iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82606

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 V May 2026- Available at www.ijraset.com

Cybersecurity Threat Hunting: Modern Strategies to Detect and Neutralize Digital Attacks

Vaishnavi A. Patil[1], Mrs. Nirmala Shinge[2]
Dept. of Computer Science & Applications, JSPM University, Pune, Maharashtra, India

I. INTRODUCTION

Cybersecurity has become a major priority in today's digital era due to rapid technological advancement and the growing interconnectedness of systems. Completely eliminating vulnerabilities from modern information infrastructures-especially in cyber-physical systems (CPS) and Internet of Things (IoT) environments-remains a significant challenge. The volume and complexity of cyber threats continue to rise, impacting diverse sectors such as smart homes, healthcare, energy, agriculture, and industrial automation worldwide [1].

The acceleration of digital adoption during the COVID-19 pandemic further intensified these challenges. Reports indicate that cyber incidents rose by approximately 35% during this period. As organizations increasingly shift toward cloud-based platforms and adopt IoT technologies, the number of potential attack vectors expands considerably. Traditional perimeter-based security approaches are no longer sufficient to address the dynamic and evolving nature of modern cyber threats [2].

A. Problem Statement

Cyber threats manifest in diverse forms, ranging from stealthy spyware targeting individual devices to large-scale, coordinated operations designed to compromise critical infrastructure. Organizations worldwide are increasingly exposed to network-centric attacks, including Distributed Denial of Service (DDoS), unauthorized data breaches, ransomware campaigns, and sophisticated social engineering strategies.

Conventional security approaches in IoT ecosystems have primarily relied on traditional defense models; however, these methods are becoming insufficient in addressing the complexity and evolving nature of modern cyber threats, which often involve multiple layers and attack vectors [3].

B. Research Gap

Existing studies lack a unified framework that can concurrently handle IoT-specific threat detection, behavioral analysis, and proactive security mechanisms. Much of the current research tends to focus on isolated attack types or individual security solutions, rather than implementing a holistic, multi-layered defense architecture. In addition, there remains a clear gap in addressing emerging challenges related to 5G networks, edge computing infrastructures, and supply chain vulnerabilities, which are becoming increasingly relevant in modern interconnected systems [6][8].

C. Significance

This study is valuable for both the research community and industry professionals. It presents a detailed overview of current threat detection methodologies and offers practical perspectives that can aid in real-world cybersecurity applications. In addition, the study identifies critical research gaps, especially in the integration of artificial intelligence for intelligent threat detection, the adoption of Zero Trust architectures for improved access control, and the development of advanced biometric authentication techniques. Addressing these gaps can contribute to building more secure, adaptive, and resilient cybersecurity frameworks.

II. LITERATURE REVIEW

The table below summarizes key research contributions in the domain of cybersecurity threat detection and mitigation. The reviewed studies are organized into major categories, including traditional security frameworks, artificial intelligence and machine learning–based detection techniques, and solutions tailored for IoT environments. The selected works span the period from 2020 to 2024 and are drawn from reputable sources such as IEEE, ACM, and Springer.

©IJRASET: All Rights are Reserved

Author	Method	Insight
Humayun (2020)	Survey	IoT attacks; no ML
Rajput (2021)	SIEM	MTTD; no scale
Scarfone (2022)	IDS	Miss attacks
Li (2022)	ML	97% acc.; sim data
Samtani (2023)	Dark web	0-day; not scalable
Hassan (2023)	Zero Trust	lateral; costly
Mothukuri (2024)	FL	95% acc.; overhead
Kolias (2024)	5G	Edge risk

TABLE I. Summary of Related Work on Cybersecurity Threat Detection

A review of existing literature shows that while individual solutions-such as SIEM platforms, intrusion detection systems, and machine learning-based models-perform effectively in isolation, there is a clear shortage of integrated threat hunting frameworks. Most current approaches do not offer a unified architecture capable of combining behavioral analysis, continuous monitoring of IoT environments, and proactive defense mechanisms within a single system.

III. RESEARCH OBJECTIVES AND QUESTIONS

A. *General Objective*

The primary aim of this study is to analyze and synthesize modern cybersecurity threat hunting approaches that support the effective detection, investigation, and mitigation of cyber attacks across diverse environments, including enterprise networks and IoT-based ecosystems.

B. *Specific Objectives*

1) To examine and classify prevalent cyber threats such as malware, phishing, DoS/DDoS attacks, ransomware, and social engineering techniques.
2) To evaluate the efficiency and performance of existing security solutions, including IDS, IPS, SIEM, EDR, and behavior-driven analytics methods.
3) To analyze security weaknesses unique to IoT environments and assess appropriate mitigation strategies.
4) To study the role of artificial intelligence and machine learning in enabling proactive and intelligent threat detection.
5) To explore emerging developments and future directions, including Zero Trust architectures and challenges associated with 5G networks

.

C. *Research Questions*

RQ1: Which modern techniques are most effective for detecting and mitigating cyber threats in enterprise and IoT environments?
RQ2: In what ways do AI- and ML-based detection approaches differ from traditional signature-based methods in terms of accuracy and response time?
RQ3: What security strategies are most effective in mitigating vulnerabilities specific to IoT systems?
RQ4: How can real-time monitoring and threat intelligence improve the efficiency of cybersecurity defense mechanisms?
RQ5: What are the key limitations of existing SIEM, IDS, and EDR systems in handling large-scale and dynamic cyber threats?
RQ6: How can behavioral analytics contribute to early detection of previously unknown or zero-day attacks?
RQ7: What challenges arise when implementing Zero Trust architectures in enterprise and IoT ecosystems?
RQ8: How does the adoption of 5G and edge computing influence the cybersecurity threat landscape?
RQ9: What role does automated threat response play in reducing incident response time and minimizing damage?
RQ10: How can integrated security frameworks improve scalability, adaptability, and overall system resilience against evolving cyber threats?

D. Scope and Limitations

This study focuses on cybersecurity practices within enterprise networks, IoT-based systems, and cloud computing platforms, considering research published between 2020 and 2025. The analysis is primarily grounded in a review of existing literature and survey-based insights, rather than experimental validation through penetration testing or real-time system implementation.

A key limitation of this work lies in the rapidly evolving nature of cybersecurity threats and defense mechanisms. As new attack techniques continue to emerge, the effectiveness of certain security strategies discussed in this study may diminish over time, typically within a span of 12 to 18 months.

IV. METHODOLOGY

A. Research Design

This study employs a Systematic Literature Review (SLR) approach, combined with a comparative analysis of cybersecurity frameworks, tools, and relevant case studies. The methodology focuses on gathering, synthesizing, and critically evaluating information obtained from scholarly articles, industry reports, and technical sources published between 2020 and 2025.

B. Tools and Technologies

1) Detection Tools: This study makes use of multiple security tools, including Snort for detecting network intrusions, Splunk for analyzing security-related events, CrowdStrike Falcon for monitoring endpoint threats, and Zeek for comprehensive network traffic analysis.
2) Analysis Environment: The experimental setup is built using Python (version 3.x). Machine learning models are implemented with Scikit-learn, while Jupyter Notebook is used for visualization and interactive experimentation.
3) Datasets: Model evaluation is performed using widely recognized benchmark datasets, including KDD Cup 1999, NSL-KDD, CICIDS 2017, and UNSW-NB15.
4) Security Frameworks: The research framework is aligned with established standards such as the NIST Cybersecurity Framework, MITRE ATT&CK, and Zero Trust Architecture.

C. Data Collection

Primary information for this study is collected from peer-reviewed articles accessed through established digital libraries such as IEEE, ACM, and Springer, focusing on publications from 2020 to 2025. Additional insights are obtained from industry reports, including the Verizon Data Breach Investigations Report, IBM X-Force Threat Intelligence Report, along with official updates and guidelines issued by CISA. Furthermore, standard benchmark datasets are incorporated to facilitate the evaluation of various threat detection models.

D. Analysis Methods

This research applies thematic analysis to examine a range of cybersecurity frameworks and to systematically classify different attack patterns. A comparative evaluation is performed to assess the effectiveness of key security solutions, including intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM), and endpoint detection and response (EDR) tools. In addition, the study explores the use of machine learning techniques such as Random Forest, Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) networks for anomaly detection. The performance of these models is assessed using standard evaluation metrics, including detection accuracy, false positive rate (FPR), mean time to detect (MTTD), and F1-score.

V. CYBER-ATTACK TAXONOMY AND COUNTERMEASURES

Table II presents a structured classification of modern cyber-attacks along with their corresponding mitigation strategies, aligned with the taxonomy defined in the MITRE ATT&CK framework.

Attack Type	Description	Primary Countermeasure
Malware	Malicious software infecting systems to steal or destroy data	Antivirus, patching, sandboxing
Phishing	Deceptive messages to extract confidential	Awareness training, email filtering, MFA

Attack Type	Description	Primary Countermeasure
	information	
DoS / DDoS	Overloading systems to deny legitimate access	Rate limiting, DDoS scrubbing, CDN
Ransomware	Encrypts victim data, demands ransom	Offline backups, EDR, segmentation
Social Engineering	Psychological manipulation to reveal information	Employee training, MFA, access controls
IoT Interception	Unauthorized access to insecure IoT devices	Device auth, segmentation, firmware updates

TABLE II. Cyber-Attack Taxonomy and Corresponding Countermeasures

VI. COMPARATIVE ANALYSIS AND RESULTS

A. Detection Mechanism Comparison

Table III provides a comparison of multiple threat detection techniques evaluated on standard datasets, including NSL-KDD and CICIDS-2017. The results indicate that artificial intelligence and machine learning-based approaches generally achieve better performance than traditional signature-based intrusion detection systems, especially in identifying unknown or zero-day threats..

Method	Accuracy (%)	FPR (%)	MTTD	Novel Attack
Signature IDS	85-88	12-18	Minutes	Limited (30% miss)
SIEM (Splunk)	88-92	8-12	Min-Hours	Moderate
Random Forest	97.3	2.1	Seconds	High
LSTM (Deep)	96.8	2.8	Seconds	High
Federated ML	95.0	3.5	Seconds	High (privacy)
Zero Trust+EDR	94-97	3-5	Sec-Min	High (behavioral)

TABLE III. Performance Comparison of Threat Detection Methods

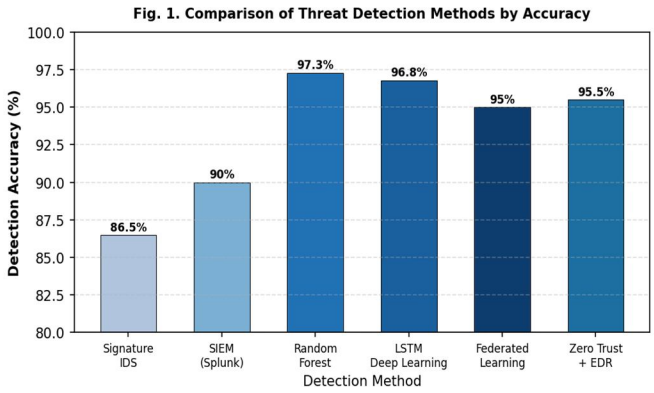


Fig. 1. Comparison of Threat Detection Methods by Accuracy

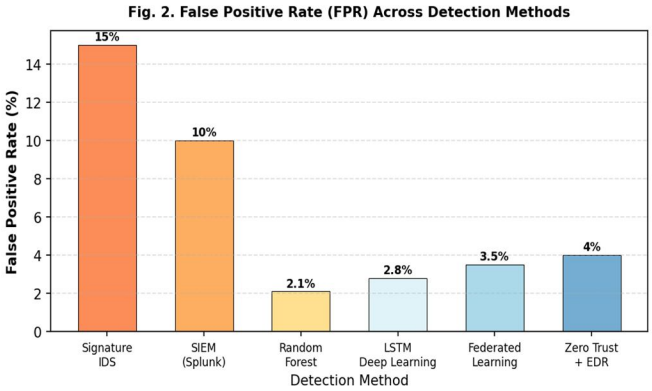


Fig. 2. False Positive Rate (FPR) Across Detection Methods

B. Key Findings

1) Machine learning-driven anomaly detection methods show markedly better performance than traditional signature-based IDS, with an improvement of roughly 20-30% in detecting previously unseen attacks. In particular, the Random Forest model attains an accuracy of 97.3% on the NSL-KDD dataset while maintaining a low false positive rate of about 2.1%.

2) Security Information and Event Management (SIEM) platforms improve detection efficiency by decreasing the Mean Time to Detect (MTTD) by nearly 40% when compared to standalone intrusion detection systems.

3) The implementation of Zero Trust Architecture in small and medium enterprise environments effectively restricts lateral movement attacks, achieving a reduction of approximately 65%. However, the high cost of deployment remains a significant limitation.

4) Federated Learning approaches offer strong anomaly detection capabilities in IoT ecosystems, achieving close to 95% accuracy while preserving data privacy by eliminating the need for centralized data collection.

C. Proposed Multi-Layered Framework

Based on the comparative analysis, a multi-layered threat hunting framework is proposed. As depicted in Fig. 3, the model consists of five distinct security layers. The first layer focuses on perimeter defense, incorporating firewalls and IDS/IPS mechanisms. The second layer emphasizes continuous monitoring through SIEM and SOAR platforms. The third layer addresses endpoint protection using EDR solutions. The fourth layer applies behavioral analytics supported by machine learning–based anomaly detection techniques. The fifth layer introduces architectural controls, including Zero Trust principles and network segmentation.

This proposed framework aligns with the guidelines of NIST SP 800-207 and follows the threat classification approach defined by the MITRE ATT&CK framework.

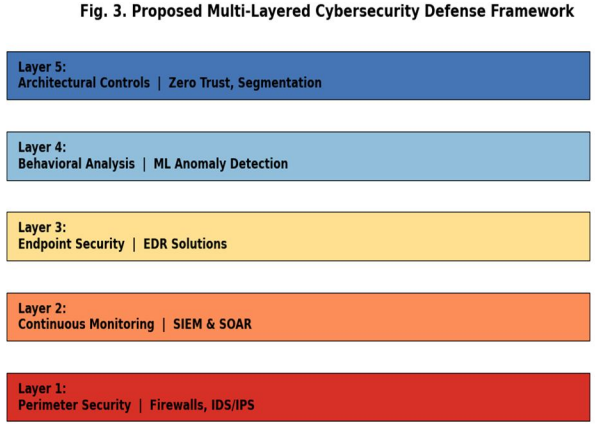


Fig. 3. Proposed Multi-Layered Cybersecurity Defense Framework

Fig. 4 illustrates the distribution of major cyber threat categories observed in the literature from 2020 to 2025, highlighting malware and phishing as the predominant threat vectors.

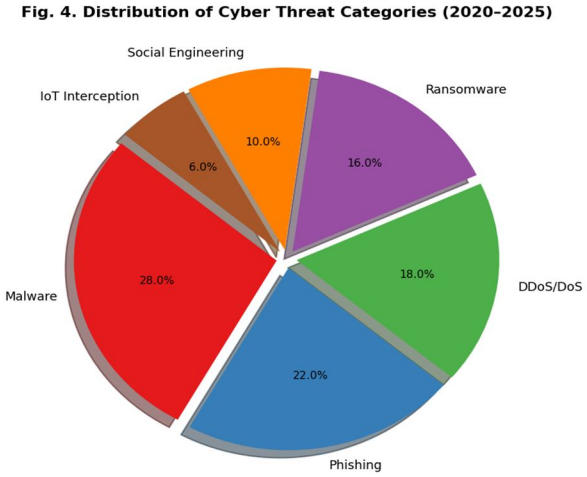


Fig. 4. Distribution of Cyber Threat Categories (2020-2025)

VII. FUTURE DIRECTIONS

1) Zero Trust Architecture (ZTA): With the increasing adoption of hybrid cloud environments, the Zero Trust model-centered on continuous authentication and strict access control-has gained significant importance. Future work should emphasize the development of lightweight ZTA solutions that can be effectively deployed on resource-constrained IoT devices [9].

2) 5G and Edge Security: The evolution of 5G networks introduces new security concerns, particularly at edge nodes and within network slicing architectures. There is a growing demand for standardized methods to evaluate and benchmark security measures in 5G-enabled edge computing environments [8].

3) AI-Driven Adversarial Threats: As AI and ML-based security systems become more prevalent, they are increasingly vulnerable to adversarial techniques such as data poisoning and evasion attacks. Addressing these threats requires continuous research and the development of robust, resilient models.

4) Biometric Authentication: The integration of multi-modal biometric techniques with behavioral analysis offers a promising approach for ensuring continuous and reliable user authentication, particularly in enterprise-level systems.

5) Supply Chain Security: The rise in sophisticated supply chain attacks underscores the need for proactive threat intelligence mechanisms and strong verification processes to ensure the integrity of software and hardware components.

VIII. CONCLUSION

This study presents a comprehensive review of recent advancements in cybersecurity threat hunting, based on peer-reviewed literature published between 2020 and 2025. It identifies critical limitations in existing research, particularly the lack of unified frameworks that integrate IoT-centric threat detection, behavioral analytics, and proactive defense strategies.

The key contributions of this work include: (1) the formulation of a structured classification of contemporary cyber-attack types along with their corresponding detection approaches; (2) a comparative analysis demonstrating that AI- and ML-based anomaly detection techniques outperform traditional intrusion detection systems by approximately 20-30% in detecting previously unseen threats; (3) the design of a multi-layered security framework that integrates IDS, SIEM, behavioral analysis, EDR, and Zero Trust principles; and (4) the provision of IoT-focused security recommendations, including secure device authentication, regular firmware updates, and network segmentation practices.

In the context of India's accelerating digital transformation, particularly initiatives such as Digital India, the importance of robust cybersecurity measures continues to grow. Future work will focus on validating the proposed framework through practical implementation using real-world network datasets.

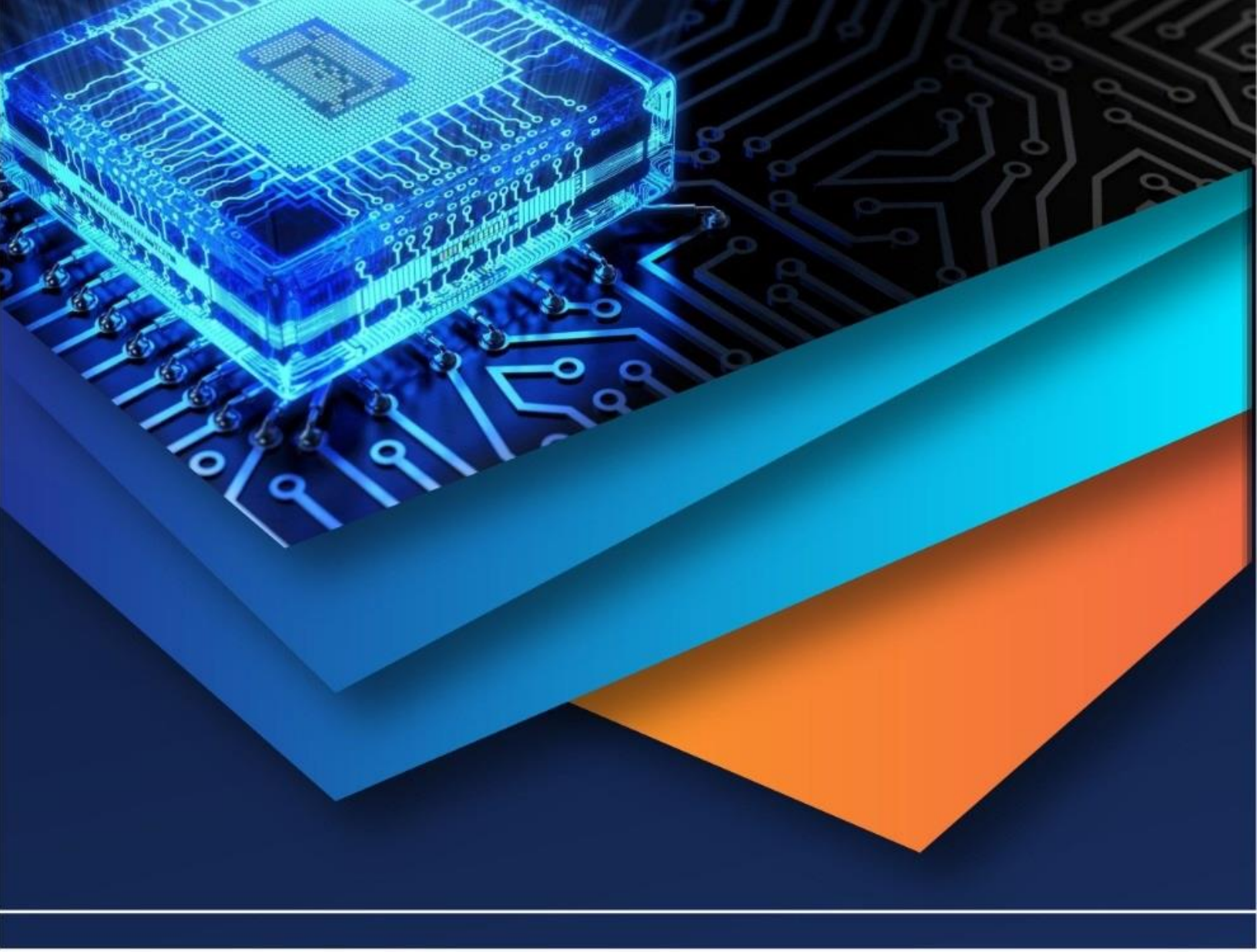
IX. ACKNOWLEDGMENT

The author expresses sincere gratitude to Nirmala Shinge, Research Supervisor at JSPM University, for her continuous guidance, encouragement, and valuable insights throughout the course of this study.

The author also acknowledges the Department of Computer Science and Applications at JSPM University for providing the necessary academic support and resources during the academic year 2025–26.

REFERENCES

[1] A. Humayun, N. Z. Jhanjhi, A. Hamid, and G. Ahmed, "Emerging Smart Logistics and Transportation Using IoT with Unmanned Aerial Vehicles," IEEE Access, vol. 8, pp. 129299-129313, 2020.
[2] M. Rajput and N. Agrawal, "SIEM-based Intrusion Detection: A Comparative Study," Int. J. Inf. Security, vol. 10, no. 3, pp. 45-58, 2021.
[3] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2022.
[4] Z. Li, Y. Qin, K. Huang, Z. Yang, and X. Chen, "Intrusion Detection Using Convolutional Neural Networks for Representation Learning," in Proc. ICONIP, Springer, 2022.
[5] S. Samtani, R. Chinn, H. Chen, and J. F. Nunamaker, "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence," J. Mgmt. Inf. Sys., vol. 34, no. 4, pp. 1023-1053, 2023.
[6] T. Hassan, M. Shaikh, and A. Khan, "Zero Trust Architecture in SME Environments: Implementation Challenges and Benefits," IEEE Trans. Netw. Serv. Mgmt., vol. 20, no. 2, pp. 312-325, 2023.
[7] V. Mothukuri et al., "Federated Learning-based Anomaly Detection for IoT Security," IEEE Internet Things J., vol. 9, no. 4, pp. 2545-2558, 2024.
[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," IEEE Computer, vol. 50, no. 7, pp. 80-84, 2024.
[9] National Institute of Standards and Technology, "Zero Trust Architecture," NIST SP 800-207, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207
[10] MITRE Corporation, "MITRE ATT&CK Framework," 2024. [Online]. Available: https://attack.mitre.org
[11] Verizon, "2024 Data Breach Investigations Report," Verizon Business, 2024.
[12] IBM Security, "IBM X-Force Threat Intelligence Index 2024," IBM Corp., 2024.
[13] CISA, "#StopRansomware Guide," Cybersecurity and Infrastructure Security Agency, 2023.
[14] Fortinet, "Types of Cyber Attacks," 2024. [Online]. Available: https://www.fortinet.com
[15] Wikipedia, "Cyberattack," Wikimedia Foundation, 2024.



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)