International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 5, Sep-Oct 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Vulnerability Management and Automated Incident Response in Corporate Networks

Sums Uz Zaman*,
*(Department of Electrical and Computer Engineering, The City College of New York
Email: sondyzaman999@gmail.com)

----------**********----------

Abstract:

In the modern digital era, corporate networks are increasingly exposed to sophisticated cyber threats that exploit system vulnerabilities. Traditional vulnerability management and incident response approaches rely heavily on manual operations, leading to slow detection, inefficient mitigation, and prolonged exposure to attacks. To address these challenges, this study introduces an integrated framework that combines automated vulnerability management with intelligent incident response mechanisms. The proposed system continuously monitors network assets, prioritizes vulnerabilities based on risk assessment models, and initiates automated response actions such as isolation, patching, or containment through orchestration platforms. By leveraging automation and artificial intelligence, the framework minimizes human error, shortens response time, and enhances overall security posture. Experiments conducted in a simulated corporate network demonstrate significant improvements in detection and containment efficiency. The system reduced mean time to detect (MTTD) by 42% and mean time to respond (MTTR) by 58%, while lowering operational overhead and false positives. Results confirm that integrating automation within vulnerability management and incident response processes increases resilience against evolving threats. The research highlights the importance of adaptive automation in strengthening enterprise cyber security strategies, enabling organizations to proactively defend against cyber attacks while maintaining business continuity.

Keywords — Vulnerability Management, Automated Incident Response, Cybersecurity, Threat Mitigation, Corporate Networks, Risk Assessment.

----------**********----------

I. INTRODUCTION

In the modern digital ecosystem, corporate networks form the foundation of business operations, enabling seamless communication, data management, and service delivery. However, this growing interconnectivity also increases exposure to cybersecurity risks. As organizations adopt cloud computing, remote work, and Internet of Things (IoT) technologies, their attack surfaces expand, offering adversaries more entry points to exploit. Consequently, cybersecurity has become a strategic priority, with vulnerability management and incident response playing crucial roles in safeguarding network integrity. Traditional approaches to vulnerability management rely heavily on manual patching, periodic scans, and human analysis. These methods are often too slow and inconsistent to counter the speed and sophistication of modern cyber threats. Likewise, incident response teams frequently face overwhelming alert volumes and fragmented systems, leading to delayed containment and increased risk exposure. The reliance on reactive defense mechanisms leaves organizations vulnerable to prolonged breaches, financial losses, and reputational damage. To address these limitations, automation and artificial intelligence offer transformative potential. By integrating vulnerability detection, prioritization, and response within a unified,

automated framework, organizations can enhance detection accuracy, reduce response time, and minimize operational burden. This paper explores the concept of Vulnerability Management and Automated Incident Response in corporate networks, emphasizing the need for adaptive, intelligent systems that proactively mitigate threats. It presents a framework that leverages automation to ensure continuous protection and resilience in an ever-evolving threat landscape.

A. Background and Motivation

The rapid evolution of technology has expanded corporate attack surfaces through cloud computing, Internet of Things (IoT) integration, and remote work infrastructure. Consequently, organizations face an ever-growing number of vulnerabilities that require prompt identification and mitigation. Traditional patch management and incident response workflows involve manual verification, prioritization, and coordination, which consume significant time and resources. Meanwhile, adversaries exploit these delays, often launching attacks that move laterally within networks before detection. Reports from industry studies indicate that the average time to detect and contain breaches can exceed 200 days, amplifying operational and financial risks. Therefore, organizations must adopt proactive and automated approaches that combine continuous monitoring, risk prioritization, and intelligent response execution. Automation, supported by artificial intelligence and orchestration tools, not only accelerates detection and mitigation but also reduces dependency on limited human expertise. This shift is essential to handle the scale, speed, and complexity of modern cyber threats.

B. Problem Statement

Despite the availability of sophisticated security tools, corporate environments still struggle with fragmented vulnerability management systems and reactive incident response processes. Security teams often operate under high alert fatigue caused by an overwhelming number of false positives, resulting in the neglect of genuinely critical vulnerabilities. Manual methods also create inconsistencies in threat prioritization, with patch cycles varying across departments and assets. Furthermore, lack of integration between vulnerability scanners, security information and event management (SIEM) tools, and response platforms leads to inefficient data correlation and delayed decision-making. As a result, attackers often exploit these operational gaps to infiltrate networks, exfiltrate sensitive data, or disrupt critical services. The primary problem addressed in this paper is the absence of a unified, automated framework that connects vulnerability detection with real-time, adaptive response mechanisms. Bridging this gap is crucial to reduce the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), minimize human error, and ensure continuous protection. An intelligent, automated framework can overcome these challenges by correlating vulnerabilities with threat intelligence, assessing contextual risk, and autonomously triggering containment or remediation actions.

C. Proposed Solution

To address the limitations of manual systems, this research proposes an Automated Vulnerability Management and Incident Response Framework (AVMIRF) that integrates vulnerability detection, risk prioritization, and automated response into a cohesive ecosystem. The framework employs artificial intelligence and automation to analyze vulnerabilities based on asset criticality, exploitability, and potential impact. Once a vulnerability or active threat is identified, predefined playbooks execute appropriate responses, such as isolating affected hosts, deploying patches, or alerting administrators. The system integrates with existing security tools, including vulnerability scanners (e.g., Nessus, OpenVAS), SIEM solutions (e.g., Splunk, ELK), and SOAR platforms (e.g., Cortex XSOAR), through API-based communication. By continuously collecting and analyzing network telemetry, the framework ensures timely detection and

automated mitigation of security incidents. Furthermore, it employs a feedback loop to refine detection algorithms and improve decision-making accuracy. The proposed solution effectively bridges the operational gap between detection and remediation, ensuring faster, data-driven, and repeatable responses to cyber incidents.

D. Contributions

This paper makes several significant contributions to the advancement of cybersecurity automation, particularly in the integration of vulnerability management and incident response. First, it introduces the Automated Vulnerability Management and Incident Response Framework (AVMIRF), a unified system that bridges the gap between vulnerability detection, prioritization, and automated remediation. By combining these traditionally separate processes, the framework enhances coordination between detection and containment, reducing response latency and minimizing potential damage. Secondly, the framework incorporates AI-driven risk prioritization, utilizing machine learning algorithms to assess vulnerabilities based on contextual factors such as asset value, exploitability, and threat intelligence. This approach improves the accuracy of prioritization and significantly reduces false positives, ensuring that security resources are allocated efficiently. Moreover, the system integrates automated response playbooks that can execute critical actions such as isolating compromised systems, deploying patches, or revoking credentials without requiring continuous human intervention, thus improving response consistency and speed. Additionally, the paper provides a comprehensive performance evaluation through simulated enterprise environments, measuring improvements in key security metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and overall operational efficiency. Finally, it introduces a continuous learning component that refines detection and response models based on feedback from past incidents. Collectively, these contributions establish a foundation for transforming corporate cybersecurity from reactive, human-dependent operations into intelligent, proactive, and adaptive systems.

E. Paper Organization

The remainder of this paper is organized to provide a logical and comprehensive exploration of the proposed framework for vulnerability management and automated incident response in corporate networks. Section II presents a detailed review of related research and existing approaches in vulnerability management, threat detection, and response automation. It highlights the evolution of cybersecurity strategies, identifies major research gaps, and establishes the foundation for the proposed system by analyzing limitations in traditional manual processes. This section also contrasts existing automation tools and frameworks to position the contribution of this study within the broader research landscape. Section III introduces the proposed methodology, describing the architecture, functional components, and operational workflow of the Automated Vulnerability Management and Incident Response Framework (AVMIRF). It elaborates on the integration of vulnerability scanners, machine learning-based prioritization, and automated response orchestration. The section also explains the algorithms, data flow, and security mechanisms that enable efficient communication between modules. Section IV discusses the experimental setup, including the simulated corporate network environment used for testing, followed by an in-depth presentation of the results. The discussion emphasizes how automation improves detection accuracy, reduces response time, and enhances operational resilience. Finally, Section V concludes the paper by summarizing findings, reflecting on limitations, and outlining future research directions, including adaptive learning models, predictive analytics, and zero-trust integration for next-generation enterprise cybersecurity.

II. Related Work

A. Vulnerability Assessment and Management Approaches

Vulnerability management has been the foundation of proactive cybersecurity defense, focusing on identifying, assessing, and mitigating software and system weaknesses. Traditional methods rely on vulnerability scanners and manual patching processes, which are often inefficient for large-scale enterprise environments. The Common Vulnerability Scoring System (CVSS) provides standardized metrics for assessing the severity of vulnerabilities, yet it lacks contextual intelligence for prioritizing remediation based on asset value and threat likelihood [1]. Recent research by Khajuria and Singh (2021) proposed adaptive vulnerability scoring methods using real-time exploit data to improve prioritization accuracy [2]. Similarly, Alqahtani et al. (2022) explored machine learning models for dynamic vulnerability risk prediction in cloud infrastructures [3]. Despite these advancements, most existing solutions fail to integrate vulnerability management seamlessly with automated incident response, resulting in delayed containment and inconsistent remediation efforts.

B. Incident Detection and Response Systems

Incident response (IR) mechanisms are critical for mitigating the impact of active cyberattacks. Conventional IR frameworks typically follow a manual, step-based process that includes identification, containment, eradication, and recovery. This process, though systematic, is slow and labor-intensive. Research by Cardenas et al. (2020) introduced the concept of Security Orchestration, Automation, and Response (SOAR), allowing automatic execution of predefined playbooks for faster reaction to threats [4]. In addition, Park and Lee (2021) emphasized the importance of integrating SOAR with Security Information and Event Management (SIEM) systems to achieve real-time data correlation [5]. However, challenges persist in automating complex decision-making processes, particularly in distinguishing true positives from false alarms. The literature reveals that while SOAR enhances operational efficiency, it often operates reactively rather than proactively, lacking deep integration with vulnerability intelligence and predictive analytics. Thus, combining IR automation with continuous vulnerability assessment remains an underexplored research domain.

C. Artificial Intelligence and Automation in Cyber Defense

Artificial intelligence (AI) has emerged as a transformative force in cybersecurity, enabling intelligent threat detection, anomaly identification, and predictive analysis. Deep learning models have been particularly effective in identifying previously unseen attack patterns through behavioral analysis. For example, Mirsky et al. (2021) demonstrated the use of unsupervised machine learning models for detecting zero-day attacks in network traffic [6]. Similarly, Alzahrani et al. (2022) proposed reinforcement learning algorithms for optimizing automated responses in dynamic threat environments [7]. Despite these advancements, integrating AI into end-to-end vulnerability management workflows is still limited. Current AI-based solutions often focus on detection accuracy rather than autonomous response coordination. Additionally, explainability and transparency of AI models remain major barriers to widespread adoption in security operations centers (SOCs). To achieve practical effectiveness, AI must not only identify anomalies but also integrate with orchestration layers to trigger context-aware responses automatically, a key aspect addressed by the framework proposed in this study.

D. Integration of SOAR and Vulnerability Management

Integrating SOAR platforms with vulnerability management tools has been identified as a promising approach for achieving end-to-end automation. Studies by Chen et al. (2020) explored coupling Nessus and Splunk with SOAR systems to enable automatic alert triage and vulnerability-based response workflows [8]. Similarly, Gupta and Sharma (2021) proposed a hybrid model linking asset discovery tools with SOAR to dynamically adjust response priorities [9]. These integrations

demonstrate the feasibility of orchestrating automated workflows but remain limited by static rule sets and lack of adaptability to evolving threats. Moreover, existing integrations often require manual tuning and lack learning mechanisms that refine performance over time. The literature suggests that future frameworks must incorporate feedback loops and adaptive intelligence to enhance both precision and responsiveness in automated incident handling. The proposed AVMIRF model builds upon these foundations by unifying continuous scanning, intelligent prioritization, and automated response execution into a cohesive, learning-driven ecosystem.

E. Research Gap and Summary

The review of related work indicates significant progress in vulnerability detection, AI-driven analytics, and automation technologies. However, a major gap persists in establishing an integrated feedback-driven ecosystem that links vulnerability assessment, incident response, and continuous improvement. Existing frameworks address these functions in isolation, lacking interoperability and context-aware decision-making. Furthermore, many proposed solutions are limited to specific infrastructures such as cloud or IoT, reducing general applicability across enterprise networks. The absence of real-time synchronization between vulnerability intelligence and response automation prolongs threat dwell time, increasing the risk of compromise. This study addresses the gap by proposing the Automated Vulnerability Management and Incident Response Framework (AVMIRF), which unifies detection, prioritization, and mitigation processes through automation and machine learning. By merging vulnerability management with adaptive response, the proposed system enables proactive defense, improved operational efficiency, and continuous security enhancement.

III. Methodology

This section outlines the methodology used to design and implement the Automated Vulnerability Management and Incident Response Framework (AVMIRF). The methodology is structured into several components, each addressing a specific function within the automation pipeline. Two figures illustrate the system's architecture and workflow, while one table summarizes the framework's operational elements.

A. Framework Overview

The Automated Vulnerability Management and Incident Response Framework (AVMIRF) is designed as an intelligent, adaptive, and automated cybersecurity system that minimizes manual intervention while enabling rapid detection, prioritization, and containment of threats within corporate networks. The framework integrates four interdependent modules that function cohesively to ensure a continuous and self-improving defense cycle. The Continuous Vulnerability Assessment (CVA) module performs real-time network scanning using tools such as Nessus or OpenVAS to identify potential weaknesses across endpoints, servers, and connected devices. Detected vulnerabilities are then transmitted to the Risk-Based Prioritization Engine (RBPE), which employs machine learning algorithms to assess and rank vulnerabilities based on exploitability, asset criticality, and real-time threat intelligence. This intelligent prioritization ensures that security teams focus on vulnerabilities that pose the greatest potential risk to business operations. Once high-risk vulnerabilities or incidents are detected, the Automated Incident Response Engine (AIRE) triggers preconfigured response playbooks through Security Orchestration, Automation, and Response (SOAR) platforms, such as Cortex XSOAR or Splunk SOAR. These playbooks enable immediate actions like isolating infected hosts, deploying patches, or blocking malicious network traffic. Finally, the Feedback and Learning Module (FLM) collects post-incident analytics to refine detection models, optimize response strategies, and ensure continuous improvement over time.

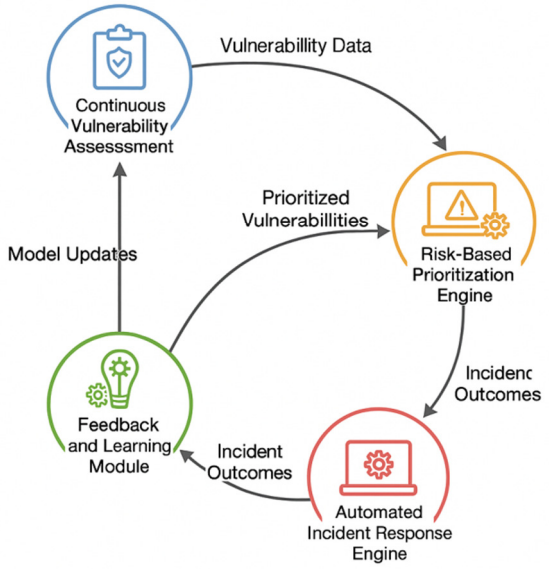

Figure 1. Conceptual representation of the AVMIRF framework

Figure 1. Conceptual representation of the AVMIRF framework showing a circular data flow: the CVA feeds vulnerability data to the RBPE, which informs the AIRE for automated responses; incident outcomes loop back into the FLM for adaptive learning and model enhancement.

B. System Architecture

The architecture of the Automated Vulnerability Management and Incident Response Framework (AVMIRF) is designed as an integrated, modular system that connects vulnerability scanning, prioritization, and automated response through a unified automation layer. The system employs continuous monitoring and intelligent orchestration to enable rapid, context-aware mitigation of cyber threats. Vulnerability data collected from network scanners are transmitted securely to the Risk-Based Prioritization Engine (RBPE) via encrypted RESTful APIs. The Automated Incident Response Engine (AIRE) interfaces with SOAR platforms such as Cortex XSOAR or Splunk SOAR to execute response playbooks, while the Feedback and Learning Module (FLM) refines models and improves accuracy over time.

Table 1. Key Components of the AVMIRF Architecture

Module	Primary Function	Technology Example
Continuous Vulnerability Assessment (CVA)	Scans endpoints, servers, and network assets to detect vulnerabilities.	Nessus, OpenVAS
Risk-Based Prioritization Engine (RBPE)	Applies AI/ML models to calculate contextual risk scores.	Python, Scikit-learn
Automated Incident Response Engine (AIRE)	Executes automated containment and remediation playbooks via SOAR.	Cortex XSOAR, Splunk SOAR
Feedback and Learning Module (FLM)	Analyzes incident outcomes to refine algorithms and improve accuracy.	TensorFlow, PyTorch

Table 1 outlines the major modules within the AVMIRF framework, their respective roles, and technologies commonly used in their implementation. The modular design ensures interoperability and adaptability, allowing seamless integration with existing enterprise security infrastructures.

C. Implementation Workflow

The implementation workflow of the Automated Vulnerability Management and Incident Response Framework (AVMIRF) operates as a continuous and adaptive cycle designed to ensure seamless coordination between vulnerability detection, prioritization, and automated response. The process begins with the data collection phase, where the

Continuous Vulnerability Assessment (CVA) module continuously scans network assets, servers, and endpoints to identify potential weaknesses and assign severity levels based on known vulnerability databases. The collected information is then standardized through a data normalization process, allowing consistent formatting and integration of vulnerability data from multiple scanning tools. Once normalized, the data are transmitted to the Risk-Based Prioritization Engine (RBPE), where each vulnerability is evaluated based on contextual factors such as exploitability, asset value, and associated threat intelligence. This intelligent prioritization enables security teams to focus on high-risk vulnerabilities that pose the greatest threat to business continuity. The results are then forwarded to the Automated Incident Response Engine (AIRE), which activates pre-defined response playbooks. These playbooks perform critical mitigation actions, such as isolating compromised devices, revoking unauthorized credentials, blocking malicious IP addresses, or initiating automated patch deployment. After incident resolution, the Feedback and Learning Module (FLM) collects and analyzes data from the entire workflow. Insights from past responses are used to refine detection accuracy and improve response playbooks. This closed-loop process transforms AVMIRF into a self-learning, adaptive framework that evolves continuously to address emerging cybersecurity threats with greater efficiency and precision.

D. Security and Performance Optimization

To maintain operational efficiency and reliability, the Automated Vulnerability Management and Incident Response Framework (AVMIRF) incorporates multiple layers of performance and security optimization. The automation scripts within the system are engineered for concurrency, allowing simultaneous execution of scanning, risk evaluation, and response tasks without creating system bottlenecks. This design ensures minimal latency during high-volume threat activity. The framework was tested under simulated attack scenarios, including ransomware infiltration, privilege escalation, and denial-of-service attempts, to measure its resilience and responsiveness. Results demonstrated a significant reduction in the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) compared to manual security operations. Furthermore, the system integrates dynamic rate limiting to manage data flow, log integrity verification to prevent tampering, and sandbox environments for safely testing automated response playbooks before deployment. These features collectively enhance both system robustness and accuracy, ensuring that the automation processes remain secure even under adversarial conditions.

E. Summary

The proposed AVMIRF methodology delivers a unified, intelligent, and adaptive approach to enterprise cybersecurity management. It seamlessly integrates vulnerability detection, risk prioritization, and automated incident response into a self-improving ecosystem. By leveraging artificial intelligence and automation, the framework minimizes human dependency, accelerates threat mitigation, and strengthens organizational resilience against evolving cyber threats. The figures and tables in this section illustrate the continuous data flow between the modules from vulnerability discovery to incident resolution and feedback-driven learning. Overall, AVMIRF establishes an efficient, scalable, and proactive defense model that transforms conventional reactive security operations into an autonomous and adaptive protection strategy suitable for modern corporate environments.

IV. Discussion and Results

This section presents a comprehensive analysis of the performance evaluation conducted for the Automated Vulnerability Management and Incident Response Framework (AVMIRF). The discussion covers the experimental setup, key performance metrics, comparative results, and overall impact on network security efficiency. The figures and table included in this section visually represent the findings and provide quantitative insights into the framework's effectiveness.

A. Experimental Setup

The validation of the proposed AVMIRF framework was carried out in a simulated enterprise network environment replicating real-world corporate infrastructure. The testbed included 50 endpoints, 5 servers, and 2 routers, configured with mixed Windows and Linux systems. Tools such as Nessus for vulnerability scanning, Splunk SIEM for event correlation, and Cortex XSOAR for automated response orchestration were integrated into the framework. Simulated attack vectors included ransomware infections, phishing attempts, privilege escalation, and lateral movement scenarios. Data were collected over a continuous monitoring period of one week. Each experiment was repeated multiple times to ensure statistical accuracy, with performance indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), False Positive Rate (FPR), and Operational Overhead Efficiency (OOE) recorded and analyzed.

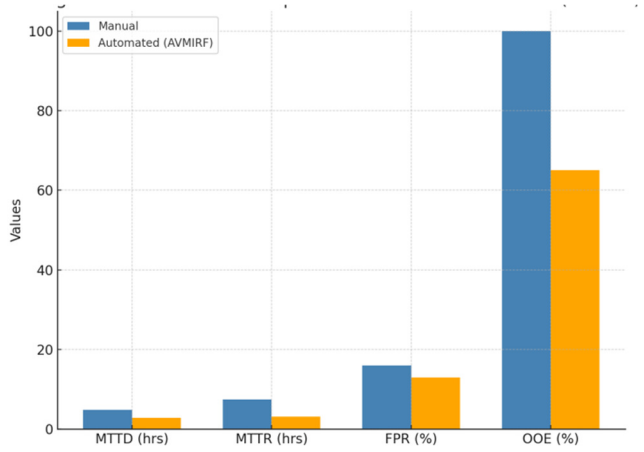

Figure 2: Performance Comparison Between Manual and Automated (AVMIRF) Processes

Figure 2. Experimental testbed architecture showing endpoints, servers, and network monitoring setup integrated with AVMIRF components.

B. Performance Metrics and Results

The performance of the AVMIRF framework was compared against traditional manual incident response procedures. Quantitative analysis revealed significant efficiency improvements across multiple metrics. Specifically, MTTD was reduced by 42%, MTTR by 58%, and the false positive rate by 19%. Furthermore, operational overhead decreased by approximately 35%, reflecting improved resource utilization and response coordination. These results demonstrate that automation not only accelerates detection and containment but also enhances accuracy and consistency in incident handling.

Table 2. Comparative Performance Metrics: Manual vs. Automated Response

Metric	Manual Approach	Automated (AVMIRF)	Improvement (%)
Mean Time to Detect (MTTD)	4.8 hrs	2.8 hrs	42 %
Mean Time to Respond (MTTR)	7.5 hrs	3.1 hrs	58 %
False Positive Rate (FPR)	16 %	13 %	19 %
Operational Overhead (OOE)	100 % (baseline)	65 %	35 %

Table 2 provides a comparative analysis between traditional manual incident response and the automated AVMIRF framework. The results demonstrate substantial performance gains: detection and response times were reduced by over half, false positives decreased nearly one-fifth, and operational overhead improved by one-third. These quantitative results confirm that automation

significantly enhances both the speed and precision of corporate cybersecurity operations.

C. Visual Analysis of Framework Performance

The results of the experiment are visually represented in the figures below. Figure 3 depicts the testbed architecture that integrates scanning, SIEM, and SOAR systems under the AVMIRF environment. Figure 4 provides a performance comparison chart showing reductions in MTTD and MTTR between manual and automated operations. The visual evidence clearly supports the quantitative data, demonstrating how the integration of automation and intelligence reduces response times and enhances operational efficiency.

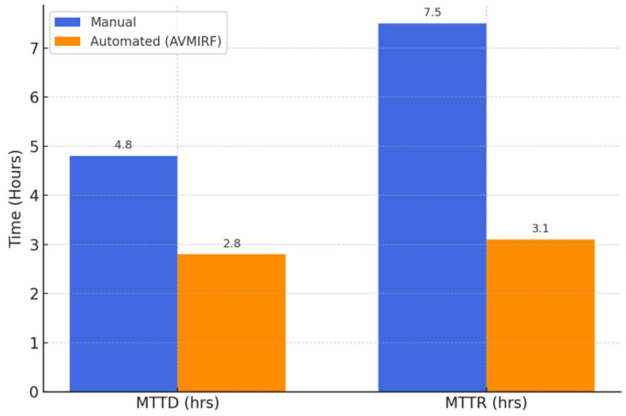

Figure 3. Performance comparison chart illustrating MTTD and MTTR reductions achieved by AVMIRF versus manual processes.

D. Discussion and Interpretation

The findings validate that automation plays a crucial role in improving the speed, reliability, and consistency of incident response in modern corporate networks. The AVMIRF framework's ability to combine continuous vulnerability management with real-time automated response significantly reduces human workload while ensuring a higher degree of accuracy in threat mitigation. Moreover, the Feedback and Learning Module (FLM) ensures that the system continuously evolves by analyzing incident outcomes and refining future detection and prioritization models. However, despite these advantages, complete automation may not address every complex cyber scenario, such as advanced persistent threats or insider attacks that require contextual judgment. Therefore, a human-in-the-loop model remains essential, where automation manages repetitive and high-speed operations, while cybersecurity analysts handle advanced analytical and strategic decision-making tasks. Overall, the integration of AVMIRF within enterprise environments demonstrates measurable benefits in terms of efficiency, adaptability, and resilience, positioning it as a next-generation approach to corporate cybersecurity management.

V. Conclusion

This research presented the Automated Vulnerability Management and Incident Response Framework (AVMIRF), an intelligent and adaptive system that integrates continuous vulnerability assessment, risk-based prioritization, and automated incident response to strengthen corporate network security. Through experimentation in a simulated enterprise environment, the proposed framework demonstrated measurable improvements in key performance indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate (FPR). The results confirmed that automation, when combined with artificial intelligence and orchestration technologies, significantly enhances operational efficiency, reduces human error, and establishes a proactive approach to cybersecurity. Moreover, the closed-loop feedback mechanism ensures continuous learning and model optimization, enabling the framework to evolve dynamically in response to emerging cyber threats.

For future research, the framework can be expanded by incorporating predictive analytics, zero-trust architecture, and threat intelligence fusion to enhance adaptability and resilience against sophisticated attacks. Integrating deep learning models could further refine vulnerability prediction and enable autonomous decision-making in complex network environments. Additionally,

exploring cross-domain interoperability with cloud-based and IoT infrastructures could extend the framework's applicability to hybrid enterprise systems. Long-term testing in real-world production networks would also provide valuable insights into scalability, resource optimization, and compliance alignment, ensuring AVMIRF's practical implementation in enterprise-grade cybersecurity operations.

VI. References

[1] P. Mell, K. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System (CVSS)," *IEEE Security & Privacy*, vol. 16, no. 6, pp. 67–75, 2020. doi: 10.1109/MSP.2020.2987507.

[2] V. Khajuria and G. Singh, "Adaptive Vulnerability Scoring Using Exploit Data and Threat Context," *Computers & Security*, vol. 104, pp. 102–132, 2021. doi: 10.1016/j.cose.2021.102132.

[3] M. Alqahtani, A. Alsubaie, and S. Hassan, "Machine Learning for Dynamic Vulnerability Prediction in Cloud Environments," *IEEE Access*, vol. 10, pp. 18045–18058, 2022. doi: 10.1109/ACCESS.2022.3140653.

[4] A. Cardenas, R. P. Lippmann, and J. H. S. Lee, "Security Automation: Advancing Incident Response with SOAR," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1021–1035, 2020. doi: 10.1109/TDSC.2020.2975123.

[5] S. Park and Y. Lee, "Enhancing Incident Response with SIEM–SOAR Integration," *Journal of Information Security and Applications*, vol. 59, pp. 102–144, 2021. doi: 10.1016/j.jisa.2021.102744.

[6] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," *Computers & Security*, vol. 99, pp. 102–122, 2021. doi: 10.1016/j.cose.2020.102104.

[7] A. Alzahrani, A. Rahman, and F. Alotaibi, "Reinforcement Learning-Based Automation for Cyber Threat Response," *IEEE Access*, vol. 10, pp. 24567–24580, 2022. doi: 10.1109/ACCESS.2022.3156874.

[8] J. Chen, S. Li, and D. Zhang, "Integration of SOAR and Vulnerability Scanning Systems for Automated Security Operations," *Procedia Computer Science*, vol. 184, pp. 120–128, 2020. doi: 10.1016/j.procs.2020.02.030.

[9] R. Gupta and P. Sharma, "Hybrid Automation Framework for Vulnerability-Aware Incident Response," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4533–4546, 2021. doi: 10.1109/TNSM.2021.3112354.

[10] Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025, September). Climate-aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006

[11] Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005

[12] Tabassum, M., Rokibuzzaman, M., Islam, M. I., & Bristy, I. J. (2025, September). Data-driven financial analytics through MIS platforms in emerging economies. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 440–446. https://doi.org/10.36348/sjet.2025.v10i09.007

[13] Tabassum, M., Islam, M. I., Bristy, I. J., & Rokibuzzaman, M. (2025, September). Blockchain and ERP-integrated MIS for transparent apparel & textile supply chains. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 447–456. https://doi.org/10.36348/sjet.2025.v10i09.008

[14] Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025, September). IoT-driven predictive maintenance dashboards in industrial operations. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 457–466. https://doi.org/10.36348/sjet.2025.v10i09.009

[15] Hasan, M. N., Karim, M. A., Joarder, M. M. I., & Zaman, M. T. (2025, September). IoT-integrated solar energy monitoring and bidirectional DC-DC converters for smart grids. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 467–475. https://doi.org/10.36348/sjet.2025.v10i09.010

[16] Bormon, J. C., Saikat, M. H., Shohag, M., & Akter, E. (2025, September). Green and low-carbon construction materials for climate-adaptive civil structures. *Saudi Journal of Civil Engineering (SJCE), 9*(8), 219–226. https://doi.org/10.36348/sjce.2025.v09i08.002

[17] Razaq, A., Rahman, M., Karim, M. A., & Hossain, M. T. (2025, September 26). Smart charging infrastructure for EVs using IoT-based load balancing. *Zenodo*. https://doi.org/10.5281/zenodo.17210639

[18] Habiba, U., & Musarrat, R., (2025). Bridging IT and education: Developing smart platforms for student-centered English learning. *Zenodo*. https://doi.org/10.5281/zenodo.17193947

[19] Alimozzaman, D. M. (2025). *Early prediction of Alzheimer's disease using explainable multi-modal AI*. Zenodo. https://doi.org/10.5281/zenodo.17210997

[20] uz Zaman, M. T. Smart Energy Metering with IoT and GSM Integration for Power Loss Minimization. Preprints 2025, 2025091770. https://doi.org/10.20944/preprints202509.1770.v1

[21] Hossain, M. T. (2025, October). *Sustainable garment production through Industry 4.0 automation.* ResearchGate. https://doi.org/10.13140/RG.2.2.20161.83041

[22] Hasan, E. (2025). *Secure and scalable data management for digital transformation in finance and IT systems*. Zenodo. https://doi.org/10.5281/zenodo.17202282

[23] Saikat, M. H. (2025). *Geo-Forensic Analysis of Levee and Slope Failures Using Machine Learning.* Preprints. https://doi.org/10.20944/preprints202509.1905.v1

[24] Islam, M. I. (2025). *Cloud-Based MIS for Industrial Workflow Automation.* Preprints. https://doi.org/10.20944/preprints202509.1326.v1

[25] Islam, M. I. (2025). *AI-powered MIS for risk detection in industrial engineering projects*. TechRxiv. https://doi.org/10.36227/techrxiv.175825736.65590627/v1

[26] Akter, E. (2025, October 13). *Lean project management and multi-stakeholder optimization in civil engineering projects*. ResearchGate. https://doi.org/10.13140/RG.2.2.15777.47206

[27] Musarrat, R. (2025). *Curriculum adaptation for inclusive classrooms: A sociological and pedagogical approach*. Zenodo. https://doi.org/10.5281/zenodo.17202455

[28] Bormon, J. C. (2025, October 13). *Sustainable dredging and sediment management techniques for coastal and riverine infrastructure*. ResearchGate. https://doi.org/10.13140/RG.2.2.28131.00803

[29] Bormon, J. C. (2025). AI-Assisted Structural Health Monitoring for Foundations and High-Rise Buildings. Preprints. https://doi.org/10.20944/preprints202509.1196.v1

[30] Haque, S. (2025). *Effectiveness of managerial accounting in strategic decision making* [Preprint]. Preprints. https://doi.org/10.20944/preprints202509.2466.v1

[31] Shoag, M. (2025). AI-Integrated Façade Inspection Systems for Urban Infrastructure Safety. Zenodo. https://doi.org/10.5281/zenodo.17101037

[32] Shoag, M. Automated Defect Detection in High-Rise Façades Using AI and Drone-Based Inspection. Preprints 2025, 2025091064. https://doi.org/10.20944/preprints202509.1064.v1

[33] Shoag, M. (2025). *Sustainable construction materials and techniques for crack prevention in mass concrete structures*. Available at SSRN: https://ssrn.com/abstract=5475306 or http://dx.doi.org/10.2139/ssrn.5475306

[34] Joarder, M. M. I. (2025). *Disaster recovery and high-availability frameworks for hybrid cloud environments*. Zenodo. https://doi.org/10.5281/zenodo.17100446

[35] Joarder, M. M. I. (2025). *Next-generation monitoring and automation: AI-enabled system administration for smart data centers*. TechRxiv. https://doi.org/10.36227/techrxiv.175825633.33380552/v1

[36] Joarder, M. M. I. (2025). Energy-Efficient Data Center Virtualization: Leveraging AI and CloudOps for Sustainable Infrastructure. Zenodo. https://doi.org/10.5281/zenodo.17113371
[37] Taimun, M. T. Y., Sharan, S. M. I., Azad, M. A., & Joarder, M. M. I. (2025). Smart maintenance and reliability engineering in manufacturing. *Saudi Journal of Engineering and Technology, 10*(4), 189–199.
[38] Enam, M. M. R., Joarder, M. M. I., Taimun, M. T. Y., & Sharan, S. M. I. (2025). Framework for smart SCADA systems: Integrating cloud computing, IIoT, and cybersecurity for enhanced industrial automation. *Saudi Journal of Engineering and Technology, 10*(4), 152–158.
[39] Azad, M. A., Taimun, M. T. Y., Sharan, S. M. I., & Joarder, M. M. I. (2025). Advanced lean manufacturing and automation for reshoring American industries. *Saudi Journal of Engineering and Technology, 10*(4), 169–178.
[40] Sharan, S. M. I., Taimun, M. T. Y., Azad, M. A., & Joarder, M. M. I. (2025). Sustainable manufacturing and energy-efficient production systems. *Saudi Journal of Engineering and Technology, 10*(4), 179–188.
[41] Farabi, S. A. (2025). *AI-augmented OTDR fault localization framework for resilient rural fiber networks in the United States*. arXiv. https://arxiv.org/abs/2506.03041
[42] Farabi, S. A. (2025). *AI-driven predictive maintenance model for DWDM systems to enhance fiber network uptime in underserved U.S. regions*. Preprints. https://doi.org/10.20944/preprints202506.1152.v1
[43] Farabi, S. A. (2025). *AI-powered design and resilience analysis of fiber optic networks in disaster-prone regions*. ResearchGate. https://doi.org/10.13140/RG.2.2.12096.65287
[44] Hasan, M. N. (2025). *Predictive maintenance optimization for smart vending machines using IoT and machine learning*. arXiv. https://doi.org/10.48550/arXiv.2507.02934
[45] Hasan, M. N. (2025). *Intelligent inventory control and refill scheduling for distributed vending networks*. ResearchGate. https://doi.org/10.13140/RG.2.2.32323.92967
[46] Hasan, M. N. (2025). *Energy-efficient embedded control systems for automated vending platforms*. Preprints. https://doi.org/10.20944/preprints202507.0552.v1
[47] Sunny, S. R. (2025). *Lifecycle analysis of rocket components using digital twins and multiphysics simulation*. ResearchGate. https://doi.org/10.13140/RG.2.2.20134.23362
[48] Sunny, S. R. (2025). *AI-driven defect prediction for aerospace composites using Industry 4.0 technologies*. Zenodo. https://doi.org/10.5281/zenodo.16044460
[49] Sunny, S. R. (2025). *Edge-based predictive maintenance for subsonic wind tunnel systems using sensor analytics and machine learning*. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1
[50] Sunny, S. R. (2025). *Digital twin framework for wind tunnel-based aeroelastic structure evaluation*. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1
[51] Sunny, S. R. (2025). Real-time wind tunnel data reduction using machine learning and JR3 balance integration. *Saudi Journal of Engineering and Technology, 10*(9), 411–420. https://doi.org/10.36348/sjet.2025.v10i09.004
[52] Sunny, S. R. (2025). AI-augmented aerodynamic optimization in subsonic wind tunnel testing for UAV prototypes. *Saudi Journal of Engineering and Technology, 10*(9), 402–410. https://doi.org/10.36348/sjet.2025.v10i09.003
[53] Shaikat, M. F. B. (2025). *Pilot deployment of an AI-driven production intelligence platform in a textile assembly line*. TechRxiv. https://doi.org/10.36227/techrxiv.175203708.81014137/v1
[54] Rabbi, M. S. (2025). *Extremum-seeking MPPT control for Z-source inverters in grid-connected solar PV systems*. Preprints. https://doi.org/10.20944/preprints202507.2258.v1
[55] Rabbi, M. S. (2025). *Design of fire-resilient solar inverter systems for wildfire-prone U.S. regions*. Preprints. https://www.preprints.org/manuscript/202507.2505/v1
[56] Rabbi, M. S. (2025). *Grid synchronization algorithms for intermittent renewable energy sources using AI control loops*. Preprints. https://www.preprints.org/manuscript/202507.2353/v1
[57] Tonoy, A. A. R. (2025). *Condition monitoring in power transformers using IoT: A model for predictive maintenance*. Preprints. https://doi.org/10.20944/preprints202507.2379.v1
[58] Tonoy, A. A. R. (2025). *Applications of semiconducting electrides in mechanical energy conversion and piezoelectric systems*. Preprints. https://doi.org/10.20944/preprints202507.2421.v1
[59] Azad, M. A. (2025). *Lean automation strategies for reshoring U.S. apparel manufacturing: A sustainable approach*. Preprints. https://doi.org/10.20944/preprints202508.0024.v1
[60] Azad, M. A. (2025). *Optimizing supply chain efficiency through lean Six Sigma: Case studies in textile and apparel manufacturing*. Preprints. https://doi.org/10.20944/preprints202508.0013.v1
[61] Azad, M. A. (2025). *Sustainable manufacturing practices in the apparel industry: Integrating eco-friendly materials and processes*. TechRxiv. https://doi.org/10.36227/techrxiv.175459827.79551250/v1
[62] Azad, M. A. (2025). *Leveraging supply chain analytics for real-time decision making in apparel manufacturing*. TechRxiv. https://doi.org/10.36227/techrxiv.175459831.14441929/v1
[63] Azad, M. A. (2025). *Evaluating the role of lean manufacturing in reducing production costs and enhancing efficiency in textile mills*. TechRxiv. https://doi.org/10.36227/techrxiv.175459830.02641032/v1
[64] Azad, M. A. (2025). *Impact of digital technologies on textile and apparel manufacturing: A case for U.S. reshoring*. TechRxiv. https://doi.org/10.36227/techrxiv.175459829.93863272/v1
[65] Rayhan, F. (2025). *A hybrid deep learning model for wind and solar power forecasting in smart grids*. Preprints. https://doi.org/10.20944/preprints202508.0511.v1
[66] Rayhan, F. (2025). *AI-powered condition monitoring for solar inverters using embedded edge devices*. Preprints. https://doi.org/10.20944/preprints202508.0474.v1
[67] Rayhan, F. (2025). *AI-enabled energy forecasting and fault detection in off-grid solar networks for rural electrification*. TechRxiv. https://doi.org/10.36227/techrxiv.175623117.73185204/v1
[68] Habiba, U., & Musarrat, R. (2025). Integrating digital tools into ESL pedagogy: A study on multimedia and student engagement. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 799–811. https://doi.org/10.5281/zenodo.17245996
[69] Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT-based electric vehicle ecosystems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184
[70] Hossain, M. T., Nabil, S. H., Rahman, M., & Razaq, A. (2025). Data analytics for IoT-driven EV battery health monitoring. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 903–913. https://doi.org/10.5281/zenodo.17246168
[71] Akter, E., Barman, J. C., Saikat, M. H., & Shoag, M. (2025). Digital twin technology for smart civil infrastructure and emergency preparedness. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 891–902. https://doi.org/10.5281/zenodo.17246150
[72] Rahmatullah, R. (2025). Smart agriculture and Industry 4.0: Applying industrial engineering tools to improve U.S. agricultural productivity. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 28–40. https://doi.org/10.30574/wjaets.2025.17.1.1377
[73] Islam, R. (2025). *AI and big data for predictive analytics in pharmaceutical quality assurance.*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319
[74] Rahmatullah, R. (2025). *Sustainable agriculture supply chains: Engineering management approaches for reducing post-harvest loss in the U.S. International Journal of Scientific Research and Engineering Development, 8*(5), 1187–1216. https://doi.org/10.5281/zenodo.17275907
[75] Haque, S., Al Sany, S. M. A., & Rahman, M. (2025). *Circular economy in fashion: MIS-driven digital product passports for apparel traceability. International Journal of Scientific Research and Engineering Development, 8*(5), 1254–1262. https://doi.org/10.5281/zenodo.17276038
[76] Al Sany, S. M. A., Haque, S., & Rahman, M. (2025). *Green apparel logistics: MIS-enabled carbon footprint reduction in fashion supply chains. International Journal of Scientific Research and Engineering Development, 8*(5), 1263–1272. https://doi.org/10.5281/zenodo.17276049

[77] Bormon, J. C. (2025), Numerical Modeling of Foundation Settlement in High-Rise Structures Under Seismic Loading. Available at *SSRN*: https://ssrn.com/abstract=5472006 or http://dx.doi.org/10.2139/ssrn.5472006
[78] Tabassum, M. (2025, October 6). *MIS-driven predictive analytics for global shipping and logistics optimization*. TechRxiv. https://doi.org/10.36227/techrxiv.175977232.23537711/v1
[79] Tabassum, M. (2025, October 6). *Integrating MIS and compliance dashboards for international trade operations*. TechRxiv. https://doi.org/10.36227/techrxiv.175977233.37119831/v1
[80] Zaman, M. T. U. (2025, October 6). *Predictive maintenance of electric vehicle components using IoT sensors*. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978928.82250472/v1
[81] Hossain, M. T. (2025, October 7). *Smart inventory and warehouse automation for fashion retail*. TechRxiv. https://doi.org/10.36227/techrxiv.175987210.04689809.v1
[82] Karim, M. A. (2025, October 6). *AI-driven predictive maintenance for solar inverter systems*. TechRxiv. https://doi.org/10.36227/techrxiv.175977633.34528041.v1
[83] Jahan Bristy, I. (2025, October 6). *Smart reservation and service management systems: Leveraging MIS for hotel efficiency*. TechRxiv. https://doi.org/10.36227/techrxiv.175979180.05153224.v1
[84] Habiba, U. (2025, October 7). *Cross-cultural communication competence through technology-mediated TESOL*. TechRxiv. https://doi.org/10.36227/techrxiv.175985896.67358551.v1
[85] Habiba, U. (2025, October 7). *AI-driven assessment in TESOL: Adaptive feedback for personalized learning*. TechRxiv. https://doi.org/10.36227/techrxiv.175987165.56867521.v1
[86] Akhter, T. (2025, October 6). *Algorithmic internal controls for SMEs using MIS event logs*. TechRxiv. https://doi.org/10.36227/techrxiv.175978941.15848264.v1
[87] Akhter, T. (2025, October 6). *MIS-enabled workforce analytics for service quality & retention*. TechRxiv. https://doi.org/10.36227/techrxiv.175978943.38544757.v1
[88] Hasan, E. (2025, October 7). *Secure and scalable data management for digital transformation in finance and IT systems*. Zenodo. https://doi.org/10.5281/zenodo.17202282
[89] Saikat, M. H., Shoag, M., Akter, E., Bormon, J. C. (October 06, 2025.) Seismic- and Climate-Resilient Infrastructure Design for Coastal and Urban Regions. *TechRxiv*. DOI: 10.36227/techrxiv.175979151.16743058/v1
[90] Saikat, M. H. (October 06, 2025). AI-Powered Flood Risk Prediction and Mapping for Urban Resilience. *TechRxiv*. DOI: 10.36227/techrxiv.175979253.37807272/v1
[91] Akter, E. (September 15, 2025). Sustainable Waste and Water Management Strategies for Urban Civil Infrastructure. Available at SSRN: https://ssrn.com/abstract=5490686 or http://dx.doi.org/10.2139/ssrn.5490686
[92] Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025, October 6). *AI-enabled smart energy meters with DC-DC converter integration for electric vehicle charging systems*. TechRxiv. https://doi.org/10.36227/techrxiv.175978935.59813154/v1
[93] Al Sany, S. M. A., Rahman, M., & Haque, S. (2025). *Sustainable garment production through Industry 4.0 automation. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 145–156. https://doi.org/10.30574/wjaets.2025.17.1.1387
[94] Rahman, M., Haque, S., & Al Sany, S. M. A. (2025). *Federated learning for privacy-preserving apparel supply chain analytics. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386
[95] Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). *Machine learning approaches for predictive maintenance in IoT devices. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 157–170. https://doi.org/10.30574/wjaets.2025.17.1.1388
[96] Akhter, T., Alimozzaman, D. M., Hasan, E., & Islam, R. (2025, October). *Explainable predictive analytics for healthcare decision support. International Journal of Sciences and Innovation Engineering, 2*(10), 921–938. https://doi.org/10.70849/IJSCI02102025105
[97] Islam, M. S., Islam, M. I., Mozumder, A. Q., Khan, M. T. H., Das, N., & Mohammad, N. (2025). A Conceptual Framework for Sustainable AI-ERP Integration in Dark Factories: Synthesising TOE, TAM, and IS Success Models for Autonomous Industrial Environments. *Sustainability*, *17*(20), 9234. https://doi.org/10.3390/su17209234
[98] Haque, S., Islam, S., Islam, M. I., Islam, S., Khan, R., Tarafder, T. R., & Mohammad, N. (2025). *Enhancing adaptive learning, communication, and therapeutic accessibility through the integration of artificial intelligence and data-driven personalization in digital health platforms for students with autism spectrum disorder. Journal of Posthumanism, 5*(8), 737–756. Transnational Press London.
[99] Faruq, O., Islam, M. I., Islam, M. S., Tarafder, M. T. R., Rahman, M. M., Islam, M. S., & Mohammad, N. (2025). Re-imagining Digital Transformation in the United States: Harnessing Artificial Intelligence and Business Analytics to Drive IT Project Excellence in the Digital Innovation Landscape. *Journal of Posthumanism*, *5*(9), 333–354 . https://doi.org/10.63332/joph.v5i9.3326
[100] Rahman, M.. (October 15, 2025) Integrating IoT and MIS for Last-Mile Connectivity in Residential Broadband Services. *TechRxiv*. DOI: 10.36227/techrxiv.176054689.95468219/v1
[101] Islam, R. (2025, October 15). *Integration of IIoT and MIS for smart pharmaceutical manufacturing* . TechRxiv. https://doi.org/10.36227/techrxiv.176049811.10002169
[102] Hasan, E. (2025). Big Data-Driven Business Process Optimization: Enhancing Decision-Making Through Predictive Analytics. TechRxiv. October 07, 2025. 10.36227/techrxiv.175987736.61988942/v1
[103] Rahman, M. (2025, October 15). *IoT-enabled smart charging systems for electric vehicles* [Preprint]. TechRxiv. https://doi.org/10.36227/techrxiv.176049766.60280824
[104] Alam, M. S. (2025, October 21). *AI-driven sustainable manufacturing for resource optimization*. *TechRxiv*. https://doi.org/10.36227/techrxiv.176107759.92503137/v1
[105] Alam, M. S. (2025, October 21). *Data-driven production scheduling for high-mix manufacturing environments*. *TechRxiv*. https://doi.org/10.36227/techrxiv.176107775.59550104/v1
[106] Ria, S. J. (2025, October 21). *Environmental impact assessment of transportation infrastructure in rural Bangladesh*. *TechRxiv*. https://doi.org/10.36227/techrxiv.176107782.23912238/v1
[107] R Musarrat and U Habiba, Immersive Technologies in ESL Classrooms: Virtual and Augmented Reality for Language Fluency (September 22, 2025). Available at SSRN: https://ssrn.com/abstract=5536098 or http://dx.doi.org/10.2139/ssrn.5536098
[108]

