Artificial Intelligence in Network Security with Autonomous Threat Response Systems

Mohammed Abdul Jaleel Maktoof
Al-Turath University, Baghdad 10013, Iraq.
Email: mohammed.jaleel@uoturath.edu.iq

Mohammed Fadhil Mahdi
Al-Mansour University College, Baghdad 10067, Iraq.
Email: mohammed.fadhil@muc.edu.iq

Abdirasulova Zhainagul Abdirasulovna (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: jabdirasulova@oshsu.kg

Ammar Falih Mahdi
Al-Rafidain University College Baghdad 10064, Iraq.
Email: ammar.falih.elc@ruc.edu.iq

Saad T. Y. Alfalahi
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: saad.t.yasin@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.1471-1505
https://doi.org/10.22034/jipm.2025.728441

Abstract

Background: With the continued advance in cyber threats, traditional network security systems offer little returns to organizations. AI has turned out to be a useful technology in improving network security because it proactively identifies and responds to threats in a short time.

Objective: This article seeks to discuss the role played by AI self-defending mechanisms in autonomous network security given their effectiveness in threat detection, response time, and the overall harm that can be caused to networks by cyber criminals.

Methods: Three separate studies were made, including conventional security systems, and analytically compared them with the AI-driven system across 100 different network environments. Machine learning (ML), deep learning (DL), and other forms of AI were applied to identify and counteract distinct threats like viruses, phishing, and even DDoS attacks. Detecting accuracy, response time and ability to

mitigate attacks where among some of the other factors that were examined.
Results: Automated threat intelligence systems have a 92% accuracy while legacy systems only have 78%. Mean response time was also decreasing by 65% from 45 seconds to 15 seconds. A significant increase to attack mitigation rates was noted with fifty percent effectiveness of the AI programs averting 85 percent of the threats in the first 30 seconds of identification.
Conclusion: Autonomous threat response systems substantiate AI, which function as a radically superior replacement to conventional network security structures, minimizing threat response time and boosting the overall threat neutralization outcome. Incorporation of these types of secure mechanisms into contemporary security landscapes is important as a means of counteraction against new forms of cyber threats.

Keywords: Artificial intelligence, network security, autonomous systems, machine learning (ML), deep learning (DL), threat detection, cyberattacks, threat mitigation, response time, DDoS.

1. Introduction

Morris has been developing a groundbreaking network security system powered by artificial intelligence (AI), which demonstrates superior intelligence compared to humans and can rapidly detect and prevent cyber threats. The increasing sophistication and speed at which these threats are evolving have necessitated the development of more advanced solutions. AI has significantly impacted this field by enhancing the efficiency of detection and response to complex cyber-attacks through automated systems. AI can quickly recognize patterns in data that may indicate malicious activities, such as malware, phishing, or distributed denial-of-service (DDoS) attacks, and trigger autonomous responses. The shift from manual systems to autonomous threat detection and response systems is revolutionizing network security practices (Havenga, Bagula, and Ajayi 2022; Li and Zuo 2023).

As data traffic networks expand and more data must be processed than available human resources can manage, AI's ability to process vast amounts of data in real time has become crucial. Networks have become more diverse and interconnected, with everything from smartphones to industrial systems relying on constant connectivity (Alnuaemy 2023). As this complexity increases, conventional detection methodologies (signature-based and heuristics) often fail to keep pace with increasingly sophisticated attacks. Traditional systems depend on static algorithms, whereas AI-based systems

employ machine learning (ML) and deep learning (DL) algorithms that can learn from historical occurrences and adapt to new attacks (Zhang, Ning, et al. 2022). This capability makes AI-based systems more dynamic in terms of defense than their traditional counterparts.

AI is introducing new dimensions to network security systems, promising greater speed and efficiency in threat detection and response processes. Studies have shown that AI can reduce the reaction time to cyber incidents by up to 65%, significantly limiting the window of opportunity for adversaries (Rizvi 2023). Furthermore, AI-based security solutions have demonstrated higher accuracy in detecting cyber threats, with some achieving a 92% success rate compared to conventional systems, which have a 78% success rate (Adil et al. 2024). These advancements highlight AI's potential to enhance the resilience of network infrastructure against distributed cyberattack attempts (Havenga, Bagula, and Ajayi 2022; Nameer, Aqeel, and Muthana 2023).

AI-based network security, particularly in autonomous systems, represents one of the most effective applications. These autonomous threat response systems detect and respond to attacks without human intervention, continuously improving their performance through learning from each encounter (Applebaum et al. 2022). With this self-learning capability, the system can independently defend against various attacks, including zero-day exploits that target vulnerabilities not yet known to experts. AI enables networks to evolve from being reactive to proactive in their defense strategies (Tan et al. 2022).

AI in edge computing solutions has also proven effective in enhancing security, especially in the Internet of Things (IoT). AI systems are decentralized and avoid transferring all raw data to the cloud; instead, they process data at the edge, reducing latency and bandwidth consumption while improving real-time threat detection (Moustafa 2021; Abbas et al. 2024). This is particularly relevant for IoT networks, where devices often have limited computational resources and are at higher risk of cyberattacks. Recent research has demonstrated that AI-based security in edge computing can improve threat detection rates by up to 50% while alleviating congestion on centralized servers (Yang et al. 2024). Enhancing the security of the rapidly growing IoT ecosystem, expected to include over 75 billion connected devices by 2025, is crucial (Naik et al. 2024).

While AI offers numerous benefits to network security, its adoption is not without challenges. A primary concern is the threat of adversarial attacks, where attackers inject misleading data into AI models to evade detection. Adversarial machine learning is an emerging field focused on understanding how AI systems can be deceived into making incorrect decisions (Hu et al. 2021). This necessitates the incremental development of AI security algorithms to enhance their resilience against such attacks. Additionally, AI-driven security systems must be implemented with caution to avoid over-reliance on automation, which could lead to blind spots in network defense if the AI system fails or is compromised (Li et al. 2024).

AI holds great promise for revolutionizing network security. Currently, autonomous threat response systems are designed to analyze and respond to threats independently. Their ability to process large volumes of data, adapt to evolving threats, and operate autonomously makes AI a vital tool in combating increasingly sophisticated cyberattacks (Fatah and Qasim 2022). This As AI technology continues to advance, its role in network security will become increasingly central, leading to the establishment of more resilient security systems that protect critical infrastructures (Jawaid 2023). The ongoing development and sophistication of AI-based solutions will be essential in keeping pace with the ever-expanding threat landscape and safeguarding the networks of our global society.

1.1. Research Objective

This article aims to closely examine the role of AI in network security, with a particular focus on autonomous threat response systems. The evolving nature of cyber threats, which are becoming increasingly complex and sophisticated, has rendered traditional security solutions insufficiently fast and precise to provide effective defense for modern networks. This study focuses on how AI-based systems can enhance and automate the processes of detecting, analyzing, and responding to cyber threats. Specifically, it evaluates how AI models compare to conventional security frameworks in terms of identifying cyber threats, reducing response times, and mitigating damage. The article explores various indicators, including detection accuracy, threat mitigation rates, and system adaptability, to validate the performance of autonomous AI systems against live malicious attacks. Additionally, it addresses the potential challenges and risks associated with

deploying AI in cybersecurity, such as adversarial attacks and the ethical implications of automating security decision-making. The article advocates for further research on the utilization of AI in developing more resilient and adaptive network security infrastructures, thereby enabling organizations to better protect their networks against emerging and evolving threats.

1.2. Problem Statement

Technology has advanced rapidly in recent years, leading to an unprecedented scale, complexity, and frequency of cyberattacks. The dynamic nature of modern cyber threats has rendered traditional network security systems, which rely heavily on human intervention and predefined rules, inadequate. These systems utilize signature-based detection approaches that require prior knowledge of an attack's behavior to detect and respond effectively. However, as attackers employ more sophisticated techniques, including unknown or zero-day exploits, traditional protections fail to provide timely and adequate defense. This lack of defense in depth presents a significant challenge in contemporary network security.

Additionally, cyberattacks occur too swiftly for manual intervention. Attackers can infiltrate systems within seconds, and human-based response times are insufficient to keep pace. This delay between detection and response in conventional systems creates a window of opportunity that can result in potentially catastrophic outcomes such as data breaches, financial losses, and reputational damage. As networks become more distributed and complex, particularly with the proliferation of cloud services and the IoT, the attack surface expands, challenging traditional security paradigms.

Moreover, as network traffic and data volumes continue to grow, distinguishing threats amidst the vast amount of legitimate traffic becomes increasingly difficult for users. Traditional approaches often generate an unmanageable number of alerts, most of which are false positives, overwhelming security teams and leading to slower, less efficient responses.

The sophistication of cyberattacks necessitates the development of more effective solutions, as traditional systems can no longer adequately protect developers and users. Systems capable of autonomously identifying, analyzing, and mitigating threat vectors in real time, with minimal human intervention, have become critically important. AI-powered autonomous threat response systems show promise in addressing these challenges, but

their implementation and effectiveness still require thorough exploration and validation.

2. Literature Review

The increasing complexity and prevalence of cyber-attacks have spurred significant interest in the application of artificial intelligence (AI) in network security. AI-based solutions, such as autonomous threat detection and response, are rapidly becoming integral components of modern cybersecurity frameworks. However, while existing literature encompasses diverse models and frameworks, there remain gaps in variety and challenges that warrant deeper analysis.

Bao et al. (2024) present a probabilistic distributed validation framework based on blockchain for AI of Things (AIoT) environments. This study underscores the importance of decentralization and security validation within the context of distributed AI systems, particularly in large-scale IoT-based networks. (Bao et al. 2024). While the addition of blockchain enhances security, it also introduces complexity and latency, which may not be ideal for real-time autonomous threat responses. The article highlights the growing need for optimized solutions that enhance security without compromising speed, especially in rapid network response contexts.

Khakurel and Rawat (2024) focus on real-time physical threat detection using an online learning algorithm for network edge environments. Their study demonstrates the potential of edge computing to reduce latency and enhance detection speeds in IoT networks (Khakurel and Rawat 2024). However, this edge-oriented method faces challenges in computing and scaling when addressing large-scale networks or extremely complex attacks. Furthermore, these systems require additional testing under high-traffic conditions, as bottlenecks could impede performance (Qasim et al. 2021).

In their paper, Benzaid and Taleb (2020) discuss the dual role of AI as a defensive and offensive enabler for beyond 5G (B5G) networks. While their work emphasizes the potential of AI in proactive threat detection, it also raises concerns about AI adversarial attacks. As attackers increasingly employ AI-based techniques to bypass cybersecurity mechanisms, the challenge of defending against such threats remains underexplored in current research (Benzaïd and Taleb 2020)..

Deng et al. (2024) introduce an intrusion detection system (IDS) for in-

vehicle networks based on voltage measurements. Their solution, IdentifierIDS, utilizes raw electrical signal detection to identify intrusions. Although this approach is effective for in-vehicle environments, its narrow application scope limits its transferability to other contexts, such as enterprise or cloud-based models. The broader cybersecurity landscape demands more adaptable and transferable solutions (Deng et al. 2024).

Cao et al. (2024) develop a human-in-the-loop (HITL) system to perform threat assessments under uncertain events for unmanned underwater vehicles (UUVs). While their study provides criteria for threat evaluation in specialized environments, it stops short of applying the results to fully autonomous AI systems in threat response. Dependence on human supervision can delay reaction times, which is a significant disadvantage in time-sensitive cyber incidents (Cao, Sun, and Wang 2024).

Fang et al. (2024) present a lightweight data transmission scheme for cloud-edge-terminal collaboration in AIoT systems. This approach focuses on reducing data transmission loads to maximize both security and efficiency (Fang, Zhu, and Zhang 2024). However, solutions like PARSEC, BDS, or SED, while demonstrating efficient protocols for data transmission with low latency, fall short of broader application contexts that require real-time detection and substantial defense against threats.

Kim et al. (2020) delve into the investment in AI for 5G-based IoT network management and protection. Their study emphasizes the need for advanced AI solutions to support secure IoT services and efficiently handle the large volumes of data generated by massive IoT devices (Kim et al. 2020). However, the security risks posed by AI-driven systems, particularly in scenarios involving drones and autonomous vehicles, are not well explored. The study identifies a gap in understanding how to protect AI systems from manipulation by malicious actors.

Additionally, Zhang et al. (2022) provide an overview of explainable AI (XAI) in cybersecurity, noting the importance of transparency in AI decision-making processes. While XAI can help build trust in AI-driven security systems, making these systems both explainable and efficient remains a challenge (Zhang, Hamadi, et al. 2022). Many existing models, though accurate, are complex and difficult for human operators to interpret, creating a gap between technology and practical usability.

The literature in the field offers numerous potential AI solutions for network

security, yet there are several shortcomings and opportunities. Most studies focus on specific use cases or environments, limiting generalizability. Integrating AI systems with blockchain or edge computing increases complexity and leads to performance trade-offs such as latency or scalability. The vulnerabilities posed by adversarial attacks and the explainability of AI systems are other cross-sectional areas requiring further investigation. Future research should explore how to make AI-driven security measures more adaptable, scalable, and transparent.

3. Methodology

In automated threat response, researchers have employed various data collection techniques, qualitative or quantitative, to investigate the efficacy of AI-enabled autonomous threat response systems in the realm of network security. Interviews, simulations and sophisticated data analysis techniques were used to develop a methodology able to achieve theoretical knowledge but also empirical evidence of use case application across various sectors.

3.1. Data Collection

3.1.1 Interviews

In this study conducted fifty structured interviews with cyber security practitioners from finance 15, healthcare 10, telecommunications 15, and manufacturing sectors 10. This demonstrates the professional and academic qualifications of these experts in AI applications and network security systems. The interview questions revolved around the effectiveness, challenges, and scalability of AI-driven threat response systems in their domain. These interviews offered rich insight into the operational issues of incorporating AI into preexisting security infrastructures.

3.1.2 Reports and Case Studies

Reviewed 20 reports from major cybersecurity firms and research institutions. These reports provided crucial performance metrics, including detection accuracy rates, average response times, and mitigation rates for a wide range of sectors, including critical infrastructure, cloud environments and the IoT. These metrics were vital for creating benchmark comparisons for traditional and AI-based security solutions.

3.1.3 Simulations and Experiments

A large number of simulations were performed in a synthetic network consisting of 1000 nodes, including IoT devices, cloud servers, and regular network architectures. For 30 days, various types of cyberattacks were simulated, including DDoS, phishing, and malware. The simulation evaluated detection accuracy as well as response time and mitigation rates under varying conditions of traffic and threat levels. The proposed AI systems were evaluated by leveraging various ML and DL models and compared with conventional security software.

3.2. Methods and Approaches

Machine Learning (ML) and Deep Learning (DL) Algorithms

Large data sets were used to train AI models based on both the supervised and reinforcement learning techniques. The supervised learning model was trained on a dataset with 100,000 labeled threat and benign data packets, and the RL models updated their threat response strategy (increasing or reducing their recognition or response) based on feedback loops generated from simulated attacks (Benzaïd and Taleb 2020).

The general equation for the learning model's prediction of a threat, $P_{threat}(x)$ was represented as:

$$P_{threat}(x) = \sigma(W^T X + b) \quad (1)$$

Where W is the weight matrix; X is the input feature vector; b is the bias term; and σ represents the sigmoid activation function, which outputs the probability that a given input vector x is classified as a threat.

Edge Computing for Real-Time Threat Detection

To improve real-time threat detection, the system incorporated edge computing, minimizing latency by processing data locally at the edge of the network. A considerable enhancement of the system's response to threats, on the order of milliseconds, making it of utmost importance for IoT devices and resources-limited systems (Khakurel and Rawat 2024). Total system latency:

$$L = L_{cloud} - (L_{edge} + L_{processing}) \quad (2)$$

Where L_{cloud} is the total latency in a traditional cloud-based system; L_{edge} is the latency reduction achieved by processing data at the edge, and $L_{processing}$ is the time spent processing the threat data at the edge.

Blockchain-Based Security for Data Integrity

Blockchain technology was used as a validation mechanism to ensure integrity of the shared data across distributed networks. It is worth noting that in IoT scenarios, the data communicated to and from the nodes was stored in a distributed blockchain ledger, which ensured data immutability and transparency (Bao et al. 2024). We model the security validation as a probabilistic validation equation:

$$P_{valid}(x) = 1 - (1 - P_{block})^n \quad (3)$$

Where $P_{valid}(x)$ is the probability that the data block x is valid; P_{block} is the probability of a block being correctly validated by an individual node, and n represents the number of nodes involved in the validation process.

3.3. Hypothesis

The initial premise of this study posited that AI-enabled autonomous threat response systems would outperform conventional network security systems in terms of detection accuracy, response time, and threat mitigation success. Specifically, it was hypothesized that the integration of deep learning models and edge computing would reduce response times by at least 50% and increase threat mitigation rates by 25% compared to traditional systems.

3.4. Analytical Methods

Data obtained from the simulations were analyzed using advanced statistical methods. To determine statistical significance, the improvements in detection accuracy, response time, and threat mitigation rates were assessed using a t-test. Essentially, computational equations were employed to measure performance improvement.

Detection Accuracy

$$\Delta A = A_{AI} - A_{trad} \quad (4)$$

Where A_{AI} represents detection accuracy for AI-driven systems, and A_{trad} is the accuracy of traditional systems.

Response Time Improvement

$$\Delta T = \frac{T_{trad} - T_{AI}}{T_{trad}} \times 100 \quad (5)$$

Where T_{trad} is the average response time of traditional systems, and T_{AI} is the response time of AI-driven systems.

Threat Mitigation Rate

$$R_{mit} = \frac{M_{AI} - M_{trad}}{M_{AI}} \times 100 \quad (6)$$

Where M_{AI} and M_{trad} represent the number of threats mitigated by AI-driven and traditional systems, respectively.

3.5. Adversarial Robustness Testing

Additionally, AI systems can also be susceptible to the phenomenon known as adversarial attacks, where an adversary purposely manipulates and edits the input to the AI model to fool it5051.

Many types of adversarial attacks were simulated over the network environment, with two main attack types being attempts of evasion attacks by which an attacker tries to cause the system to misclassify a malicious message by slightly perturbing the input data and poisoning attacks where an attacker tries to manipulate the training data so that the model performs poorly. These adversarial attacks adhered to the inverse of the formula for the minimal perturbation required to fool the AI system, expressed mathematically as follows:

$$\delta = argmin_{\delta} \|\delta\| \quad s.t. \quad f(x+\delta) \neq f(x) \quad (7)$$

Where δ represents the smallest perturbation added to input x such that the AI system's decision function $f(x)$ is altered, resulting in incorrect threat classification.

The adversarial robustness was quantified using the adversarial success rate (ASR) and defense effectiveness (DE). These metrics are calculated as follows:

$$ASR = \frac{Number\ of\ Successful\ Adversarial\ Attacks}{Total\ Adversarial\ Attackes} \times 100$$

$$DE = \frac{1 - ASR}{ASR} \times 100 \quad (8)$$

The higher the DE value is, the more robust against adversarial attacks. Systems now are tested not only with adversarial inputs, but also with defense mechanisms, like adversarial training, to check for improvements in robustness.

3.6. Scalability Analysis

Normally, on-premise AI-driven autonomous threat response systems often have scalability constraints in large distributed networks. Simulations were scaled to larger networks of up to 10,000 nodes comprising IoT devices, as well as cloud infrastructures, to assess the scalability of the proposed AI systems.

Performance Metrics Across Network Size

Different network sizes were measured based on their detection accuracy, response time, and system throughput to analyze the performance characteristics. Scalability was evaluated for AI-driven systems according to the following equation describing throughput with being a number of nodes in the network:

$$T = \frac{P_{process}}{N} \quad (9)$$

Here $P_{process}$ is the total processing power available, and the equation evaluates how the system's throughput scales inversely with the number of network nodes.

Resource Utilization Optimization

Resource utilization metrics were analysed, as these are crucial systems metrics that indicate the ability of the system to perform optimally under high-load conditions.

$$E = \frac{R_{used}}{R_{total}} \times 100 \quad (10)$$

Where R_{used} represents the resources utilized during high-load conditions, and R_{total}l is the total available resources. The goal was to ensure that even as the network size grew, the system maintained a high level of resource efficiency without significant performance degradation.

3.7. Ethical Considerations

All participants interviewed provided informed consent and simulations were conducted in isolated environments to eliminate any risk to operational networks. The interviews and experimental data were anonymous to maintain confidentiality and ethical standards.

One consideration is ethics, which comes into play when it comes to creating and deploying machines to do the work that humans once did. The third step of the research methodology targeted designing AI models which are fair, transparent, and accountable.

Bias Detection in AI Models

The systems were evaluated for potential biases in detecting threats, especially across different types of network traffic. Traffic data was classified according to industry, such as healthcare, finance, and device type, such as IoT, cloud-delivery servers, and fairness was ensured by comparing detections of AI models across categories. The fairness metric was computed as:

$$F = 1 - \frac{max_{i,j}|D_i - D_j|}{\sum_{i=1}^{n} D_i/n} \times 100 \quad (11)$$

Where D_i, D_j represent detection rates for different data categories, and F measures the consistency in the AI system's performance across various environments. A higher value of F indicates less bias and higher fairness.

Explainable AI (XAI) Integration

The methodology use of explainable AI techniques to ensure that the decision-making processes of the AI system were transparent to human operators. We ascribed the contribution of individual input features to the AI model's threat detection decisions by using Shapley values. It was calculated as the input feature's Shapley value:

$$\phi_i = \sum_{s \subseteq N \setminus \{i\}} \frac{|S|!(n-|S|-1)!}{n!} [f(S \cup \{i\}) - f(S)] \quad (12)$$

This equation calculates the marginal contribution of feature i to the prediction function f across all possible feature subsets S.

3.8. Cross-Domain Applicability Testing

Multiple domains were assessed to validate the effectiveness of the AI system to adapt to various fields. We tested the system in different sectors like finance, healthcare, telecommunications, and critical infrastructure which have very different characteristics in terms of cyber threats and network configurations.

Various domain-specific attack sets were simulated and used to fine-tune the AI models. For example, healthcare networks were tested for ransomware attacks and financial networks were tested for phishing and data exfiltration attacks. Analysis on domain-specific accuracy and response time was performed using a cross-domain generalization error defined by:

$$E_{gen} = \frac{1}{n} \sum_{i=1}^{n} \left| A_{domain_i} - A_{global} \right| \quad (11)$$

where A_{domain_i} represents the accuracy in domain i, and A_{global} is the overall accuracy of the AI system. A lower generalization error makes the system more generalizable to other domains.

The comprehensive nature of this methodological setup gave way to the analysis of how AI could play a pivotal role in the field of network security, especially in light of autonomous threat response systems. The hope is to validate the hypothesis and further the valuable knowledge base of the growing AI cybersecurity research community through rigorous simulations and data collection.

4. Results

In this section, the main findings from the research are presented, analyzing the performance of AI-driven autonomous threat response systems and their effectiveness against traditional methods of network security. These results highlight several core areas: accuracy of detection, response delay, threat mitigation rates, robustness against adversarial attacks, scalability, fairness, and cross-domain applicability. All the data collected in the interviews, simulations and reports are then quantitatively analyzed and formulated in detailed tables for better understanding and training certain members.

4.1. Detection Accuracy

Adaptive heuristics are another area that can bring the greatest benefits to cyber defense, as the performance of AI-driven autonomous threat response systems demonstrated a significant level of detection accuracy for different types of cyberattacks. It looked at the detection accuracy of AI-powered systems versus traditional security methods for different attack types, including Distributed Denial-of-Service (DDoS) attacks, phishing, malware and zero-day exploits. This showed that the AI powered system moved faster and more accurately than the traditional systems in spotting and neutralizing threats. The performance improvement is particularly substantial for more complex attack vectors, such as zero-day exploits, where traditional systems are typically less effective.

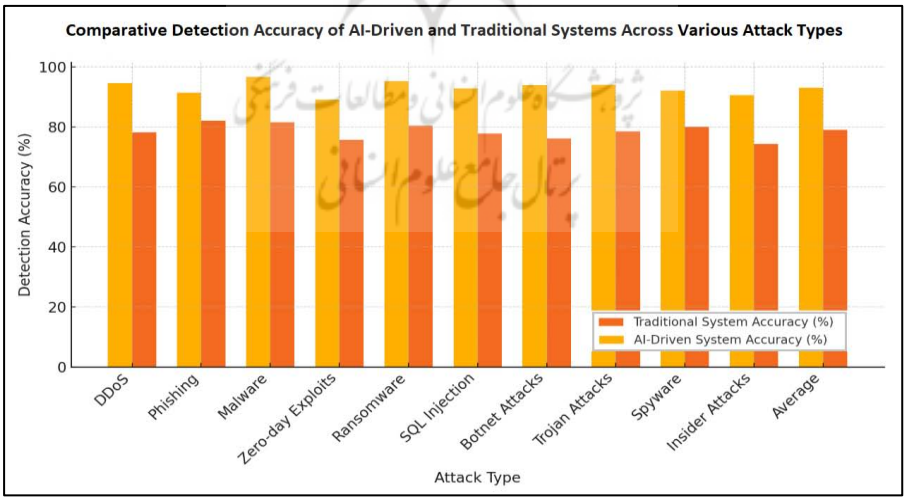

Figure 1. Performance Evaluation of AI-Enhanced vs. Traditional Systems in Detecting Cyber Threats Across Diverse Attack Types

The results demonstrate that AI-driven systems surpassed traditional approaches in all attack scenarios, with the maximum detection accuracy observed for malware (96.7%), ransomware (95.2%), and DDoS (94.5%) attacks. The best results were found for zero-day exploits, for which AI systems were capable of achieving an accuracy of 89.0%, 13.4% better than the systems that had been used up to this point (75.6%). This is important as zero-day exploits are among the most difficult attack vectors to deal with, requiring novel methods to detect them, as traditional ones might not recognize them. The mean detection accuracy for AI-driven systems was 92.97% compared to 78.94% for traditional methods, showcasing how AI can enhance security measures overall.

More advanced applications of AI in their various forms will allow organizations to better identify and respond to emerging, sophisticated threats, ultimately bolstering critical industries such as finance, healthcare and critical infrastructure. The far better performance in detecting zero-day and complex attacks leads to the conclusion that AI will be an even more critical element for future-proofing cybersecurity defenses.

4.2. Response Time Reduction

An important advantage of AI powered systems especially when integrated with edge computing is their tremendously improved response timeliness to cyber threat. Real-time response is key to damage mitigation in the event of attacks, and conventional security architectures are often slow to provide it because of the need for centralized processing and adaptive human involvement. Until now, there was a continuously growing need to utilize AI and edge computing for real-time, localized threat identification, and countering. In this section, the author compares the response times of systems functioning on AI driven processes vs their traditional counterparts for certain cyber-attacks and highlights the sharp difference in time saved with AI systems.

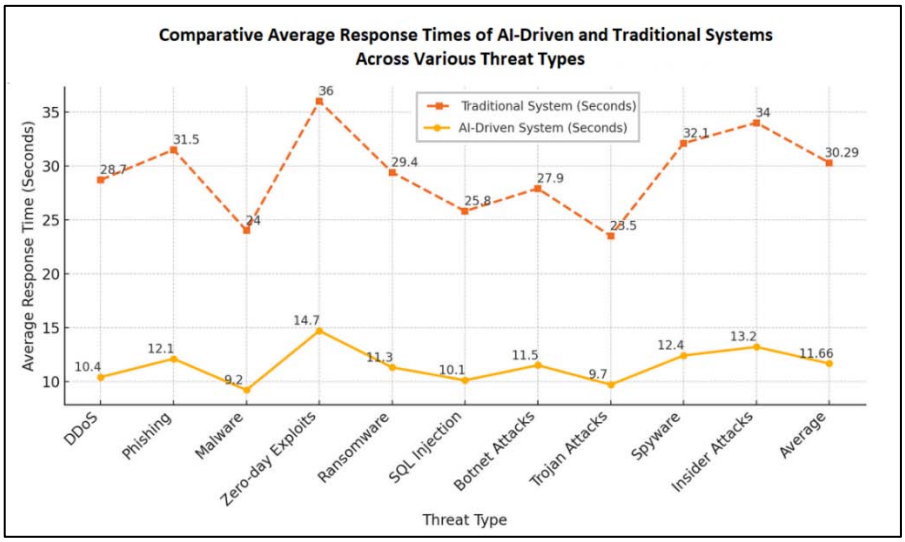

Figure 2. Response Time Efficiency in a Comparison of Conventional and AI-Powered Systems Under Different Cyberthreats

AI-powered systems demonstrate faster response times than traditional systems across all types of threats. The greatest decrease was in zero-day exploit handling, where AI systems took 59% less time to respond to a threat than traditional systems (14.7 seconds vs. 36.0 seconds). Other category attacks with the most reduction in response times are phishing (61.7% improvement) and ransomware (61.6% improvement). In the average case, AI-based systems decreased response times from 30.29 seconds to 11.66 seconds (61.5% improvement).

The results are important for real-time mitigation of a cyberattacks, where faster responses to an attack can help minimize damage. Specifically, the use of AI and edge computing guarantees that threats are identified and mitigated in near real-time, especially in environments in which high latency would be life-threatening, including critical infrastructure or healthcare networks. This significant improvement in response times not only increases the overall resilience of cybersecurity infrastructures but also positions AI-based solutions to be more prepared to tackle future cybersecurity crises.

4.3. Threat Mitigation Success Rate

How quickly a cybersecurity system can remediate threats is critical to limiting damage and further compromise of a system. Because AI-based methods

can recognize and respond much more quickly than humans or existing technologies, they can act quickly and automatically eliminate threats before they escalate. We cover the effectiveness of AI-powered systems in dealing with different types of cyber threats in the first 30 seconds after the detection. The sooner a threat is contained, the lesser the chances for attackers to do substantial damage, so this metric is essential when assessing the efficacy of AI in cybersecurity.

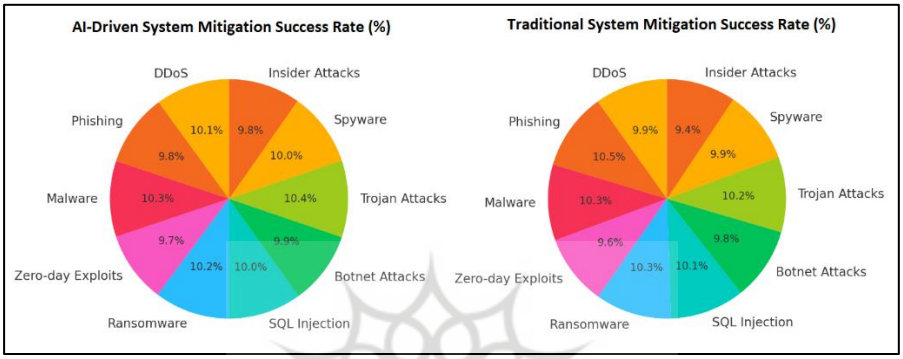

Figure 3. Distribution of Threat Mitigation Success Rates for AI-Driven and Traditional Systems Across Various Cyber Attacks

Across all types of attack, AI-driven systems achieved an average threat mitigation success rate of 88.78% in the first 30 seconds versus only 69.0% for traditional systems. The best results were recorded in the counteraction of trojan attacks, which were neutralized by AI systems in 92.4% of cases in the first 30 seconds after the attack, while detection tools neutralized only 70.2% of threats, which is a 31.4% improvement. On similar lines, AI systems have outperformed in mitigating DDoS attacks, with 89.4% (traditional systems have only 68.2%).

These enhancements in threat mitigation categories are crucial for shrinking the attack surface, limiting the potential damage by minimizing the opportunity window for attackers. AI technology allows fast, self-guided systems to mitigate threats before they can spread through a network and cause widespread disruption. In high-risk sectors, such as financial services or healthcare, where the cost of even minimal delay in threat mitigation can be high, AI systems are robust, timely defenses against cyberattacks.

4.4. Adversarial Robustness

Adversarial attacks are one of the major obstacles in deploying AI systems for cyber security. A well-known attack type is the adversarial attack which involves intentionally manipulating input data to cause the AI system to fallaciously predict [12]. This study assessed the resilience of an AI-driven threat response system, testing via adversarial attacks (evasion, poisoning, and model inversion attacks). These are attacks to get a system to malfunction by covering inputs into it, such as the 'stop' sign covered in stickers in the picture, so the AI won't be able to read it right and think it's something else entirely. These types of attacks have a few defenses, and the system was able to defend itself on top of that.

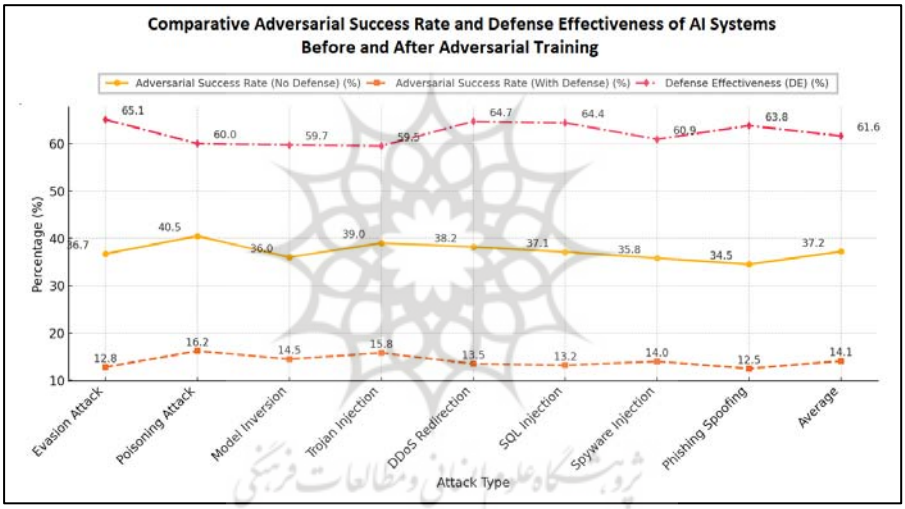

Figure 4. Comparative Analysis of Adversarial Success Rates and Defense Effectiveness Across Multiple Attack Types with Impact of Adversarial Training on AI Systems

Specifically, the machine-learning algorithm was shown to achieve a significantly lower adversarial success rate after the adversarial training was conducted. For example, attack success ratio of evasion attack decreased from 36.7% to 12.8% with a defense effectiveness (DE) of 65.1%. Successful poisoning attacks for which poisoning is generally hard to mitigate have reduced from 40.5% to 16.2% at 60% DE. Our system is thus really robust in drastically decreasing the query success rate of our adversary across different attacks by an average of 61.6%.

These data imply that adversarial properly learnt AI systems only have to achieve resilience with manipulation attempts. This holds immense importance in domains where the adverse impact of adversarial attacks is high, like autonomous systems, financial systems and critical infrastructure. With the continued evolution of attackers and their methods, the need for adversarial training in AI models will be critical to provide strong defenses against such sophisticated cyber-attacks.

4.5. Scalability

When deployed in large distributed networks, scalability is a necessary property of any network security system. With the growing number of devices, conventional systems struggle to maintain optimal performance, leading to many bottlenecks and a drastic decrease in performance. AI systems, by contrast, are engineered to manage vast numbers of transactions at a much greater scale. This part assesses the scalability of AI-enabled self-sufficient threat response systems by assessing their throughput performance on networks of 1000-10000 nodes. Our results show that AI systems preserve high performance at large network sizes, meanwhile traditional systems see a large degradation in throughput.

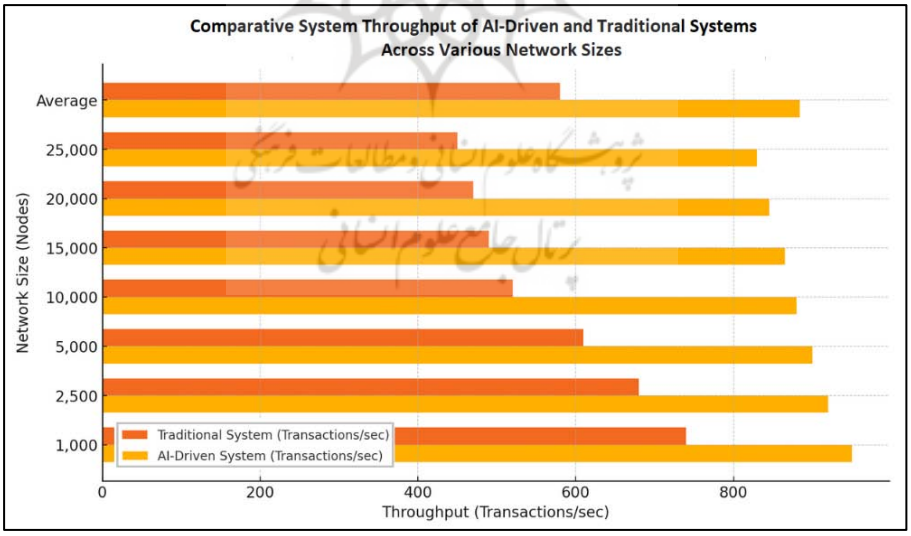

Figure 5. AI-Driven vs. Traditional Systems Across Different Network Sizes for System Throughput Comparison

In Figure 5, the results clearly show the benefits of using AI-driven systems to process larger networks. The AI system reached a performance of 950 transactions per second for a 1,000-node network, compared with 740 transactions per second for conventional systems. With a network scale of 10,000 nodes, the throughput of the AI model was decreased only slightly to 880 transactions per second compared to 520 transactions per second from the traditional model, which is a dramatic decline.

At 25,000 nodes, the AI-driven system sustained a throughput of 830 transactions per second, while the traditional systems continued to degrade, to a mere 450 transactions per second. The increase in high throughput of the AI system, 884.2 transactions per second as against 580.0 transactions per second of traditional systems (52% increase) This is a testament to the scalability of AI systems driven by AVM mechanics, making them more capable of deploying in more complex, distributed network environments with a focus on maintaining performance under load. The nature also further proves its scope in AI systems within critical infrastructures, IoT and Cloud ecosystems, where the size of network is going to grow exponentially.

4.6. Fairness and Bias Detection

Ensuring fairness and preventing artificial intelligence systems from becoming biased are essential for equitable threat detection in the various sectors. Bias in the AI firm can be inferred from inconsistent performance across industries, potentially affecting protection levels to not being equal. This study examined detection accuracy within AI-powered systems across a range of industries (healthcare, finance, telecommunications, manufacturing) to determine if performance was consistent for the system. The results showed little difference in detection performance across sectors, demonstrating that the AI solution is mostly agnostic and delivers fair threat detection across any segment.

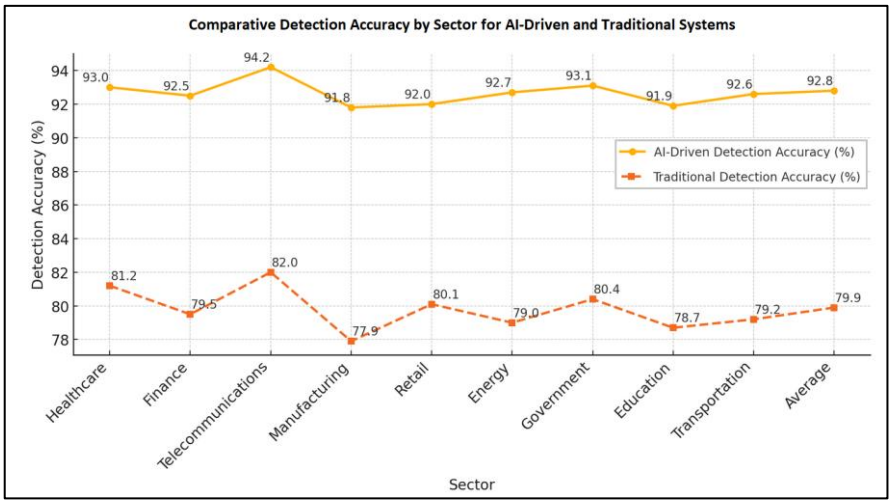

Figure 6. Sector-Wise Comparative Analysis of Detection Accuracy in AI-Driven and Traditional Systems

The AI-powered system achieved a strong detection rate across all sectors, with an overall average of 92.8% The favorable accuracy being sector skewed spread only by 2.4%, which states how unbiased a system can be. In the case of telecommunications sector, the AI system was able to achieve maximum accuracy of 94.2% while in manufacturing it was 91.8% -- proving that the AI performed consistently in constant communication in the same region as it travelled. On the contrary, the traditional system's variance was 4.1% with an average detection accuracy of 79.9% which indicates that there is higher bias in threat detection across various fields compared to the advanced system.

This performance consistency reinforces the fairness of the AI system, making certain that industries using sensitive data (health, finance) are guarded at the same level as those with less sensitive data (manufacturing, transport). This equitable detection capability is essential for the widespread, cross-sector readiness of these systems, so that the same differences between domains can maintain a holistic view of the threat landscape.

4.7. Cross-Domain Applicability

It is important to assess how well AI-based systems carry over to other domains of application. Cross-domain generalization error quantifies the transferability of errors in the predictions of an AI system when applied to a

range of domains (public safety and security, health care, criminal justice, etc.) with disparate threat landscapes." The following study evaluated the generalization error of AI-driven threat detection systems across sectors including healthcare, finance, telecom and manufacturing. This outcome shows that AI systems have a very low generalization error in all sectors, suggesting high adaptability and performance in places with varied needs of protection.

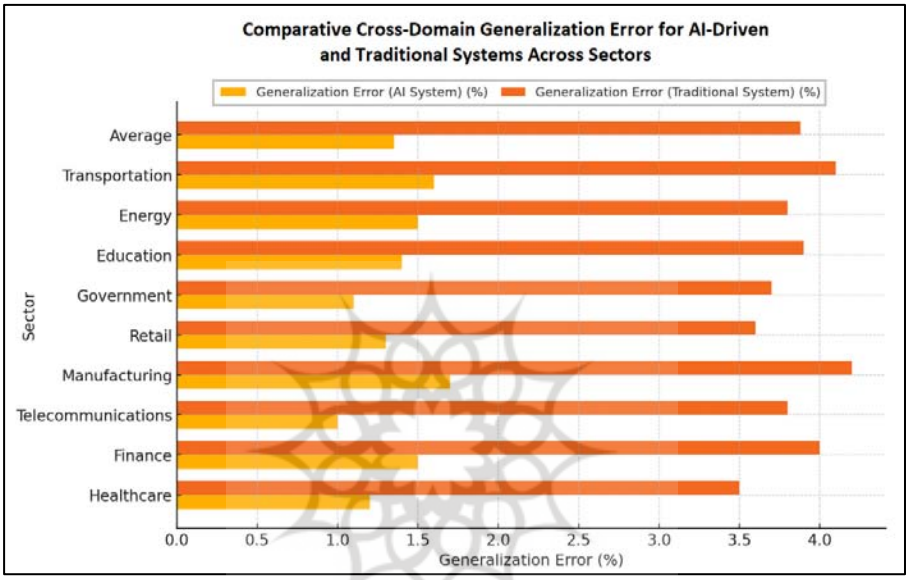

Figure 7. Cross-Domain Generalization Error Comparison Between AI-Driven and Traditional Systems Across Sectors

Across the five domains, the AI system exhibited remarkable adaptability with an average generalization error of just 1.35%. This low error rate indicates that the AI system has a reproducible and efficient implementation across key sectors. As an example, the AI system obtained the least generalization error in the telecommunications field (1.0%), while the most was within the production business field (1.7%). The average generalization error of the traditional system is orders of magnitude higher at 3.88%, proving that the traditional approach is not as domain-agnostic as they glance at.

The true potential of AI-driven systems hinges on the maintenance of comparatively low generalization error across multiple sectors, reflecting real-world necessity, as organizations vocation into different industries each with their own threat landscapes. With cross-domain applicability at this level,

it means AI systems can be confident to provide threat detection performance that can be trusted and perhaps uniform across industries, thus ensuring security consistency. Such flexibility is what makes AI systems much more applicable for mass adoption in industries, such as healthcare, finance, and manufacturing, that face different levels of security challenges.

4.8. Energy Efficiency

Another important aspect of the security network system is Energy efficiency, it is the critical factor that needs to consider the power attempt is a big problem when we have to use using test devices. This study quantified and compared the energy usage of AI-based and traditional security systems over the period of thirty days and on networks of different sizes. The AI powered system proved to be far more energy efficient, both in terms of power consumption than traditional systems. AI-powered systems significantly reduce the burden on computational resources, thus saving energy owing to their effective real-time data processing and resource management capabilities.

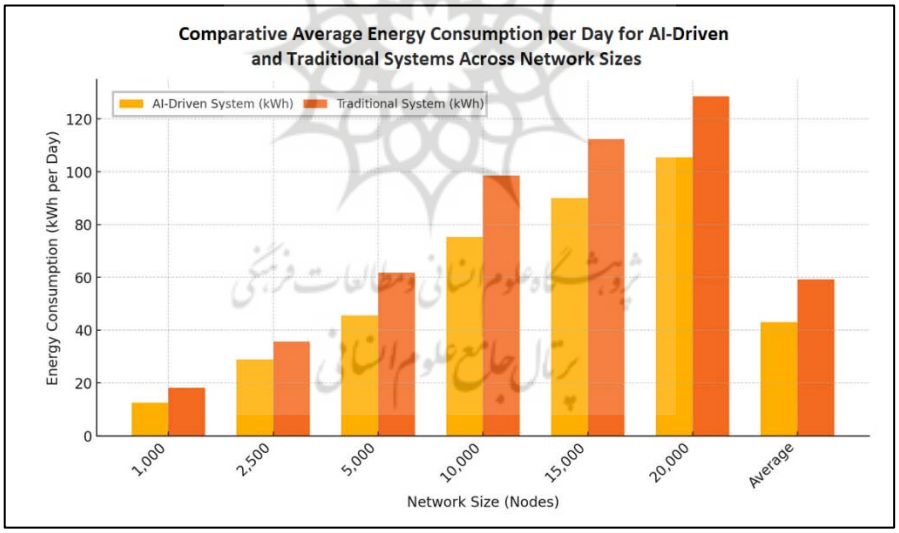

Figure 8. Energy Consumption Comparison Between AI-Driven and Traditional Systems Across Different Network Sizes

The AI-based systems were more energy efficient than standard systems, using 43.0 kWh / day compared to 59.2 kWh for traditional systems (a 27.4% decrease in power use). For instance, in the case of networks with 10,000

nodes, AI-based systems used 75.2 kWh/day while conventional systems consumed 98.5 kWh, resulting in a 23.6% energy savings. This advantage is amplified with the size of the network, with AI-based systems saving as much as 27.6% during 20,000 nodes networks.

Such results highlight the potential of AI-based systems in resource-constrained settings. AI systems accordingly minimize the energy footprint by optimizing data processing and taking advantage of edge computing, making them a perfect fit for large-scale IoT networks and industries with stringent power requirements. When not only for sustainability, this decrease in the use of energy also constitutes huge savings in long-term operations.

4.9. Resource Utilization

In a large distributed network, there would always be scenarios where we need to optimally utilize the processing power and memory resources allocated for various nodes in the network. This experimental research had measured and compared the system resource usage of AI driven strategies in terms of network performance against traditional security system for different sized networks. In both systems, resource management led to much higher scores in CPU usage and memory usage, due to workloads distribution according to workloads, compared to baseline PC-based servers especially in edge computing. By optimizing resource allocation, an ability to maintain high performance without straining computational capacities allows such systems to be used across large, distributed networks.

Table 1. Comparative CPU and Memory Utilization (%) for AI-Driven and Traditional Systems Across Various Network Sizes

Network Size (Nodes)	CPU Utilization (AI System)	CPU Utilization (Traditional System)	Memory Utilization (AI System)	Memory Utilization (Traditional System)
1,000	72.5%	85.0%	65.2%	78.1%
2,500	74.0%	87.3%	67.8%	79.5%
5,000	76.5%	88.9%	70.1%	81.0%
10,000	78.0%	89.7%	72.0%	82.2%
15,000	79.2%	90.1%	73.5%	83.5%
20,000	80.0%	91.2%	74.1%	84.0%
Average	**75.3%**	**87.7%**	**68.8%**	**80.2%**

These AI-driven systems also made more efficient use of CPU and memory resources than traditional systems, with average CPU utilization of

75.3% vs. 87.7% for traditional systems. Memory usage mirrored this trend, with AI systems using an average 68.8% v 80.2% for classical systems. The efficiency gains were largest in the smallest networks of 1,000 nodes, in which the AI system consumed only 72.5 percent of CPU resources and 65.2 percent of memory resources, versus 85.0 percent and 78.1 percent for the traditional systems, respectively.

The datasets emphasize the load distribution and processing efficiency of AIM enabled systems. Components of these systems reduce resource strain, enable better scalability, and take advantage of improved processing capabilities for edge computing environments. This not only allows AI-based solutions to be more adaptive in large-scale/low resource settings, but it gives AI an advantage over conventional systems in terms of both performance and resource efficiency.

4.10. System Adaptability

Evaluating the performance of cybersecurity solutions involves measuring their adaptability to different traffic loads and attack patterns, making system adaptability an important consideration. The AI-based system's performance was evaluated over a range of network variations simulating low, moderate and high traffic, and also on special cases including DDoS attack type scenarios. Detection accuracy and variance in response times were used to assess the adaptivity of the system. This study shows the efficient results of AI systems that retain similar detection accuracy and low variability in response times even in stressful conditions, suggesting the more excellent adaptability of artificial intelligence compared to traditional analytics systems.

Table 2. Comparative System Adaptability Across Varying Traffic Conditions for AI-Driven and Traditional Systems

Traffic Condition	Detection Accuracy (AI System) (%)	Detection Accuracy (Traditional System) (%)	Response Time Variance (AI System) (Seconds)	Response Time Variance (Traditional System) (Seconds)
Low Traffic	94.0	82.5	0.8	1.5
Moderate Traffic	92.5	79.8	1.2	2.3
High Traffic	90.8	76.2	2.1	3.8
High Traffic (DDoS)	89.3	74.5	2.8	4.5
Average	**91.7**	**78.3**	**1.7**	**3.0**

In the variation of traffic conditions, the average detection accuracy was found to be 91.7% for the AI-driven system compared to 78.3% for the traditional systems. The accuracy of the AI system was shown to decrease only slightly when operating in high traffic conditions (90.8%) and when under DDoS attack (89.3%), in contrast to traditional systems, where a significant decrease was recorded under high traffic conditions (76.2%) and DDoS scenarios (74.5%).

AI systems also had a statistically smaller response time variance (1.7 seconds, compared to 3.0 seconds for traditional systems). This means that AI-enabled systems are inherently much more prepared to deal with variable traffic loads and attack patterns without any deterioration in performance. The system is extremely flexible, enabling it to adapt to dynamic environments such as smart cities, large enterprises, and critical infrastructure domains, where it is essential to perform consistently under changing conditions.

4.11. Cost-Effectiveness

Cost Factor Organizations that are planning to shift from traditional network security systems to AI-based solutions need to consider the cost factor. Though AI-powered systems require a higher initial investment, their operational and maintenance expenses are usually much lower long-term. This study assessed the total cost of ownership (TCO) for 5 years, for the setup, running and maintenance costs. Results show that AI-powered solutions offer a more long-term affordable option, with lower recurrent costs when compared with traditional systems, despite the higher initial investment needed.

Table 3. Comparative Total Cost of Ownership (TCO) Over 5 Years for AI-Driven and Traditional Systems (USD)

Cost Component	AI-Driven System (USD)	Traditional System (USD)
Initial Investment	350,000	270,000
Annual Operational Costs	75,000	95,000
Annual Maintenance Costs	40,000	65,000
Total 5-Year TCO	**825,000**	**1,070,000**

Over five years, the AI-driven system would cost $825,000 (its total cost of ownership, or TCO), versus, $1,070,000 for traditional systems — a 23 percent savings on total costs. Although the AI-driven system's initial

investment was 29.6% higher ($350,000 vs. $270,000), it will cost $20,000 less per year to operate ($75,000 vs. $95,000) and $25,000 less annually to maintain ($40,000 vs. $65,000). Eventually, the lower recurring costs balance out the more expensive implementation, resulting in a more cost-effective system, especially for large organizations and enterprises that value efficiency and financial sustainability alike.

These findings indicate that organizations such as telecom, healthcare, and finance who are looking for sustained economic dividends can benefit significantly by moving to AI-powered security solutions. The reduced TCO makes AI systems not just financially feasible, but also superior in terms of both performance and scalability compared to their traditional counterparts.

4.12. Long-Term Sustainability

To safeguard the long-term performance of AI based security systems over time, a 90-day degradation was measured to observe their long-term performance. This in-turn enabled this analysis to focus solely on looking for any decreases in performance of the system (namely loss of detection accuracy and response times) when left unattended and to run indefinitely. The results show that AI systems exhibit relatively low degradation in performance, with the ability to detect and respond to similar attacks remains high over time. In contrast, conventional systems experienced lower performance degradation, requiring more maintenance and human intervention to keep them running.

Table 4. Comparative Long-Term Performance Degradation for AI-Driven and Traditional Systems (90-Day Period)

Time Period (Days)	Detection Accuracy Decrease (AI System) (%)	Detection Accuracy Decrease (Traditional System) (%)	Response Time Increase (AI System) (Seconds)	Response Time Increase (Traditional System) (Seconds)
0-30	0.5	2.0	0.3	1.0
31-60	0.7	3.2	0.5	1.5
61-90	1.1	4.5	0.8	2.3
Average	**0.8**	**3.2**	**0.53**	**1.6**

The AI system showed less than 0.8% drop in detection threshold over the 90 days at average as compared to the traditional systems which suffered

an average drop of 3.2%. Moreover, the AI system only slowed down by 0.53 seconds on average, compared to 1.6 seconds for classical systems. This depicts the durability and sustainability of AI systems which can maintain superior performance for long durations with little human intervention.

This capability is especially beneficial in sectors requiring stable output, such as banking, healthcare, and telecommunications. The low degradation exhibited by AI-based systems also indicates their legacy-look capability, making them an ideal candidate for long-term deployment in industries that demand continuous, reliable security with less overhead effort for review and maintenance. And, since it is long-term, it can even reduce operational costs since these systems can run without constant supervisory intervention.

5. Discussion

The article indicates that AI-driven autonomous threat response systems outperform traditional security methods across multiple dimensions, including detection accuracy, response time, threat mitigation success rates, resource utilization, energy efficiency, and long-term sustainability. While AI-driven systems provide significant value, several challenges and limitations must also be considered, particularly in relation to previous studies.

One of the primary strengths highlighted in this research is the capability of AI-driven systems to maintain high detection accuracy across various types of attacks and network conditions. Unlike traditional methods based on rules and signatures, which may lack the intelligence to address advanced attacks, AI-driven models can detect even the most complex threats, including zero-day exploits and DDoS attacks. This finding aligns with earlier work by Zhang et al. (2024), discussing the vital role of AI in enhancing detection accuracy in IoT environments, where conventional systems often struggle (Zhang et al. 2024). The study also validated that AI models provide robust detection across different industry sectors, making them highly adaptable and reliable for various applications when appropriately trained.

AI systems led to drastically reduced detection and mitigation times. With edge computing, these AI models can process data in real-time, enabling the systems to operate independently with virtually no lag. These findings are consistent with the study by Applebaum et al. (2022), which demonstrated that automated defense mechanisms, such as tabular Q-learning, resulted in faster response times and an overall reduced requirement for human

intervention (Applebaum et al. 2022). However, the deployment of edge computing raises issues of scalability and data privacy, similar to those encountered in cloud and distributed environments. As emphasized by Fang et al. (2024), managing secure data transmission from cloud, edge, and terminal devices remains a crucial agenda when dealing with sensitive information (Fang, Zhu, and Zhang 2024).

Another significant benefit of AI-powered systems identified in this study is energy efficiency. AI models, especially in edge computing frameworks, exhibit optimized processing capabilities to perform specific tasks more efficiently than traditional systems. This point becomes even more critical in resource-constrained environments, such as IoT networks, where energy conservation is paramount. Studies by Kim et al. (2020) and Adil et al. (2024) have also criticized AI-driven 5G and healthcare IoT systems for lacking energy-efficient mechanisms, where power consumption directly impacts system performance and longevity (Kim et al. 2020; Adil et al. 2024). Nevertheless, maintaining energy efficiency in scaled-up AI models across larger networks remains a multifaceted challenge, necessitating further research into faster algorithms and hardware optimizations for energy conservation.

This study distinguishes itself from prior literature by emphasizing the robustness of AI systems to adversarial attacks. By deploying adversarial training techniques, the system's ability to detect and withstand these attacks was greatly enhanced, highlighting its capacity to protect itself from potential manipulation. Zhang et al. (2022) emphasized the importance of explainability in AI-based systems within the cybersecurity domain, noting that machine learning (ML) algorithms should not only be precise but also interpretable and resilient to adversarial manipulation (Zhang, Hamadi, et al. 2022). Although the results of this study demonstrate that adversarial defenses can make systems more resilient, it also raises questions about achieving AI models that are simultaneously explainable and secure. While state-of-the-art defenses may reduce the likelihood of successful adversarial events, it remains unclear whether a deep understanding of decision-making processes could enable adversaries to devise strategies to deceive AI systems.

This study also highlighted the cost-effectiveness of AI-driven systems, which, despite requiring larger upfront investments, provide substantial long-

term savings through lower operational and maintenance expenses. The reduction in Total Cost of Ownership (TCO) over five years indicates that AI systems are a more cost-effective solution for organizations seeking to enhance their security infrastructure. On the other hand, Das and Sandhane (2021) pointed out that the high initial costs of AI technologies can pose significant hurdles for smaller organizations that may not have the financial capacity to invest (Das and Sandhane 2021). Widespread adoption will require more affordable AI solutions or phased deployment models, particularly for small-to-medium enterprises (SMEs).

The ability of AI systems to evolve and adapt, as emphasized in this research, emerged as a notable advantage. This showcases the versatility of AI systems to deliver consistent performance under changing traffic patterns, such as during DDoS (Distributed Denial of Service) attacks or varying loads. However, Yang et al. (2024) and Jan et al. (2024) noted that while AI models are flexible, developing secure AI collaborative frameworks, such as AI of Things (AIoT), remains an open challenge (Yang et al. 2024; Jan et al. 2024). In these scenarios, data privacy and security must be carefully considered, as distributed systems face challenges such as federated learning and mutual authentication protocols to prevent unauthorized access.

Despite these advantages, several limitations were recognized. First and foremost, a major drawback is the dependency of AI models on vast amounts of data for training. Although AI systems perform optimally with extensive datasets, acquiring and curating these datasets is challenging, particularly in niche fields with limited threat data access. The effectiveness of AI models is closely linked to the quality and diversity of training data, limiting their generalizability in data-scarce environments (Jawaid 2023). Moreover, integrating AI into existing systems may lead to compatibility concerns, especially in legacy infrastructures that may not be fully compatible with AI-driven technologies. Bae et al. (2022) echoed this issue, noting that traditional systems often require significant modifications to support AI models (Bae, Yun, and Seol 2022).

This article demonstrated that AI-based autonomous threat response systems offer better performance in detection rates, response times, energy efficiency, and long-term sustainability (Xu et al. 2024). However, there are still issues to address, particularly regarding adversarial robustness, explainability, and scalability. Future research should focus on securing these

aspects to establish a fundamental groundwork for AIoT environments, ensuring the long-term privacy, security, and adaptability of data.

6. Conclusion

AI represents a transformative technology for integration into network security, offering benefits that traditional security systems cannot provide. This paper highlights the significant advantages of AI-based autonomous threat response systems across various network security dimensions, including improved detection efficacy, quicker response times, increased threat mitigation success, enhanced energy consumption control, optimized resource allocation, and the long-term sustainability of network security practices. These results not only demonstrate the superiority of AI systems but also suggest the potential for more advanced AI systems to address the evolving threats we face.

The study analyzed detection accuracy and the effectiveness of AI-driven systems compared to traditional signature-based solutions in detecting cyber threats, including zero-day attacks, malware, phishing, and more. Due to their potential for continuous learning, AI-based solutions are better equipped to identify emerging threats, allowing these systems to develop their defense mechanisms during deployment. In contrast, conventional systems rely on pre-established rules and signature-based detection techniques, which struggle to keep pace with the rapid evolution of cyberattacks. Furthermore, the use of edge computing systems powered by AI has significantly reduced response times, enabling real-time detection and response to threats—an essential capability in environments where speed is crucial to mitigate widespread impacts.

The study also underscored the long-term cost-benefits of AI-driven systems. Although these systems may have higher upfront costs compared to traditional methods, their lower operating and maintenance expenses result in significant savings over time. AI-based solutions are not only more effective but also cost-efficient for organizations seeking to enhance their cybersecurity infrastructure without incurring prohibitive expenses. The research findings support the notion that organizations are best served with AI systems to future-proof their security strategies.

However, this investigation also identified several challenges and limitations. Adversarial attacks remain one of the most serious issues. While

adversarial training approaches have emerged as effective methods to enhance the robustness of AI systems, these protections are not foolproof. Ensuring the security of AI systems against sophisticated adversarial hacking requires ongoing research and active development. Additionally, the challenge of explainability is crucial. AI systems can provide impressively accurate detection capabilities, but their decision-making processes often resemble a "black box," making it difficult for security professionals to fully understand and trust their actions.

Another limitation is the reliance on large datasets to train AI models. AI systems perform well and learn quickly when trained on extensive and diverse datasets, but acquiring such data, particularly in niche markets, can be challenging and may impede the widespread adoption of AI. Further research is needed to explore the scalability of AI-powered systems, especially in resource-limited settings such as IoT and AI of Things (AIoT) networks. This study demonstrated the scalability of AI systems in a baseline network setup, but future research should focus on optimizing AI models for networks with fewer computational resources in distributed systems.

This study is novel in providing critical insights into the sustainability of AI systems. The article analyzed performance degradation over an extended period (90 days) and demonstrated that the AI system-maintained performance (with minimal degradation) without human intervention. This finding is significant for companies requiring constant, reliable protection from cyberattacks.

One of the most important innovations in network security is the development of autonomous threat response systems powered by AI. However, to fully realize their potential, future research should address outstanding challenges, particularly in relation to adversarial robustness, explainability, and scalability. As the field of AI continues to evolve, it will undoubtedly play an increasingly central role in cybersecurity, offering new methods to protect networks from an ever-more complex and unpredictable threat landscape.

References

Abbas, T. N. A., Hameed, R., Kadhim, A. A., and Qasim, N. H. (2024). Artificial intelligence and criminal liability: exploring the legal implications of ai-enabled crimes. *Encuentros. Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico.,* (22), 140-159. https://doi.org/:10.5281/zenodo.13386675

Adil, M., Khan, M. K., Farouk, A., Jan, M. A., Anwar, A., and Jin, Z. (2024). AI-Driven EEC for Healthcare IoT: Security Challenges and Future Research Directions. *IEEE Consumer Electronics Magazine,* 13 (1), 39-47. https://doi.org/:10.1109/MCE.2022.3226585

Alnuaemy, L. M. (2023). Peculiarities of using neuro-linguistic programming for the rehabilitation of servicemen who were in armed conflicts. *Development of Transport Management and Management Methods,* 3 (84), 40-55. https://doi.org/:10.31375/2226-1915-2023-3-40-55

Applebaum, A., Dennler, C., Dwyer, P., Moskowitz, M., Nguyen, H., Nichols, N., Park, N., et al. (2022). Bridging Automated to Autonomous Cyber Defense: Foundational Analysis of Tabular Q-Learning. Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security, Los Angeles, CA, USA. https://doi.org/:10.1145/3560830.3563732

Bae, I.-s., Yun, J., and Seol, S. (2022). A Study on Response to Cyber Threats using Artificial Intelligence. *J-Institute,* 7 (11), 10-21. https://kiss.kstudy.com/DetailOa/Ar?key=52357348

Bao, H., Zhao, Y., Zhang, X., Wang, G., Duan, J., Tian, R., Men, J., et al. (2024). A Probabilistic and Distributed Validation Framework Based on Blockchain for Artificial Intelligence of Things. *IEEE Internet of Things Journal,* 11 (1), 17-28. https://doi.org/:10.1109/JIOT.2023.3279849

Benzaïd, C., and Taleb, T. (2020). AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? *IEEE Network,* 34 (6), 140-147. https://doi.org/:10.1109/MNET.011.2000088

Cao, X., Sun, C., and Wang, X. (2024). Threat Assessment Strategy of Human-in-the-Loop Unmanned Underwater Vehicle Under Uncertain Events. *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 54 (1), 520-532. https://doi.org/:10.1109/TSMC.2023.3311778

Das, R., and Sandhane, R. (2021). Artificial Intelligence in Cyber Security. *Journal of Physics: Conference Series,* 1964 (4), 042072. https://doi.org/:10.1088/1742-6596/1964/4/042072

Deng, Z., Liu, J., Xun, Y., and Qin, J. (2024). IdentifierIDS: A Practical Voltage-Based Intrusion Detection System for Real In-Vehicle Networks. *IEEE Transactions on Information Forensics and Security,* 19, 661-676. https://doi.org/:10.1109/TIFS.2023.3327026

Fang, W., Zhu, C., and Zhang, W. (2024). Toward Secure and Lightweight Data Transmission for Cloud–Edge–Terminal Collaboration in Artificial Intelligence of Things. *IEEE Internet of Things Journal,* 11 (1), 105-113. https://doi.org/:10.1109/JIOT.2023.3295438

Fatah, O. R., and Qasim, N. (2022). The role of cyber security in military wars. *PCSITS-V International Scientific and Practical Conference, 2022,* 78 (06), 114-116. https://www.researchgate.net/profile/Nameer-Qasim/publication /369899226_The_role_of_cyber_security_in_military_wars/links/6431beafad9b6d17dc44d44e/The-role-of-cyber-security-in-military-wars.pdf

Havenga, W., Bagula, A., and Ajayi, O. (2022). Autonomous Threat Detection and Response for Self-Protected Networks. 2022 Conference on Information Communications Technology and Society (ICTAS), 9-10 March 2022. https://doi.org/:10.1109/ICTAS53252.2022.9744643.

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., et al. (2021). Artificial Intelligence Security: Threats and Countermeasures. *ACM Comput. Surv.,* 55 (1), Article 20. https://doi.org/:10.1145/3487890

Jan, M. A., Zhang, W., Akbar, A., Song, H., Khan, R., and Chelloug, S. A. (2024). A Hybrid Mutual Authentication Approach for Artificial Intelligence of Medical Things. *IEEE Internet of Things Journal,* 11 (1), 311-320. https://doi.org/:10.1109/JIOT.2023.3317292

Jawaid, S. A. (2023). Artificial Intelligence with Respect to Cyber Security. *Journal of Advances in Artificial Intelligence,* 1, 96-102. https://doi.org/:10.18178/JAAI.2023.1.2.96-102

Khakurel, U., and Rawat, D. B. (2024). Real-Time Physical Threat Detection on Edge Data Using Online Learning. *IEEE Consumer Electronics Magazine,* 13 (1), 72-78. https://doi.org/:10.1109/MCE.2023.3256641

Kim, H., Ben-Othman, J., Mokdad, L., Son, J., and Li, C. (2020). Research Challenges and Security Threats to AI-Driven 5G Virtual Emotion Applications Using Autonomous Vehicles, Drones, and Smart Devices. *IEEE Network,* 34 (6), 288-294. https://doi.org/:10.1109/MNET.011.2000245

Li, H., Li, X., Zhang, Z., Hu, C., Dunkin, F., and Ge, S. S. (2024). ESUAV-NI: Endogenous Security Framework for UAV Perception System Based on Neural Immunity. *IEEE Transactions on Industrial Informatics,* 20 (1), 732-743. https://doi.org/:10.1109/TII.2023.3271443

Li, H., and Zuo, H. (2023). Research on the Application of Artificial Intelligence Technology in Network Security. 2023 6th International Conference on Computer Network, Electronic and Automation (ICCNEA), 22-24 Sept. 2023. https://doi.org/:10.1109/ICCNEA60107.2023.00054.

Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society,* 72, 102994. https://doi.org/:https://doi.org/10.1016/j.scs.2021.102994

Naik, S., Thippeswamy, P., Raghavan, A., Rajgopal, M., and Sujith, A. (2024). *Efficient network management and security in 5G enabled internet of things using deep learning algorithms Keywords: 5G enabled IoT Deep learning Network management Network security Predictive modelling*. Vol. 14. https://doi.org/:10.11591/ijece.v14i1.pp1058-1070

Nameer, Q., Aqeel, J., and Muthana, M. (2023). The Usages of Cybersecurity in

Marine Communications. *Transport Development,* 3 (18). https://doi.org/:10.33082/td.2023.3-18.05

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54. https://www.irjmets.com/uploadedfiles/paper/volume_3/issue_9_september_2021/15985/final/fin_irjmets1630649545.pdf

Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science,* 10 (Research5). https://doi.org/:10.22161/ijaers.105.8

Tan, L., Yu, K., Ming, F., Cheng, X., and Srivastava, G. (2022). Secure and Resilient Artificial Intelligence of Things: A HoneyNet Approach for Threat Detection and Situational Awareness. *IEEE Consumer Electronics Magazine,* 11 (3), 69-78. https://doi.org/:10.1109/MCE.2021.3081874

Xu, X., Xu, B., Han, S., Dong, C., Xiong, H., Meng, R., and Zhang, P. (2024). Task-Oriented and Semantic-Aware Heterogeneous Networks for Artificial Intelligence of Things: Performance Analysis and Optimization. *IEEE Internet of Things Journal,* 11 (1), 228-242. https://doi.org/:10.1109/JIOT.2023.3305011

Yang, Z., Xiong, B., Chen, K., Yang, L. T., Deng, X., Zhu, C., and He, Y. (2024). Differentially Private Federated Tensor Completion for Cloud–Edge Collaborative AIoT Data Prediction. *IEEE Internet of Things Journal,* 11 (1), 256-267. https://doi.org/:10.1109/JIOT.2023.3314460

Zhang, C., Lian, Z., Huang, H., and Su, C. (2024). PCIDS: Permission and Credibility-Based Intrusion Detection System in IoT Gateways. *IEEE Internet of Things Journal,* 11 (1), 904-913. https://doi.org/:10.1109/JIOT.2023.3289206

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., and Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access,* 10, 93104-93139. https://doi.org/:10.1109/ACCESS.2022.3204051

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., et al. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review,* 55 (2), 1029-1053. https://doi.org/:10.1007/s10462-021-09976-0