysis of interaction logs. The Artillery honeypot was installed on the VM and configured to observe and record traffic on specific ports. Its file structure allowed easy access to captured data, including logs and configuration settings.

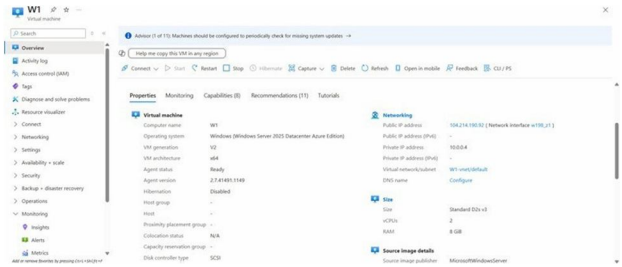


Fig. 8. Azure Virtual Machine Configuration for Honeypot Deployment

During the monitoring phase, the honeypot recorded mul- tiple unauthorized access attempts in real time. Data col- lected from Azure queries showed comprehensive details about inbound and outbound traffic. These logs included IP ad- dresses, targeted ports, timestamps, and session characteristics. Notably, connection data indicated attempts originating from various geographic locations—including Germany, China, the United States, and Singapore—suggesting international scan- ning and reconnaissance activity. The system demonstrated effective threat attraction and data collection without exposing operational infrastructure to risk. Artillery successfully logged malicious activity across the open ports, providing a valuable stream of intelligence. The Log Analytics Workspace, paired with visual dashboards, enabled security teams to track live attack trends and analyze the behavioral patterns of potential intruders.

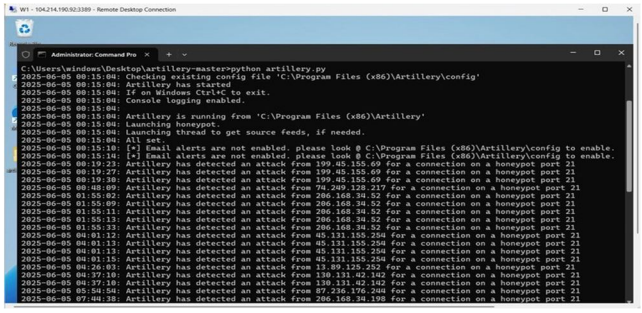


Fig. 9. Artillery honeypot running on Windows server detecting attacks on port 21.

The enriched telemetry supported by external threat intel- ligence made it possible to identify known bad actors and frequently targeted services. Automated alerting and detection rules, integrated via Microsoft Sentinel, ensured that incidents were rapidly flagged and analyzed. This contributed to con- tinuous monitoring, proactive threat defense, and enhanced incident handling capabilities.

These results validate the system's ability to serve as a func- tional, low-risk detection environment, capable of collecting and interpreting attacker behavior while enabling informed and rapid defensive actions.

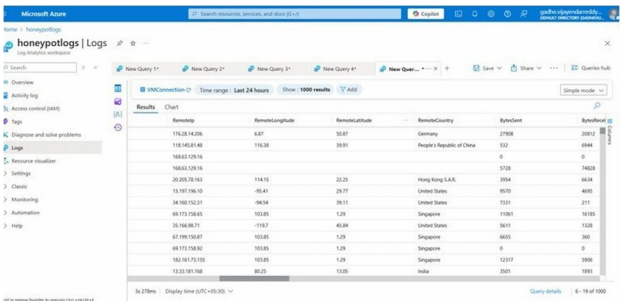


Fig. 10. Azure Log Analytics displaying attacker IPs and telemetry data from honeypot VM.

X. CONCLUSION

The development and deployment of the proposed cloud- based honeypot framework mark a significant step forward in establishing an intelligent, scalable, and adaptive approach to cybersecurity. Built on Microsoft Azure and utilizing com- ponents such as Artillery and Microsoft Sentinel, the system enables persistent monitoring, automated threat detection, and efficient incident response within dynamic cloud environments. This project has demonstrated technical feasibility and operational simplicity, while also maintaining compliance with widely accepted data protection practices. The use of modular components allows for flexible expansion and integration with other security tools, ensuring that the system can evolve alongside emerging threats and infrastructure changes. Beyond basic threat detection, the system offers strategic advantages, including enriched threat intelligence, behavioral analysis, and real-time response automation. Its proactive design minimizes exposure to risk while enhancing visibility into attacker tac- tics and techniques. The combination of telemetry analysis, automated mitigation, and centralized monitoring contributes to stronger defense capabilities across organizational assets.In conclusion, the system fulfills its primary objectives by de- livering a forward-looking cybersecurity solution that is both cost-effective and operationally robust. It enhances detection accuracy, reduces exposure to threats, and equips security teams with the insights needed to respond rapidly and intelli- gently to modern cyberattacks.

XI. ACKNOWLEDGMENT

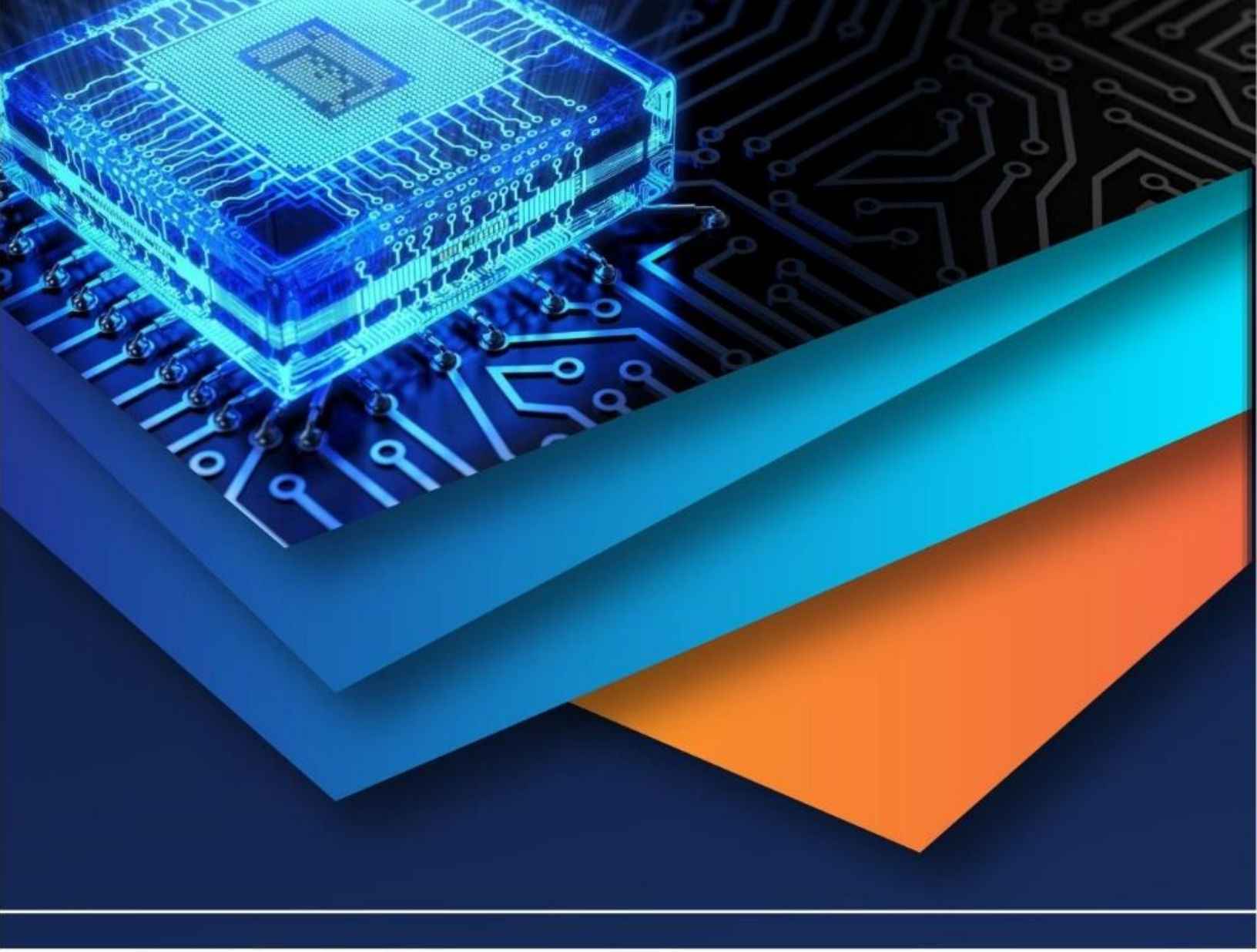
The Department of CSE(CS), Institute of Aeronautical En- gineering, Hyderabad, India, supplied the necessary materials for this paper's research study and related activities.

REFERENCES

[1] H. Almohannadi, I. Awan, J. Al Hamar, A. Cullen, J. Disso, and L. Armitage, "Elasticsearch-Based Cyber Threat Intelligence from Honeypot Data," Proceedings of the International Conference on Cyber Security, 2018.
[2] "Data Collection and Analysis in Honeypots and Honeynets," Journal of Information Security, vol. 6, pp. 45–52, 2015, by P. Sokol, P. Pekarcik, and T. Bajtos.
[3] "An Overview of Cyber-Attack Modeling Analysis Techniques," by H. Al-Mohannadi, Q. Mirza, et al. IEEE Fourth International Workshop on Cloud and Future Internet, 2016.
[4] [4] D. Ovelgonne and colleagues, "A Data-Driven Approach to Under- standing Human Behavior and Cyber Threat Susceptibility," ACM Trans. Intell. Syst. Technol. (TIST), vol. 8, no. 3, 2017.
[5] "Honeyboost: Enhancing Honeypot Performance with Data Fusion and Anomaly Detection," Proc. of the Cybersecurity Conference, 2020, N. Kandanaarachchi, H. Ochiai, and S. Rao.
[6] "Security Orchestration for Behavioral Honeypots," by M. Bartwal,
[7] S. Mukhopadhyay, R. Negi, and R. Shukla, IEEE Conf. on Security Automation, 2020.
[8] L. Wang, C. Chen, et al., "ThingPot: An Interactive IoT Honeypot," Proc. of the Int. Conf. on IoT Security, 2020.
[9] S. Panda, A. Kumar, and P. Sahu, "HoneyCar: A Honeypot Framework for Internet of Vehicles," IEEE Vehicular Technology Conf., 2021.
[10] A. Deshpande, "HoneyMesh: Preventing DDoS Attacks Using a Dis- tributed Honeypot Network," Proc. of the Int. Symp. on Network Defense, 2019.
[11] H. Fan, M. Zhang, et al., "HoneyDOC: An Efficient Honeypot Architec- ture for Document Exploits," IEEE Conf. on Threat Intelligence, 2019.
[12] Dr. Dobb's Journal of Software Tools, vol. 24, no. 12, pp. 21–29, 1999;

[13] B. Schneier, ”Attack Trees.”
[14] “Cloud Storage as an Attack Vector: A Case Study on Dropbox,” Proceedings of the USENIX Security Symposium, 2011. P. Mulazzani,
[15] S. Schrittwieser, M. Huber, and E. Weippl.
[16] ”Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” by E. Hutchins, M. Cloppert, and R. Amin, Lockheed Martin Corp., 2010.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)