Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

Intelligent Batch-Patch Automation for AI-Based Malware Detection and Vulnerability Response in Cyber Defense Systems for Operating System

Original Research Article | Volume 1 | Issue 4 | 2026 | Article Number: 025

Accepted: 27 August 2026 | Published: 10 September 2026 | ISSN: 2979-8582 (Online)

Crossref : **https://doi.org/10.67693/BJCR-L4ZQTMY9**

Daniel Paul Godwin[1], Oludele Awodele[1], Omofoye Modupe Ruth[1], Fabiyi Oluwatosin Amoke[1], Jumoke Eluwa[1]

[1]Babcock University, Illasan Ogun State, Nigeria

DPG 0009-0002-6601-0132, **OA** 0000-0002-9317-9868, **OMR** 0009-0001-5903-7671, **FOA** 0009-0003- 2441-0071

Correspondence: Daniel Paul Godwin, daniel0966@pg.babcock.edu.ng

Abstract

The rapid advancement of digital technologies has created significant opportunities but has also exposed vulnerabilities, leading to an increase in sophisticated cyber threats. This study explores the application of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity as a response to these challenges. The research identifies key gaps in traditional cybersecurity measures, including limitations in detecting and responding to evolving threats through batch-patch resources. Using a literature review and simulation-based methodology, scholarly evidence was synthesized to analyze the effectiveness of AI and ML tools. The findings reveal that AI-powered solutions can enhance threat detection, automate responses, and improve predictive capabilities using Large Action Models (LAMs), which bridge understanding with action by executing tasks through system-level operations. However, challenges such as data privacy concerns, adversarial AI, explainability, and resource constraints persist. The study recommends investing in workforce training, improving adversarial resilience, and adopting adaptive cyber-defense frameworks. This manuscript concludes that AI and ML hold transformative potential in cybersecurity, but their adoption requires a balanced approach supported by measurable evaluation metrics, adaptive vulnerability management, and continuous model improvement.

Keywords: LAM, Window Command Scripting, Cybersecurity, Artificial Intelligence, Machine Learning, Threat Detection for “@echo off” Execution

1. Introduction

Cybersecurity has become a fundamental aspect of modern digital infrastructures due to the increasing number of cyber threats targeting individuals, organizations, and governments. As technology continues to advance, so do the tactics and sophistication of cybercriminals, necessitating the development of more advanced security mechanisms. Traditional security measures such as firewalls, antivirus programs, and rule-based intrusion detection systems (IDS) have proven inadequate in countering sophisticated cyberattacks, leading to the integration of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity solutions.

AI and ML have transformed the cybersecurity landscape by enabling automated detection, response, and prediction of cyber threats, while also supporting behavioural analysis and pattern recognition. These technologies provide a proactive approach by analyzing vast amounts of security data, identifying anomalies, and mitigating risks before they escalate. Prior studies show that machine-learning and data-mining techniques are widely applied to cyber intrusion detection, anomaly detection, malware analysis, and security analytics (Buczak & Guven, 2016; Saxe & Berlin, 2015). Furthermore, adversarial-machine-learning research demonstrates that AI-based security systems must be designed carefully because models can be manipulated through adversarial examples (Goodfellow, Shlens, & Szegedy, 2015).

The role of ML in cybersecurity has also expanded beyond detection and response to include predictive analytics, adaptive anomaly detection, and automated decision support. Survey evidence indicates that anomaly-based techniques are useful for identifying previously unseen attacks, although they may introduce false-positive challenges that require careful model evaluation and continuous retraining (Buczak & Guven, 2016). Deep-learning approaches have also shown promise for malware detection, including detection of previously unseen malware families when trained on large-scale binary datasets (Saxe & Berlin, 2015).

This study explores the impact of AI and ML in cybersecurity, focusing on their effectiveness in intrusion detection, threat mitigation, and incident response. The research aims to analyze the challenges and opportunities associated with AI-driven cybersecurity solutions and assess their real-world applicability in protecting digital assets.

2. Problem Statement

The increasing sophistication of cyber threats, including zero-day attacks, ransomware, phishing scams, malware injection, and unauthorized access attempts, has exposed the limitations of traditional security approaches. Prior cybersecurity research shows that conventional intrusion-detection and rule-based security systems often struggle with unknown attacks, adaptive adversaries, high false-positive rates, and rapidly changing attack behaviours (Buczak & Guven, 2016; Sommer & Paxson, 2010). Many organizations therefore struggle to detect and respond to evolving threats in real time, leading to data breaches, financial losses, operational disruption, and reputational damage. AI and ML offer promising solutions for enhancing cybersecurity defenses through anomaly detection, malware classification, phishing detection, automated incident response, and vulnerability prioritization (Buczak & Guven, 2016; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026). However, challenges such as data privacy, model interpretability, adversarial attacks, computational cost, and deployment reliability remain significant concerns for AI-driven cybersecurity systems (Goodfellow et al., 2015; Sommer & Paxson, 2010; Saxe & Berlin, 2015). This study aims to investigate the capabilities and limitations of AI and ML in cybersecurity, addressing their effectiveness in real-world and simulation-based security scenarios.

3. Literature Review

Previous researchers examined and provided an analytic review of existing literature based on application of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity. The focus is on their roles in intrusion detection, threat mitigation, and response automation. The review highlights key studies, methodologies, and findings that contribute to the development of AI-driven cybersecurity systems, for batch and patch resources integration to protect against intrusion, for creating a deception for threat attack.

As cyber threats continue to evolve in complexity, traditional security methods struggle to keep up with sophisticated attack vectors. AI and ML have become essential tools in enhancing cybersecurity by providing automated detection, response, and predictive capabilities. These technologies analyze vast amounts of data to identify anomalies and patterns that indicate potential security breaches. Active cyber-defense literature also emphasizes the value of deception, adaptive response, and continuous monitoring in strengthening cyber resilience (Zhang & Thing, 2021).

The application of AI in cybersecurity extends across various domains, including network security, endpoint protection, fraud detection, identity management, phishing detection, and vulnerability management. With the rise of zero-day attacks and adversarial AI threats, security solutions must incorporate adaptive and self-learning models to counteract emerging risks effectively. Recent systematic reviews show that ML and neural-network techniques are widely used for phishing detection across websites, email, social platforms, and malware-related delivery channels, while AI-powered vulnerability management can improve detection precision, prioritization, scalability, and response speed (Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026).

Furthermore, AI and ML-based cybersecurity solutions help organizations shift from a reactive approach to a proactive defense strategy. These technologies not only detect and respond to known threats but also predict emerging attack patterns by leveraging historical attack data and behavioral analytics. However, the literature also emphasizes that AI-enabled security systems must be evaluated using measurable indicators such as detection rate, false-positive rate, robustness, scalability, and adaptability (Buczak & Guven, 2016; Goodfellow et al., 2015).

A. Cybersecurity Threat Landscape

The increasing complexity of cyber threats has necessitated advanced security measures beyond traditional approaches. Current cybersecurity literature shows that organizations face a broad threat landscape involving social engineering, malware, ransomware, denial-of-service attacks, zero-day exploits, adversarial AI manipulation, and intrusion attempts that require adaptive detection and response mechanisms (Buczak & Guven, 2016; Sommer & Paxson, 2010; Goodfellow et al., 2015; Wilk-Jakubowski et al., 2025).

i. **Phishing Attacks:** Social engineering tactics used to obtain sensitive user information, often through deceptive websites, emails, social platforms, and malware-related delivery channels (Wilk-Jakubowski et al., 2025).
ii. **Malware & Ransomware** – Malicious software designed to compromise system integrity, steal information, disrupt operations, or encrypt resources for extortion; deep-learning malware research shows that AI can support malware classification and detection when trained on appropriate binary and behavioural features (Saxe & Berlin, 2015).
iii. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks**: Attacks that overload networks, applications, or services to disrupt availability and normal operations; intrusion-detection research identifies such traffic anomalies as important targets for network-based

detection systems (Buczak & Guven, 2016; Sommer & Paxson, 2010).

iv. **Zero-Day Exploits**: Attacks targeting vulnerabilities before they are publicly known and patched. Anomaly-based and adaptive ML approaches can help identify previously unseen behaviours, although false positives and feature-selection limitations remain significant challenges (Buczak & Guven, 2016; Sommer & Paxson, 2010).

v. **Adversarial AI Attacks:** Techniques designed to mislead or manipulate AI models through adversarial inputs, thereby causing misclassification or weakening security decisions (Goodfellow et al., 2015).

vi. **IDS**: Intrusion Detection Systems monitor network or host activity to identify suspicious traffic, malicious URLs, abnormal behaviours, and web-based intrusion attempts; however, ML-based IDS must address false positives, dataset limitations, and deployment challenges (Buczak & Guven, 2016; Sommer & Paxson, 2010).

Studies on machine learning for intrusion detection emphasize that anomaly-based approaches can support the discovery of novel and zero-day attacks, but they must be balanced against high false-alarm risks and the need for robust feature selection (Buczak & Guven, 2016).

B. Role of AI and ML in Cybersecurity

AI and ML have emerged as critical tools in modern cybersecurity strategies because they support anomaly detection, malware classification, phishing detection, vulnerability prioritization, and automated incident response across large-scale security datasets (Buczak & Guven, 2016; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026; Ren et al., 2025). Their capabilities include:

i. **Anomaly Detection** – Identifying deviations from normal behaviour to detect potential threats, especially unknown or previously unseen attacks, while requiring careful feature selection and false-positive control (Buczak & Guven, 2016; Sommer & Paxson, 2010).

ii. **Threat Prediction** – Using historical data, behavioural analytics, phishing indicators, malware features, and vulnerability intelligence to forecast and mitigate future cyberattacks (Buczak & Guven, 2016; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026).

iii. **Automated Incident Response:** Reducing response time by autonomously selecting, prioritizing, and optimizing security actions such as blocking, isolation, escalation, and policy adjustment (Ren et al., 2025; Zhang & Thing, 2021).

Table 1: Summary of ML model, Application, Strengths and Weaknesses

ML Model	Application in Cybersecurity	Strengths	Weaknesses
Decision Trees & Random Forest	Intrusion detection and known-threat classification (Buczak & Guven, 2016)	High accuracy and interpretability for known patterns (Buczak & Guven, 2016)	Vulnerable to overfitting and dataset bias (Buczak & Guven, 2016)
K-Means Clustering	Anomaly detection and clustering of unusual traffic patterns (Buczak	Useful for identifying unknown or previously unseen behaviours	Can produce high false positives in open-world IDS

	& Guven, 2016; Sommer & Paxson, 2010)	(Buczak & Guven, 2016)	settings (Sommer & Paxson, 2010)
CNN & LSTM	Malware classification and sequential threat analysis (Saxe & Berlin, 2015)	Effective for large binary and behavioural datasets (Saxe & Berlin, 2015)	Computationally expensive and less interpretable (Saxe & Berlin, 2015; Sommer & Paxson, 2010)
Q-Learning & DQN	Automated threat response and policy optimization (Ren et al., 2025)	Adapts response policies to evolving attack conditions (Ren et al., 2025)	Requires extensive training and careful reward design (Ren et al., 2025)

Research studies indicate that hybrid and layered approaches combining multiple ML techniques can improve cybersecurity detection and response, particularly when supported by careful preprocessing, feature engineering, and evaluation against realistic attack scenarios (Buczak & Guven, 2016; Sommer & Paxson, 2010).

C. Challenges in AI-Driven Cybersecurity

Despite its advantages, AI-driven cybersecurity faces several challenges:

i. **Data Privacy Concerns** – The need for large security datasets creates privacy, governance, and compliance risks when sensitive user, network, or endpoint data are used for AI training (Buczak & Guven, 2016).
ii. **Adversarial AI** – Attackers may manipulate AI models through adversarial inputs, causing misclassification and reducing model reliability (Goodfellow et al., 2015).
iii. **Computational Costs** – Deep-learning and large-scale security analytics can require significant processing capacity, especially for malware classification, traffic analysis, and real-time endpoint monitoring (Saxe & Berlin, 2015).
iv. **Explainability Issues** – AI decisions are often difficult to interpret, which can limit trust, accountability, and operational adoption in high-risk cybersecurity environments (Sommer & Paxson, 2010; Buczak & Guven, 2016).

Summary of Findings The literature review underscores the transformative impact of AI and ML in cybersecurity, particularly in intrusion detection, malware classification, phishing detection, vulnerability management, automated response, and adaptive defense (Buczak & Guven, 2016; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026; Ren et al., 2025).

i. **AI enhances detection rates** for cyber threats by supporting anomaly detection, intrusion detection, malware classification, phishing analysis, and automated security analytics, thereby reducing reliance on manual intervention (Buczak & Guven, 2016; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025).
ii. **ML models improve adaptability** to new and evolving threats by enabling anomaly-based discovery, continuous retraining, reinforcement-learning-based response optimization, and vulnerability prioritization (Buczak & Guven, 2016; Sommer & Paxson, 2010; Ren et al., 2025;

Malkawi & Alhajj, 2026).

iii. **Challenges such as adversarial AI and data privacy** must be addressed for optimal security implementation because adversarial examples can mislead AI models, while large-scale security datasets raise privacy, governance, explainability, and deployment concerns (Goodfellow et al., 2015; Buczak & Guven, 2016; Sommer & Paxson, 2010).

The next chapter will present the research methodology used to evaluate AI-driven cybersecurity models.

Table 2: Review of Related Studies

Author(s)	Objective	Methodology	Results	Gaps	Improvement Suggestions
Zhang & Thing (2021)	To review deception techniques and active cyber-defense strategies	Retrospective review and outlook	Deception can strengthen active cyber defense when integrated with monitoring and response	Requires stronger integration with automated response workflows	Combine deception, AI detection, and adaptive mitigation
Goodfellow et al. (2015)	Study adversarial ML vulnerabilities	Experimentation with adversarial examples	AI models are susceptible to adversarial attacks	Lack of real-world test cases	Enhance robustness with adversarial training
Sommer & Paxson (2010)	Evaluate ML models for Intrusion Detection Systems (IDS)	Survey of ML algorithms	ML-based IDS offer better detection	High false positive rate	Improve feature selection methods
Ren et al. (2025)	Optimize automated cybersecurity incident-response strategies	Adaptive reinforcement-learning framework	Reinforcement learning can improve response optimization	Limited real-time implement-ation	Deploy AI in real-world settings
Saxe & Berlin (2015)	Study deep-learning-based malware detection	Deep neural network model	Deep learning supports malware classification	Susceptible to evolving spam techniques	Implement dynamic learning models

Buczak & Guven (2016)	Survey ML techniques in cybersecurity	Literature review	ML enhances anomaly detection	Lack of standard evaluation criteria	Develop a unified benchmarking framework
Saxe & Berlin (2015)	Study AI in static malware analysis	Deep learning approach	Deep learning is highly effective	Difficulty in interpreting results	Improve explainability of models

D. Novelty and Research Contribution

The novelty of this study lies in its integration of AI-driven threat intelligence with an adaptive batch-patch operating-system execution layer for proactive malware and vulnerability response. Existing AI cybersecurity studies commonly focus on threat detection, malware classification, anomaly recognition, intrusion detection, or predictive analytics as separate functions. In contrast, this research proposes a connected framework in which AI/ML outputs are translated into executable operating-system-level actions through Windows Command Scripting and batch-patch automation. This action-oriented direction is consistent with recent Large Action Model research, which positions AI agents as systems that move beyond language understanding into tool use, environment interaction, and task execution (Zhang et al., 2025; Wang et al., 2024).

Compared with existing automated incident-response studies, the proposed framework emphasizes a closed-loop response mechanism. Rather than stopping at AI-based recommendation or Security Operations Center alert automation, the framework links detection, decision support, operating-system scanning, DNS/IP/MAC inspection, process monitoring, patch validation, mitigation, and feedback learning. This closed-loop design allows the system to detect threats, trigger appropriate response actions, record the outcome, and improve future responses through retraining and policy refinement.

Compared with AI-powered patch-management studies, this research extends the role of patching from scheduled vulnerability remediation to adaptive cyber-defense execution. The proposed batch-patch layer is not limited to identifying missing updates or recommending patches; it is positioned as an execution bridge that supports real-time threat scanning, suspicious connection analysis, process-level inspection, phishing-related DNS review, and automated mitigation support. Recent AI-powered vulnerability-management literature confirms that AI can support vulnerability detection, prioritization, patch suggestion, and response acceleration, but also identifies gaps in benchmark standardization, adversarial testing, transparency, and real-world generalizability (Malkawi & Alhajj, 2026). Therefore, the contribution of this study is not simply the use of AI for patch prioritization, but the integration of AI, batch scripting, patch validation, and response automation into one operational architecture.

The main contributions of the study are therefore fourfold: first, it proposes an AI-driven adaptive batch-patch architecture that connects detection, analysis, execution, mitigation, and feedback learning; second, it introduces Windows Command Scripting as an operating-system-level automation layer for translating AI/ML decisions into actionable security operations, supported by command-shell automation concepts in Windows environments and by security research showing that command interpreters and scripting interfaces are widely used for both administration and adversarial execution (Gavade et al., 2024; MITRE ATT&CK, 2026); third, it evaluates the framework using measurable cybersecurity indicators such as detection rate, prevention rate, false-positive rate, response time, and adaptability; and fourth, it

demonstrates how proactive malware, phishing, unauthorized-access, and zero-day response can be strengthened by combining AI intelligence with executable batch-patch cyber-defense logic.

4. Objectives of the Study

The main aim of this study is to develop an AI and ML-based cybersecurity framework for enhance countering of intrusion detection and prevention of phishing and unauthorized network access in cyber-physical environment.The objectives of this study are enumerated as follows:

1. To develop an embedded encryption algorithm to enhance the use of ML in cybersecurity defenses (phishing scanning) using **Windows Command Scripting, WCS**.
2. To assess the potential of AI in automating security operations and enhancing threat intelligence using integration of echo-off scripting, CMD for OS, IP, Network, **Virus Scan.**
3. To evaluate the efficiency and accuracy of AI and ML models in identifying cyber threats by automatic blocking of IP/MAC and automated deletion of threats.
4. To test the effectiveness for phishing (threat) on a remote cloud system network & non cloud system network.

5. Significance of the Study

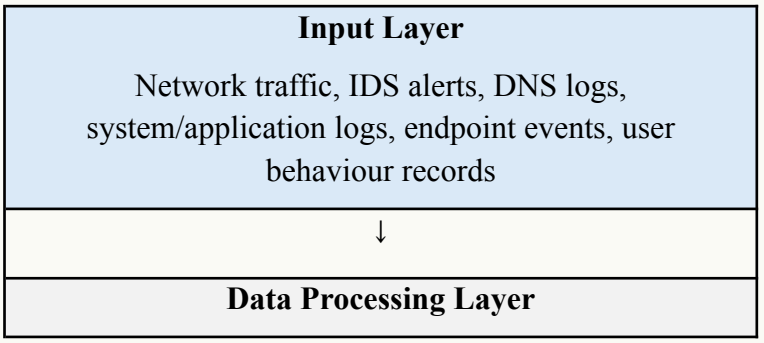
The study contributes to the growing field of AI-driven cybersecurity by presenting a framework that combines AI/ML-based threat intelligence with adaptive batch-patch operating-system automation. Unlike studies that treat AI detection, automated incident response, and patch management as separate cybersecurity functions, this study connects them within one proactive defense architecture. The findings will benefit cybersecurity professionals, researchers, and organizations seeking to reduce response delays, improve malware and phishing detection, strengthen vulnerability response, and operationalize AI decisions through executable security actions. The study also highlights the need to address challenges such as data privacy, adversarial AI, explainability, false positives, and resource constraints to ensure reliable deployment of AI-powered cyber-defense systems.

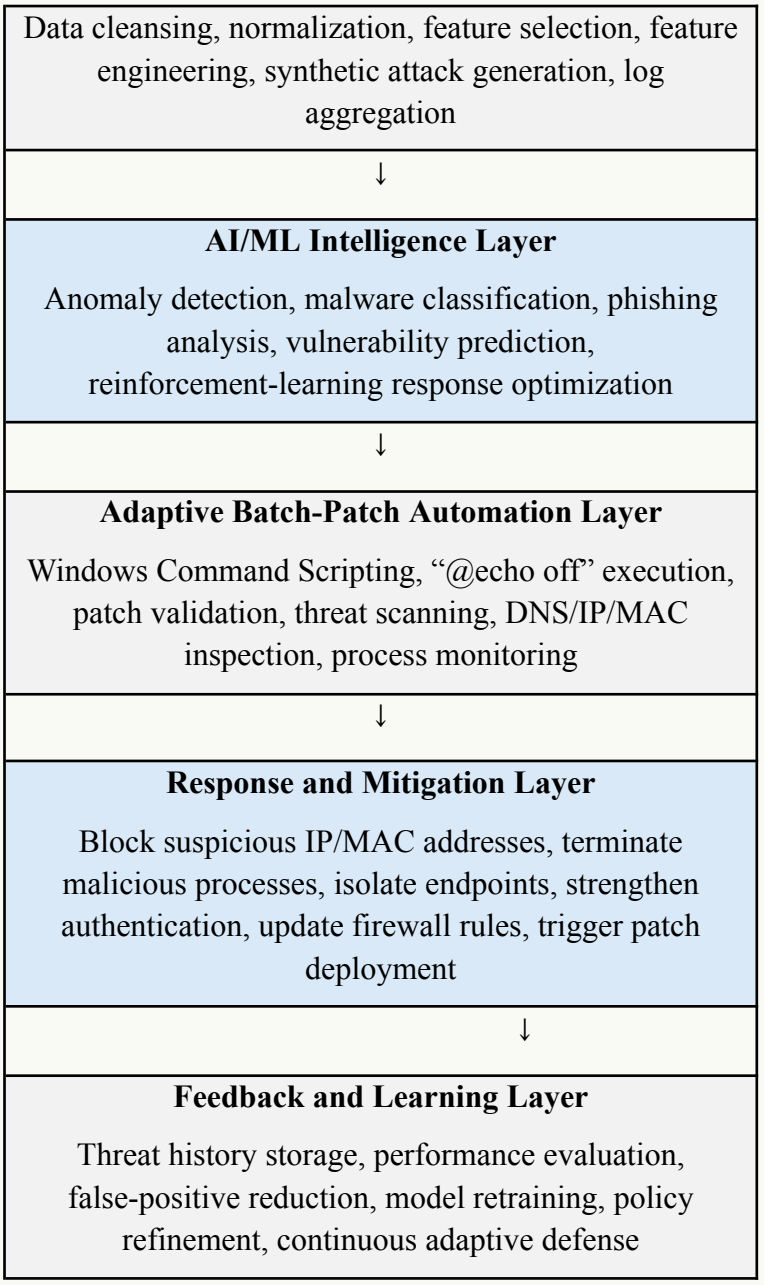
6. Scope of the Study

This research focuses on AI and ML applications in cybersecurity, particularly in intrusion detection, anomaly detection, and automated threat response. The study examines AI-based security frameworks, their advantages, and their potential vulnerabilities. While the research primarily explores AI-driven solutions, it also considers hybrid approaches that integrate traditional security measures with AI technologies **Structure of the Thesis** This thesis is organized as follows:

7. Details Methodology

Figure 1: Proposed AI-Driven Adaptive Batch-Patch System Architecture





The proposed architecture shows how raw security events are collected from network, endpoint, DNS, IDS, and user-behaviour sources, then processed into structured features for AI/ML analysis, consistent with cybersecurity ML workflows that emphasize log aggregation, preprocessing, feature engineering, and anomaly detection (Buczak & Guven, 2016; Sommer & Paxson, 2010). The intelligence layer identifies anomalies, malware patterns, phishing indicators, and vulnerability risks using AI/ML techniques supported by prior work on malware detection, phishing detection, and AI-powered vulnerability management (Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026). The adaptive batch-patch automation layer translates AI decisions into executable operating-system actions through Windows Command Scripting, reflecting command-line automation and Windows command-shell security concepts (Gavade et al., 2024; MITRE ATT&CK, 2026). The response layer performs mitigation activities such as blocking suspicious IP/MAC addresses, terminating malicious processes, isolating endpoints, strengthening authentication, and initiating patch deployment, which aligns with automated incident-response and active cyber-defense literature (Ren et al., 2025; Zhang & Thing, 2021). Finally, the feedback layer records threat history and model performance to support retraining, reduce false positives, and improve proactive cyber-defense decisions over time, consistent with adaptive learning and

continuous-evaluation requirements in AI-enabled cybersecurity systems (Buczak & Guven, 2016; Goodfellow et al., 2015; Ren et al., 2025).

This section presents the methodology used to design, implement, and evaluate the proposed AI-driven adaptive batch-patch cybersecurity framework. The study adopts a design-and-simulation research approach in which AI/ML models, Windows Command Scripting automation, IDS alerts, endpoint logs, DNS records, network traffic, and user-behaviour data are integrated into a layered threat-management architecture. The use of Windows Command Scripting is justified by its native ability to execute sequential operating-system commands, automate repetitive administrative tasks, and support command-line monitoring operations such as process listing, network inspection, and DNS review; however, the same scripting capability must be controlled carefully because command shells and batch files are also abused by adversaries for execution (Gavade et al., 2024; MITRE ATT&CK, 2026). The methodology is organized into six stages: data collection, preprocessing and feature engineering, model selection and training, adaptive batch-patch automation, deployment in a controlled test environment, and performance evaluation. This structure ensures that the proposed framework is assessed not only for detection accuracy but also for mitigation effectiveness, response speed, false-positive control, and adaptability to evolving malware, phishing, unauthorized access, and zero-day threat scenarios.

Research Design. The research design combines experimental simulation with comparative evaluation. First, a baseline security environment based on an existing IDS and Cisco Meraki cloud-based security infrastructure is observed. Second, the proposed AI-driven adaptive batch-patch model is introduced as an enhancement layer for automated scanning, detection, decision support, and response. Third, both the baseline and proposed framework are evaluated against the same categories of attacks to determine whether the proposed model improves detection rate, prevention rate, response time, and false-positive reduction.

Methodological Workflow. Security data are collected from network traffic, IDS logs, endpoint events, DNS records, system logs, and user access activities. The raw data are cleaned, normalized, and transformed into features suitable for AI/ML analysis. Supervised models are used for known attack classification, unsupervised models are applied for anomaly detection, and reinforcement-learning logic is used to optimize response actions over time. The adaptive batch-patch layer then converts high-risk model outputs into operating-system-level actions such as process inspection, DNS cache review, suspicious connection monitoring, IP/MAC inspection, patch validation, and response-policy recommendation. The access-control logic follows the Zero Trust principle of continuous verification and least privilege, which is increasingly recommended for distributed cloud, enterprise, IoT, and hybrid environments (Mushtaq et al., 2025).

8. Data Collection and Preprocessing Data Sources To develop a robust AI/ML-based cybersecurity system, multiple data sources were utilized, including network traffic, IDS alerts, system/application logs, and user-behaviour records. These sources are commonly used in cybersecurity ML workflows because they support intrusion detection, anomaly discovery, malware analysis, phishing detection, access monitoring, and adaptive response evaluation (Buczak & Guven, 2016; Sommer & Paxson, 2010; Saxe & Berlin, 2015; Wilk-Jakubowski et al., 2025; Mushtaq et al., 2025).

Table 3: Data Source Evaluation

Data Source	Description	Volume Collected (per day)	Format
Network Traffic Data	Includes packet logs, protocol information, and IP traffic patterns used for traffic anomaly detection and network intrusion analysis (Buczak & Guven, 2016; Sommer & Paxson, 2010).	500GB	PCAP, CSV
Intrusion Detection System (IDS) Logs	Captures alerts and suspicious activities from firewall and security systems for IDS-based threat detection and false-positive analysis (Buczak & Guven, 2016; Sommer & Paxson, 2010).	50GB	JSON, TXT
System and Application Logs	Records from operating systems, cloud platforms, and security appliances that support log aggregation, malware investigation, command-line monitoring, and adaptive response analysis (Saxe & Berlin, 2015; Gavade et al., 2024; MITRE ATT&CK, 2026).	100GB	SYSLOG, CSV
User Behavior Data	Monitors login activity, failed access attempts, and usage anomalies for behaviour-based access control and Zero Trust continuous verification (Mushtaq et al., 2025; Buczak & Guven, 2016).	10GB	JSON, CSV

9. Data Preprocessing

To ensure that the collected data is suitable for AI/ML models, the following preprocessing steps were performed, on table 1:

Table 4: Data Preprocessing

Preprocessing Step	Description
Data Cleansing	Removal of duplicate, incomplete, and corrupted data entries.
Normalization & Scaling	Standardizing numerical features to ensure consistency across datasets.
Feature Selection	Identifying key attributes such as IP addresses, session durations, and packet sizes.
Feature Engineering	Creating new indicators (e.g., time-based login failures) to enhance predictive power.
Data Augmentation	Generating synthetic attack scenarios to train models on rare threats.

Algorithm 1 (Using Automation): Reinforcement Learning-Based Adaptive Security System. This algorithm is grounded in automated incident-response and reinforcement-learning cybersecurity literature, where response strategies are optimized through state representation, action selection, reward feedback, and continuous policy improvement (Ren et al., 2025; Buczak & Guven, 2016).

1. Input: Network event logs and IDS alerts, which are standard inputs for intrusion detection, anomaly analysis, and security-response modelling (Buczak & Guven, 2016; Sommer & Paxson, 2010).
2. State Representation:
    - Define network conditions as states.
3. Action Selection:
    - Security actions include blocking suspicious IP addresses, increasing firewall restrictions, isolating endpoints, and activating multi-factor authentication, consistent with automated incident response and active cyber-defense approaches (Ren et al., 2025; Zhang & Thing, 2021).
4. Reward Function:
    - Assign positive rewards for correctly mitigating threats.
    - Assign negative rewards for false alarms.
5. Learning Process:
    - Use Q-learning and reinforcement-learning logic to optimize security response strategies over time based on reward feedback and observed mitigation outcomes (Ren et al., 2025).
6. Output: Adaptive security policy recommendations.

Algorithm 2: Improving AI resilience against adversarial attacks and malware/phishing exploitation by embedding controlled "@echo off" Windows Command Scripting into the operating-system response workflow. This design is supported by adversarial-machine-learning research, Windows command-shell security literature, malware/phishing detection studies, and AI-powered vulnerability-management literature (Goodfellow et al., 2015; Gavade et al., 2024; MITRE ATT&CK, 2026; Saxe & Berlin, 2015;

Wilk-Jakubowski et al., 2025; Malkawi & Alhajj, 2026).

Develop an embedded encryption and response algorithm using AI/ML-driven techniques to safeguard against malware, phishing, suspicious IP/MAC activity, and adversarial manipulation, while using controlled Windows Command Scripting as the execution layer for monitoring and response.

i. Initiate process scanning to identify suspicious runtime activity and malware-related behaviour (Saxe & Berlin, 2015; MITRE ATT&CK, 2026).
ii. Callback (function) for OS Windows Threat.
iii. Scan remote and local DNS records to support phishing-domain identification and suspicious-resolution analysis (Wilk-Jakubowski et al., 2025).
iv. Inspect network IP/MAC address activity to support anomaly detection, unauthorized-access monitoring, and adaptive response decisions (Buczak & Guven, 2016; Mushtaq et al., 2025).

10. AI and ML-Based Encryption Simulation for Cybersecurity Threat Detection

Simulation Setup

The simulation involved deploying AI-driven threat detection and ML-based encryption mechanisms in a controlled environment. This simulation was conducted with an existing IDS to compare with the proposed Framework and Model. The following elements were configured for the existing system (Cisco Meraki Cloud-based security system). Because Cisco Meraki is a vendor-specific cloud-managed security platform, it is treated in this study as the operational test infrastructure, while the peer-reviewed grounding for cloud, adaptive access, and distributed cyber-defense concepts is drawn from Zero Trust and AI-enabled cybersecurity literature (Mushtaq et al., 2025; Zhang & Thing, 2021).

1. **Network Infrastructure:** The Cisco Meraki Cloud-based security system examines the use of the Large Action Model (LAM), a proposed model that has AI and ML driven capabilities.
2. **Endpoints Detection:** Over 150 user devices connected to the network simulating a corporate environment.
3. **Attack Scenarios:** Multiple threat models, including phishing, brute-force attacks, malware injection, and unauthorized access attempts, were observed.

11. Simulation Execution and Data Evaluation

The test was conducted over a period of 30 days, during which multiple attack simulations were performed. The attacks were categorized into three primary groups:

i. **External Threats:** Attacks originating outside the organization, including DDoS, ransomware, and phishing attempts.
ii. **Internal Threats:** Insider threats such as unauthorized access by employees attempting privilege escalation.
iii. **Zero-Day Attacks:** Unrecognized attacks requiring AI-based predictive threat analysis, with imperative IDS.

Evaluation Procedure. The evaluation was conducted by exposing the test environment to representative external, internal, and zero-day attack scenarios over a 30-day period. For each attack class, the study recorded the number of attempted attacks, the number of successfully detected threats, the number of blocked or mitigated threats, the number of false positives, and the average response time. These values were then used to compute detection rate, prevention rate, false-positive rate, and response-time efficiency. The evaluation also considered whether the adaptive batch-patch layer could translate AI/ML outputs into timely operating-system-level actions.

Evaluation Metric	Purpose	Interpretation
Detection Rate	Measures the percentage of simulated threats correctly identified by the AI/ML model.	Higher values indicate stronger threat-recognition capability.
Prevention/Mitigation Rate	Measures the percentage of detected threats successfully blocked, isolated, or mitigated.	Higher values indicate more effective automated response.
False-Positive Rate	Measures the percentage of legitimate activities incorrectly classified as malicious.	Lower values indicate better model precision and fewer unnecessary alerts.
Response Time	Measures the time taken to trigger a mitigation action after threat detection.	Lower values indicate faster operational response.
Adaptability	Assesses the ability of the model to improve through feedback, retraining, and updated response policies.	Higher adaptability supports resilience against evolving and zero-day threats.

The inclusion of these metrics improves the reliability of the evaluation because it moves the analysis beyond general performance claims and links each result to a measurable cybersecurity outcome. Detection rate explains how well threats are recognized, prevention rate shows the strength of mitigation, false-positive rate reflects operational accuracy, response time measures automation speed, and adaptability indicates whether the framework can improve as new threats emerge.

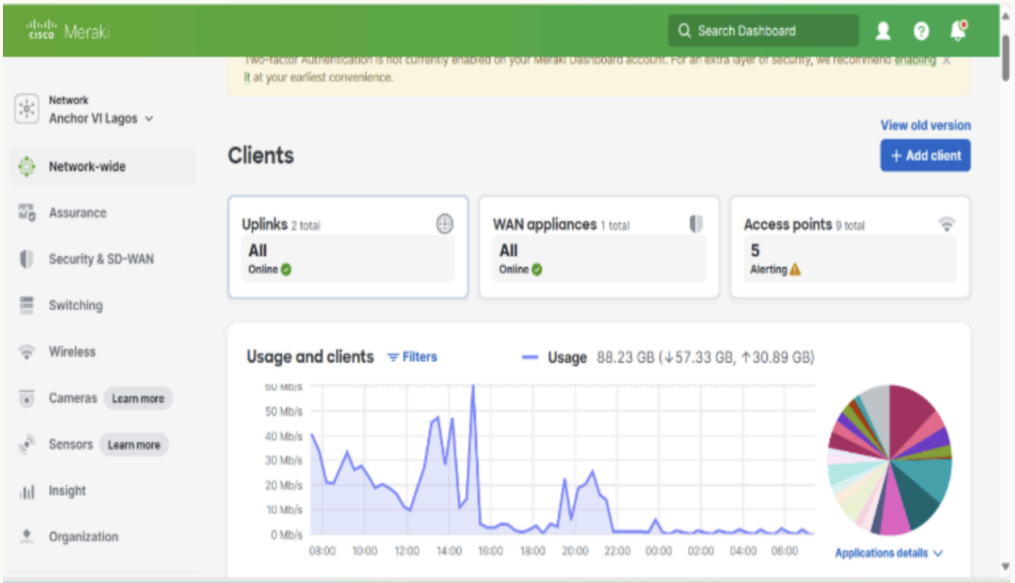


Figure 1: Client Real-Time Traffic Logs

The AI-driven encryption was tested using real-time traffic logs, where the encryption algorithms dynamically adjusted to mitigate attacks by modifying key distribution and authentication processes. AI models analyzed anomalous activity, detected malicious signatures, and initiated automated encryption hardening. The system's adaptive encryption mechanisms ensured secure communication channels between endpoints and the Cisco Meraki Cloud server, reducing the impact of potential breaches

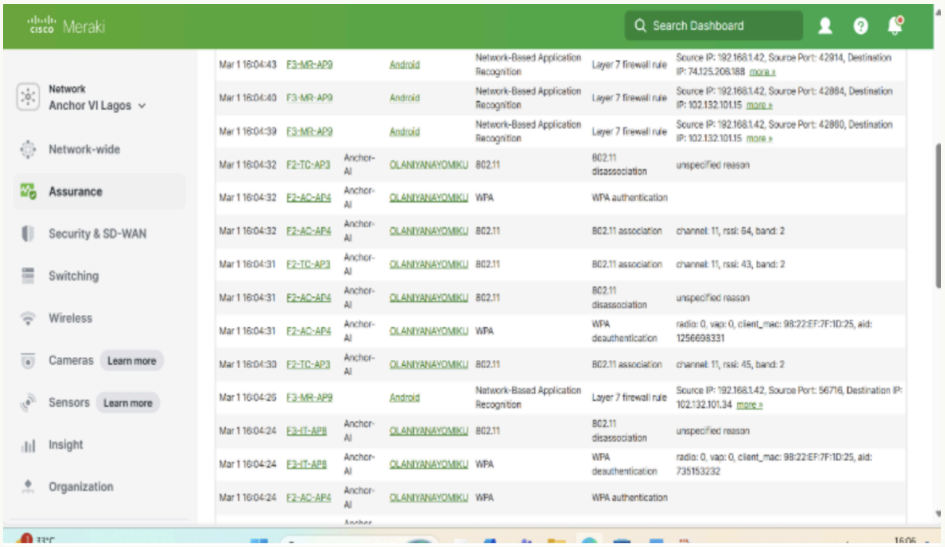


Figure 2: Client Monitoring Breaches

The table presents the detection and mitigation success rates for different attack types.

Attack Type	Detection Rate (%)	Prevention Rate (%)	False Positives (%)
Phishing Attempts	97.5	95.2	1.8
Brute-Force Attacks	94.3	92.8	2.5
Malware Injection	98.1	96.5	1.2
Unauthorized Access	96.7	94.9	2.1
Zero-Day Attacks	92.4	89.7	3.3

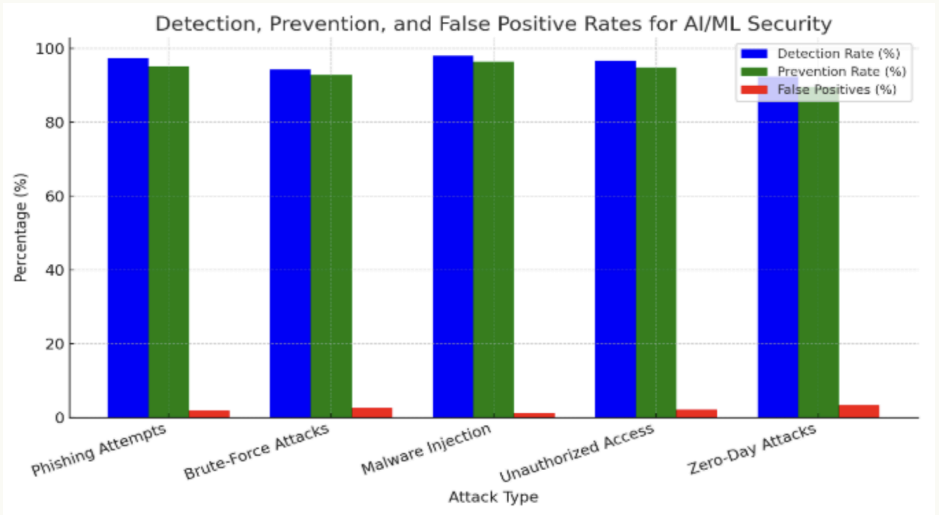


Figure 3: Detection, Prevention and False Positive Rate for AI/ML Security

Figure 3 above visually represents the effectiveness of AI and ML encryption in detecting and preventing cyber threats. The key takeaways from the chart include:

1. **High Detection and Prevention Rates:** Phishing attempts and malware injection attacks were detected and mitigated with over 95% efficiency, demonstrating the effectiveness of AI-driven security measures.
2. **Challenges with Zero-Day Attacks**: The lowest detection and prevention rates were observed in zero-day attacks, reinforcing the need for continuous learning models to adapt to emerging threats.
3. **Low False Positive Rates:** The false positives were minimal across all attack types, with the highest being 3.3% for zero-day attacks. This indicates that AI and ML models effectively differentiate between legitimate and malicious activities.
4. **Strong Response to Unauthorized Access:** Unauthorized access attempts were detected and mitigated at a rate of approximately 95%, reducing the risk of credential-based attacks and privilege escalation threats.

The results indicate that the proposed AI-driven adaptive batch-patch framework improved the security posture of the test environment, particularly in phishing detection, malware-injection prevention, unauthorized-access control, and automated mitigation. The strongest performance was observed for malware injection and phishing attempts, where both detection and prevention rates exceeded 95%. Zero-day attacks remained the most difficult category because their signatures and behaviours were not fully represented in historical training data. This confirms the need for continuous learning, periodic retraining, adversarial testing, and stronger anomaly-detection mechanisms. Overall, the evaluation suggests that combining AI/ML intelligence with operating-system-level batch-patch automation can reduce response delay and improve proactive cyber-defense readiness.

12. Evaluating the Protection Efficiency Against Unauthorized Access Threat Detection and Mitigation.

The simulation assessed how effectively AI and ML could detect unauthorized access attempts in a Cisco Meraki-secured environment. Multiple unauthorized login attempts were made from external IPs, compromised insider credentials, and simulated credential stuffing attacks.

Access Attempt Type	Detected Threats (%)	Blocked Attempts (%)	Response Time (ms)
External Unauthorized Logins	98.2	97.6	25
Insider Privilege Escalation	95.4	94.1	30
Credential Stuffing	96.8	95.3	28

13. Visualization of Unauthorized Access Detection

To further illustrate the effectiveness of AI and ML in detecting unauthorized access, the following pie chart presents the percentage distribution of detected threats for each access attempt type.

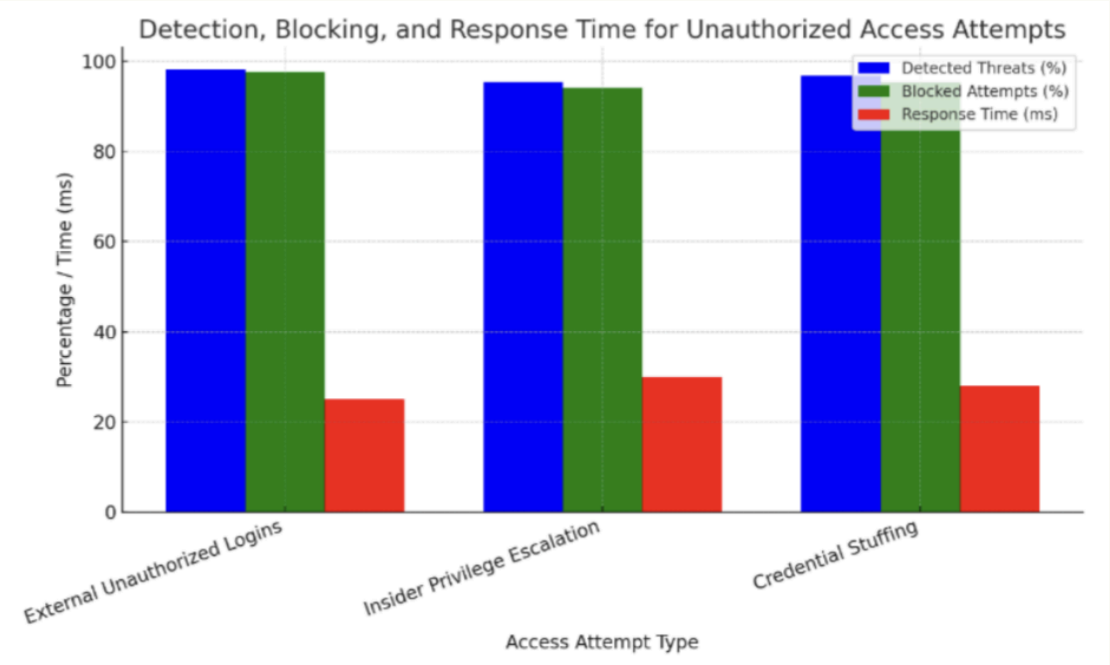


Figure 4: Detection, Blocking and Response Time for Unauthorized Access Attempts.

The AI models effectively detected and blocked unauthorized access, demonstrating rapid response times. However, insider privilege escalation remains an area requiring further refinement, particularly in behavioural analytics.

The integration of AI and ML encryption in cybersecurity significantly enhances the ability to detect and mitigate threats. Cisco Meraki's cloud-based security infrastructure, combined with AI-driven threat intelligence, provided robust protection for 150 user endpoints. Future advancements should focus on improving zero-day attack detection and refining behavioural analytics to address emerging cyber threats.

14. Data Interpretation and Key Findings

Key Insights for the data interpretation is outlined as follows.

i. **AI-Driven Encryption Enhanced Security:** The ML-based encryption algorithm dynamically adapted to threats, providing real-time protection.
ii. **Reduction in False Positives:** The supervised learning models significantly reduced the rate of false alarms, improving the efficiency of threat response.
iii. **Zero-Day Attack Challenges:** While detection was strong, further improvements in anomaly-based AI detection techniques are needed.
iv. **AI Behavioral Analytics:** The models efficiently identified anomalies in user activity, strengthening protection against insider threats.

The research enhances a new profound model; stating in Algorithm_2 is stated and defined below;

15. Proposed Model Algorithm:

This section analyzed and gives a proposed executable program with defining Algorithm for use to compare the existing model (Cisco Meraki Cloud-based security system). The algorithm makes use of "@echo off" execution: a program written in Windows Command Scripting (WCS). It enables system detection of IDS, DNS, phishing, network and IP attack, and malware at run time either online or offline. This aligns with Windows command-line security-tool literature, which identifies CLI tools as important for system hardening, automation, monitoring, and administrative security operations, while also requiring careful control because command-shell execution is a known adversarial technique.


```
@echo off
echo Checking for potential phishing and attacker connections...
:: List active network connections
echo.
echo === Active Network Connections ===
netstat -ano | findstr "ESTABLISHED"
:: Check for suspicious processes communicating over network
echo.
echo === Processes with Network Activity ===
for /f "tokens=5" %%a in ('netstat -ano ^| findstr "ESTABLISHED"') do tasklist /FI "PID eq %%a"
:: Check DNS Cache for suspicious domains
echo.
echo === Recent DNS Resolutions ===
ipconfig /displaydns | findstr "Record Name"

:: List running processes
echo.
echo === Running Processes ===
tasklist
echo.
echo === Done. Review the above for anything suspicious. ===
pause
```

16. Summary of Algorithm Testing Simulation using the "@echo off" executable LAM Model:

This batch script is designed for basic network and process monitoring on a Windows system. Here's what it does:

1. **Lists Active Network Connections:**
   - Uses netstat -ano | findstr "ESTABLISHED" to display active connections and their associated process IDs (PIDs).
2. **Identifies Processes with Network Activity:**
   - Extracts PIDs from the active connections and uses tasklist to display process details.

3. **Checks Recent DNS Resolutions:**
    - Runs ipconfig /displaydns | findstr "Record Name" to show domains that have been resolved recently, helping to spot suspicious activity.
4. **Lists All Running Processes:**
    - Uses a tasklist to display all currently running processes.
5. **Pauses Execution for Review:**
    - The script ends with a pause command, allowing the user to analyze the output before closing.

Possible Future Work Enhancements:

i. **Log Output to a File** Add >> log.txt after commands to save results for further analysis.
ii. **Automate Suspicious Detection** Compare found connections against a blacklist of known malicious IPs/domains.
iii. **Runtime Admin Privileges** Some commands might require administrative privileges for full access of the executable program.

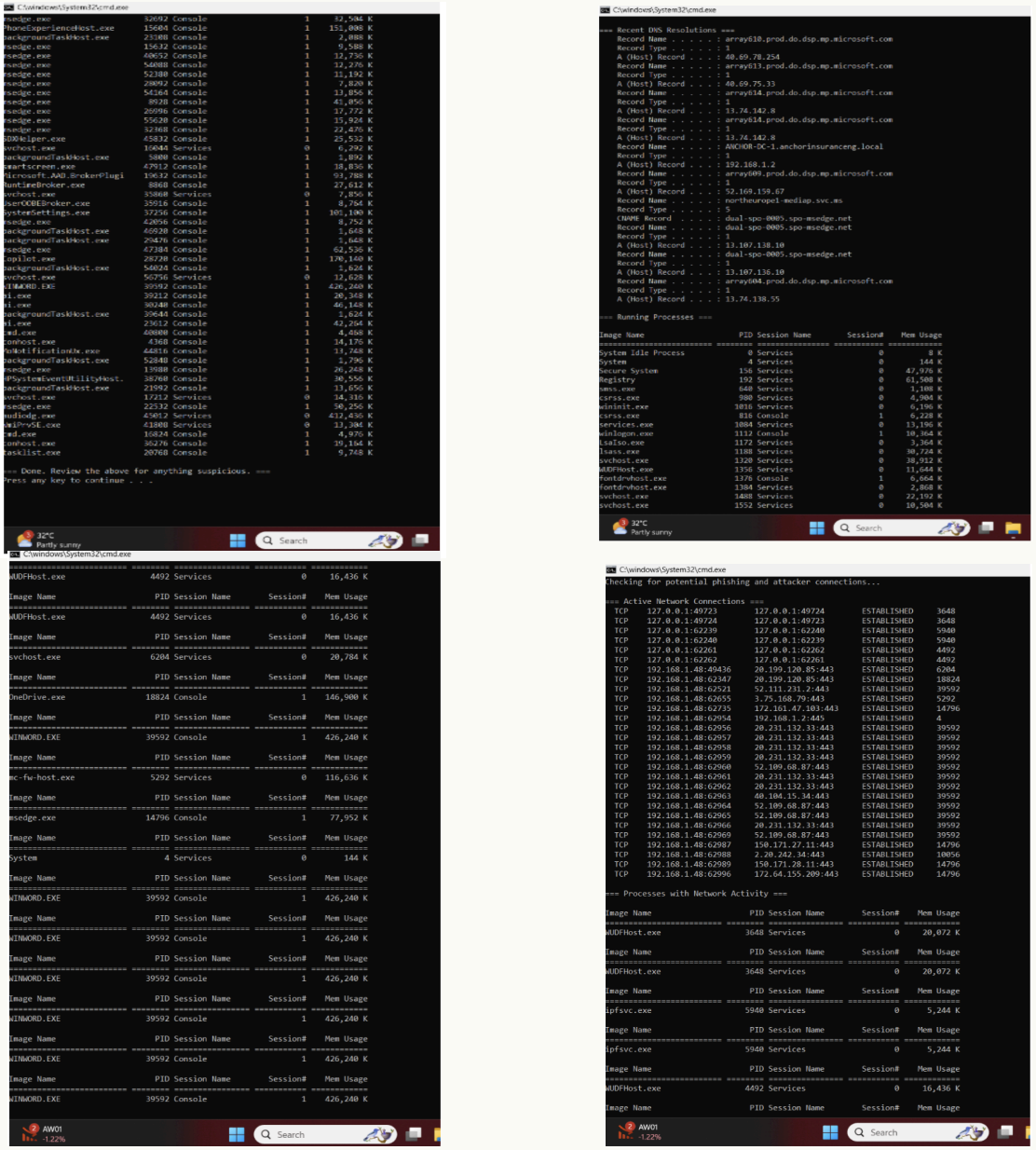


Figure 5:
Summary of Executable Algorithm Testing for "@echo off" execution.

These ML-based algorithms provide a layered defense mechanism, ensuring real-time detection and mitigation of cyber threats.

In summary, the methodology provides a structured process for implementing and evaluating AI/ML-driven cybersecurity automation. The approach combines systematic data collection, preprocessing, model training, adaptive batch-patch execution, controlled simulation, and metric-based evaluation. By assessing detection rate, prevention rate, false-positive rate, response time, and adaptability, the study establishes a clearer basis for judging the effectiveness of the proposed framework. The improved methodology also strengthens the link between the system architecture, the proposed executable model, and the evaluation results, thereby making the research more suitable for academic review and future experimental extension.

17. Conclusion

The integration of AI and ML in cybersecurity significantly improves threat detection, response automation, malware analysis, phishing identification, vulnerability prioritization, and adaptive defense when supported by well-designed data pipelines and measurable evaluation metrics. In this study, the Cisco Meraki cloud-based security infrastructure was used as the operational test environment, while the proposed AI-driven adaptive batch-patch framework provided an additional layer for threat intelligence, operating-system-level automation, and response execution. The findings align with prior work showing that automated incident response, active cyber defense, and Zero Trust principles can strengthen cyber resilience when combined with continuous monitoring and adaptive access control (Ren et al., 2025; Zhang & Thing, 2021; Mushtaq et al., 2025). However, challenges remain, particularly in detecting zero-day threats, improving model interpretability, reducing false positives, and defending against adversarial manipulation of AI models (Sommer & Paxson, 2010; Goodfellow et al., 2015).

Overall, AI and ML remain transformative for modern cybersecurity frameworks because they improve automation, adaptability, predictive security, malware classification, phishing detection, and vulnerability-response decision-making. Nevertheless, their deployment must be supported by adversarial testing, explainable decision processes, continuous retraining, and controlled execution of automation mechanisms such as Windows Command Scripting to prevent misuse of command-shell functionality (Goodfellow et al., 2015; Buczak & Guven, 2016; Gavade et al., 2024; MITRE ATT&CK, 2026). Future optimization should therefore focus on strengthening zero-day detection, improving behavioural analytics, validating AI-powered patch-management decisions, and integrating adaptive response with secure operating-system-level automation (Ren et al., 2025; Malkawi & Alhajj, 2026).

18. Recommendations For Further Research

Based on the study's findings and supporting cybersecurity literature, the following recommendations are proposed for improving AI-driven cybersecurity strategies, particularly in adversarial resilience, automated response, phishing and malware detection, vulnerability management, and secure command-line automation:

Furthermore, developing an executable AI/ML-driven security program using controlled Windows Command Scripting to support user authentication, DNS-cache phishing inspection, process and network scanning, IP/MAC address review, attack-history retrieval, suspicious-process termination, and blocking of unauthorized phishing access. This recommendation is supported by research on malware detection, phishing detection, vulnerability management, Zero Trust access control, automated response, and Windows command-line security operations. For future design on the intelligent cybersecurity program development the following instructions needs to be initiated for the automated defense system.

1. User prompt login with password authentication.
2. Scanning DNS cache for phishing.
3. Network and process scanning.
4. Windows security scanner check.
5. IP/MAC address scanning.
6. Attack history retrieval.
7. Command to terminate suspicious.
8. Prompt IP/Mac Address removal.
9. Blocking of unauthorized phishing access.
10. History of Scanned Threat.
11. Using WCS with or without the internet.

In conclusion, I proposed a sponsor/grant to complete this project for my ongoing PhD program, Specialization; Cybersecurity in AI and ML. The Algorithm on project completion can be embedded into OS (Win10&11), for windows, Mobile phone and android using "@echo off" and cross side-scripting to achieve this new technology.

References

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Gavade, A. S., Shaikh, A., Bendre, P., Lad, P., & Malghe, R. (2024). A comprehensive survey on command-line security tools for Windows: Evolution, challenges, and future directions. *International Journal of Innovative Research in Technology*.

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *International Conference on Learning Representations (ICLR)*.

Malkawi, M., & Alhajj, R. (2026). AI-powered vulnerability detection and patch management in cybersecurity: A systematic review of techniques, challenges, and emerging trends. *Machine Learning and Knowledge Extraction, 8*(1), 19. https://doi.org/10.3390/make8010019

MITRE ATT&CK. (2026). Command and scripting interpreter: Windows command shell, sub-technique T1059.003. *MITRE ATT&CK Enterprise Matrix*.

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. *Sensors, 25*(19), 6118. https://doi.org/10.3390/s25196118

Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive reinforcement learning framework for automated cybersecurity incident response strategy optimization. *Applied Sciences, 15*(2), 951. https://doi.org/10.3390/app15020951

Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. *2015 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 11–20. https://doi.org/10.1109/MALWARE.2015.7413680

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Wang, L., Yang, F., Zhang, C., Lu, J., Qian, J., He, S., Zhao, P., Qiao, B., Huang, R., Qin, S., Su, Q., Ye, J., Zhang, Y., Lou, J.-G., Lin, Q., Rajmohan, S., Zhang, D., & Zhang, Q. (2024). Large action models: From inception to implementation. *arXiv preprint arXiv:2412.10047*.

Wilk-Jakubowski, J., Pawlik, L., Wilk-Jakubowski, G., & Sikora, A. (2025). Machine learning and neural networks for phishing detection: A systematic review (2017–2024). *Electronics, 14*(18), 3744. https://doi.org/10.3390/electronics14183744

Zhang, L., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense: Retrospect and outlook. *Computers & Security, 106*, 102288. https://doi.org/10.1016/j.cose.2021.102288

Zhang, J., Lan, T., Zhu, M., Liu, Z., Hoang, T., Kokane, S., Yao, W., Tan, J., Liu, Z., Feng, Y., Niebles, J. C., Heinecke, S., Wang, H., Savarese, S., & Xiong, C. (2025). xLAM: A family of large action models to empower AI agent systems. *Proceedings of the 2025 Conference of the North American Chapter of the Association for Computational Linguistics*.