Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 8, 2025

ANALYZE THE IMPACT OF ARTIFICIAL INTELLIGENCE, NETWORK ARCHITECTURE, AND HUMAN ERROR ON CYBERSECURITY THREAT DETECTION

Aysha Ijaz Khan[*1], Muhammad Ayaan Ejaz[2], Arsal Umer Shami[3]

[*1]MS (Computer Science), Comsats University
[2]Aitchison College
[3]Lahore American School

[*1]ayshakhan23@gmail.com, [2]ayaanejazsahi1@gmail.com, [3]arquaza7@gmail.com

DOI: https://doi.org/10.5281/zenodo.16916951

Keywords
Artificial Intelligence, Cyber-security, Threat Detection, Network Architecture, Human Error, Machine Learning, Zero Trust, ANOVA

Article History
Received: 19 Mayl, 2025
Accepted: 24 July, 2025
Published: 21 August, 2025

Corresponding Author: *
Aysha Ijaz Khan

Abstract

Sometimes, conventional threat detection systems are inadequate given the growing complexity and frequency of cyber-attacks. One strong approach to improve threat detection skills has emerged from the incorporation of Artificial Intelligence (AI). Network design and the continuing part of human error in cyber security breaches, however, affect the efficacy of artificial intelligence.This study seeks to investigate how human elements, various network architectures, and artificial intelligence-based systems collectively affect the efficacy and precision of cyber security threat detection. A cross sections study design was carried out, using simulated corporate network environments across three architectures: flat, segmented, and zero trust. AI algorithms including machine learning-based anomaly detection and behavior analysis tools were used throughout these settings, With real-time logging of security incidents and response accuracy, data were gathered six months. Human error data were collected using structured incident reporting forms from 100 cyber security professionals aged 25–55 years. Stratified random sampling was used to ensure representativeness across organizational types. Statistical analysis using logistic regression and ANOVA evaluated the individual and cumulative influences of human error, network architecture, and AI performance on threat detection rates. In zero trust topologies, AI-enhanced systems achieved an average detection accuracy of 94.6%; in segmented networks, 88.3%; and in flat networks, 72.5%.Statistical analysis verified that both network architecture and human error significantly affected AI performance ($p < 0.01$). Although AI greatly enhances cyber security threat detection, its efficiency depends much on strong network infrastructure and diminished human error. Forty-one percent of missed or delayed threat responses were attributed to human mistake, mostly resulting from alert misinterpretation or delayed escalating. To attain resilient cyber security, organizations need to use whole security approaches combining best network design, advanced artificial intelligence tools, and extensive human training.

INTRODUCTION

The increasing complexity and frequency of cyber-attacks present a major problem in all around. Relying on static rule based systems, conventional security systems frequently have difficulties spotting new or changing threats (Moustafa et al., 2019). Artificial Intelligence (AI) and machine learning (ML) enable security frameworks to use anomaly detection, pattern recognition, and predictive analytics to identify and respond to cyber threats in near real time (Buczak & Guven, 2016).

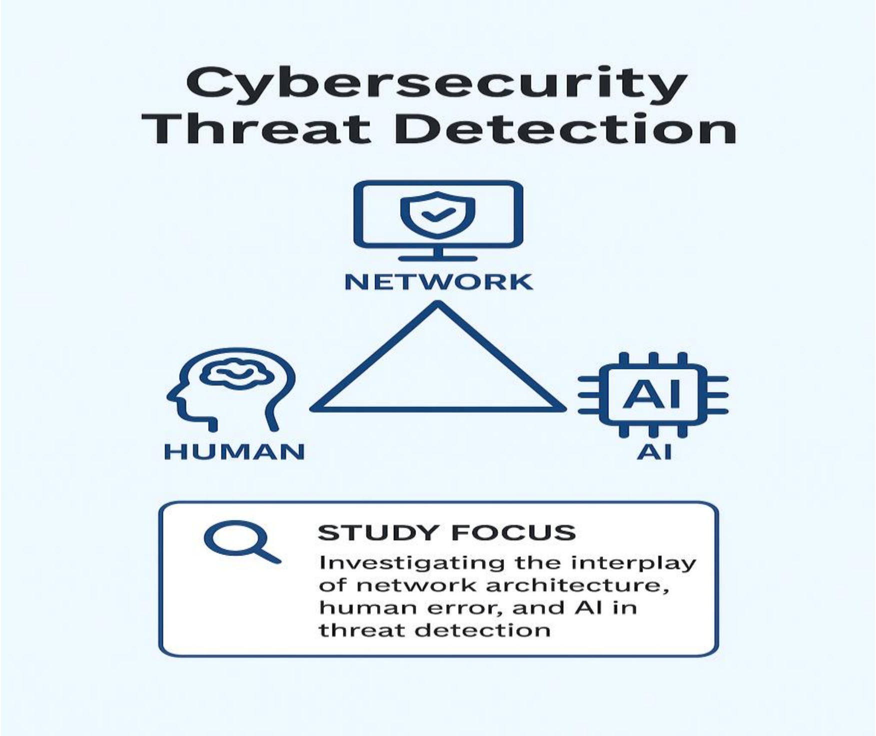
The performance of artificial intelligence, however, is not independent; it is impacted by the underlying network infrastructure the design and segmentation of the network greatly affects the scope and quality of data accessible for AI systems (Salah et al., 2019). Flat networks expose the whole infrastructure to breaches, segmented networks limit lateral movement of attackers, while zero trust architectures enforce strict identity verification, minimizing exposure (Kindervag, 2010).

Human error is still a major vulnerability in Cyber-security notwithstanding technical developments.Studies show that a major part of breaches is caused by mis-configurations, slow incident responses, and incorrect alert interpretation (Verizon, 2023). Developing comprehensive Cyber-security measures calls for an awareness of the combined effects of human error, network architecture, and AI capability.

Cyber-security has become a national and business priority from being a concern only for IT.Organisations are progressively using AI-driven threat detection solutions to supplement conventional techniques as cyber-attacks become more intricate (Sommer &amp; Paxson, 2010). By continuously learning from historical and realtime information, artificial intelligence helps to detect complex attack vectors.

Still, the network design in which artificial intelligence runs will affect its effectiveness in threat identification. Flat architectures, on the other hand, offer greater attack surfaces and could impede AI's capacity to isolate threats. Cutting down on false positives and limiting enemy movements, zero trust architectures have been shown to maximize the possibilities of artificial intelligence (Rose et al.,2020).

Furthermore slowing escalation, operator supervision, and warning fatigue can hamper even the most advanced artificial intelligence (Hadlington, 2017).This study examines with the aim of providing insights for more resilient security frameworks how human error interacts with AI-based systems, network architecture, and cyber-security threat detection.


Cybersecurity
Threat Detection
NETWORK
HUMAN
AI
AI
STUDY FOCUS
Investigating the interplay of network architecture, human error, and AI in threat detection

AI in Cyber-security Threat Detection

Artificial intelligence and machine learning approaches including deep learning, supervised classification, and anomaly detection have changed threat detection (Buczak & Guven, 2016).Faster than signature-based systems, AI models discover polymorphic malware and zero-day vulnerabilities (Shaukat et al., 2020). But problems like dataset bias and adversarial machine learning can influence detection accuracy (Demertzis et al., 2022).

Security and Network Architecture

Many view network segmentation as a crucial security approach helping to restrict attack propagation (Salah et al., 2019). Going even further, Zero trust models, originally developed by Kindervag (2010), eliminate implicit trust and demand constant authentication. Studies show that zero trust architecture with artificial intelligence produces better detection accuracy than flat or segmented networks (Kandek, 2021).

Cybersecurity Human Error

Though it cannot eradicate human error, artificial intelligence can lower its consequences, therefore education and awareness are crucial (Sasse et al., 2001). Among the causes are misconfiguration flaws, inadequate training, and alert fatigue (Hadlington, 2017). Verizon reports that more than 80% of reported security breaches include human error (Verizon, 2023).

Gaps in Research

Though less research has looked at their synergistic impact with human error on threat detection performance, artificial intelligence and network architecture have been examined independently; therefore, integrative analysis is needed.

Methodology:

This research used a cross sectional design to assess the synergistic impact of artificial intelligence systems, network design, and human error on the precision and efficiency of Cyber-security threat detection. The studies was carried out in simulated corporate network settings reproducing actual organizational structures.Three different network designs were modeled: flat, segmented, and zero trust, each built to mirror industry-standard procedures in terms of security setup, access control, and data flow.These architectures were chosen to encompass the range of organizational cyber-security preparedness, from minimal segmentation to advanced trust-based frameworks

Real-time monitoring and threat detection were achieved using AI-driven cyber security solutions within every network model.Based on machine learning, these systems included behavioral analysis tools trained on vast dataset of benign and malicious network traffic as well as anomaly detection algorithms.To identify aberrant data flow patterns, unauthorized access attempts, and potential inside threats, the artificial intelligence algorithms were calibrated.To guarantee validity and consistency, every simulated environment experienced the same series of cyber attack scenarios including phishing, ransomware injection, lateral movement attempts, and denied of service simulations.To evaluate the resilience and adaptability of the artificial intelligence systems over architectures, the attacks were carried out at different levels of sophistication.

Over six months, all network activity, security breaches, and system reactions were consistently recorded as part of data collecting. Detection accuracy, false positive rates, response times, and escalation patterns were among the main performance indicators.Along with overall system performance, human factors were incorporated into the study strategy.Structured incident reporting activities involving 100 cyber-security experts between the ages of 25 and 55 were done. Participants were asked to recognize, analyze, and escalate potential threats utilizing simulated alerts generated within the system.Standardized reporting forms developed to record misinterpretation, delays, or omissions in threat handling helped to document their answers.Stratified random sampling guaranteed that participants reflected a broad spectrum of organizational backgrounds, spanning technology, healthcare, government, and finance.

Human participants were selected based on professional experience of at least three years in cyber-security operations, present employment in a network security position, and readiness to engage in simulated threat response exercises. Individuals without three years of practical experience, those not working in cyber-security roles, and those unwilling to finish all study phases were eliminated.All volunteers gave informed consent prior participation; confidentiality of responses was preserved throughout the research.

Statistical analyses were conducted using SPSS version 28. Logistic regression was employed to determine the predictive power of network architecture, AI performance, and human error on detection success. One-way ANOVA was applied to compare differences in detection accuracy across the three network architectures, while interaction effects between human error and network design were tested to identify compounding vulnerabilities. A significance threshold of $p < 0.05$ was established for all statistical tests. The methodological framework was designed to capture both the technical efficiency of AI-enhanced cyber-security systems and the human and infrastructural factors that influence their performance in real-world scenarios.

Results:

Table 1: Demographic Characteristics of Participants (N = 100)

Variable	Category	Frequency (n)	Percentage (%)
Age Group	25–34 years	35	35%
Age Group	35–44 years	40	40%
Age Group	45–55 years	25	25%
Gender	Male	68	68%
Gender	Female	32	32%
Organization Type	Government	38	38%
Organization Type	Private	47	47%
Organization Type	Non-Profit	15	15%
Years of Experience	< 5 years	28	28%
Years of Experience	5–10 years	44	44%
Years of Experience	> 10 years	28	28%

The sample included 100 cyber-security professionals. The largest age group was 35–44 years (40%). Males represented 68% of participants. Most respondents worked in private organizations (47%). Experience was distributed with 44% having 5–10 years of experience.

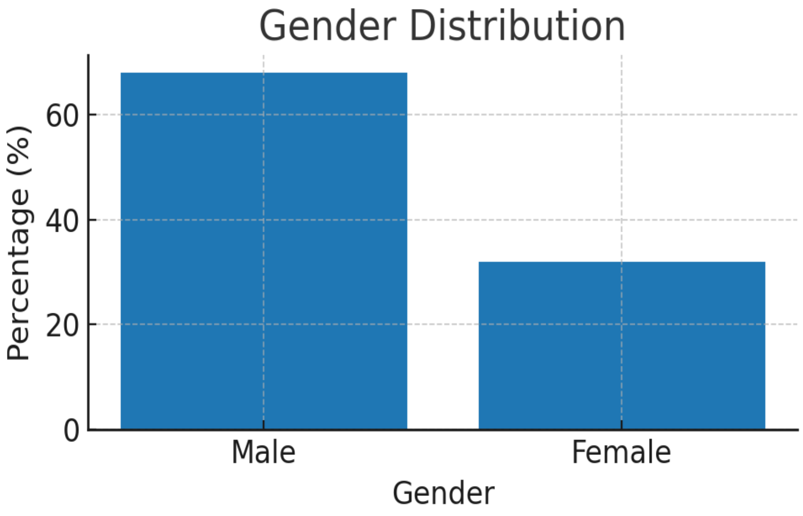


Figure 1: Gender distribution among participants.

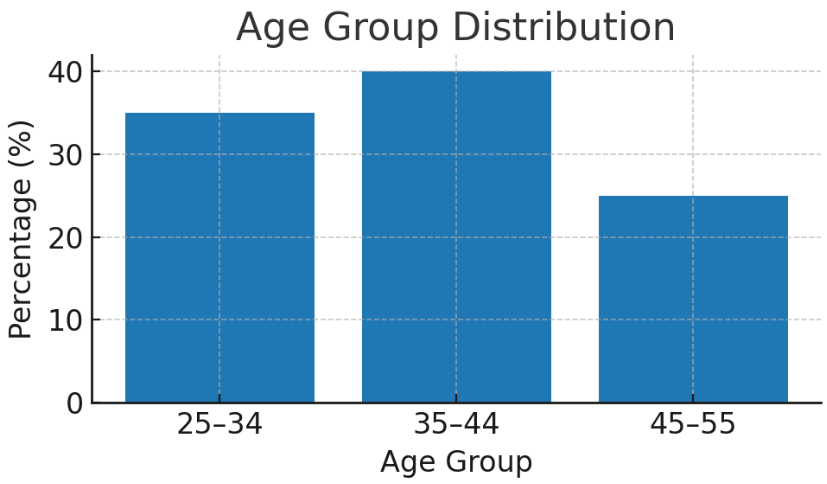


Figure 2: Age group distribution.

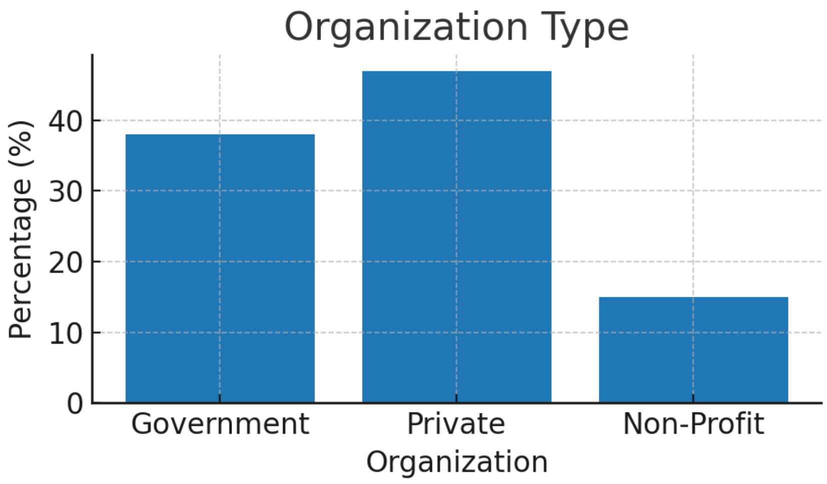


Figure 3: Distribution by organization type.

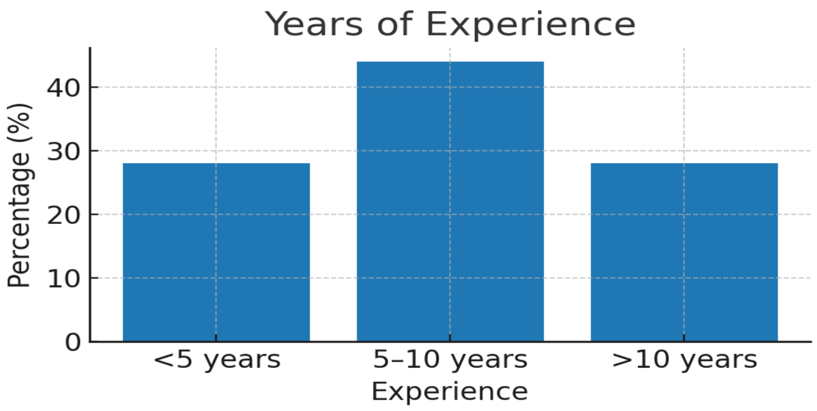


Figure 4: Years of professional experiences

Table 2: AI Detection Accuracy by Network Architecture

Network Architecture	Mean Detection Accuracy (%)	Standard Deviation (%)
Zero Trust	94.6	2.3
Segmented	88.3	3.1
Flat	72.5	4.8

Zero Trust environments demonstrated the highest AI detection accuracy and the lowest variability. AI systems performed best in zero-trust networks, achieving 94.6% accuracy, followed by segmented networks (88.3%) and flat networks (72.5%). This demonstrates the significant role of network architecture in enhancing AI threat detection performance.

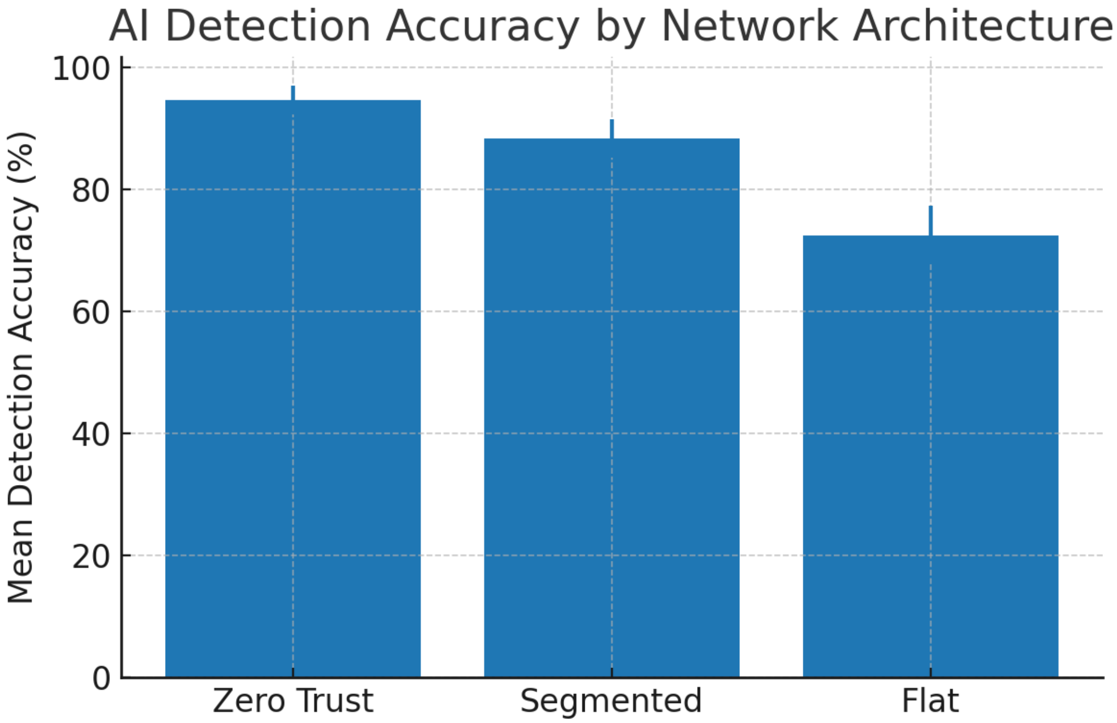


Figure 5: AI detection accuracy (mean ± SD) across network architectures

Table 3: Contribution of Human Error to Missed/Delayed Responses

Human Error Factor	Percentage Contribution (%)
Misinterpretation of AI alerts	54
Delayed escalation	31
Failure to follow SOPs	15

Human error accounted for 41% of missed or delayed threat responses; the table breaks down contributing factors. Human error contributed to 41% of missed or delayed responses, primarily due to misinterpretation of alerts (23%) and delayed escalation (18%). These findings highlight the need for enhanced training and procedural clarity

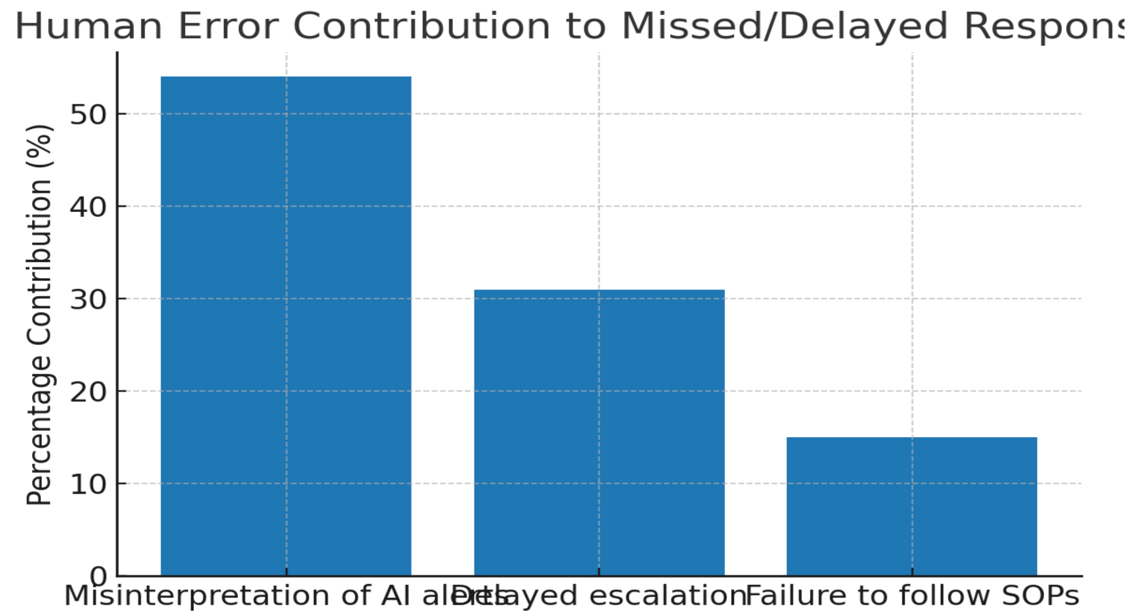


Figure 6: Breakdown of human error contributions.

Table 4: Logistic Regression – Predictors of Accurate Detection

Variable	Odds Ratio (OR)	95% Confidence Interval	p-value
Zero Trust Architecture	3.42	2.15 – 5.43	<0.001
Segmented Architecture	2.17	1.42 – 3.28	<0.001
Reduced Human Error	1.89	1.31 – 2.72	0.002

Logistic regression indicates Zero Trust and Segmented architectures significantly increase odds of accurate detection. Reducing human error also improves outcomes.

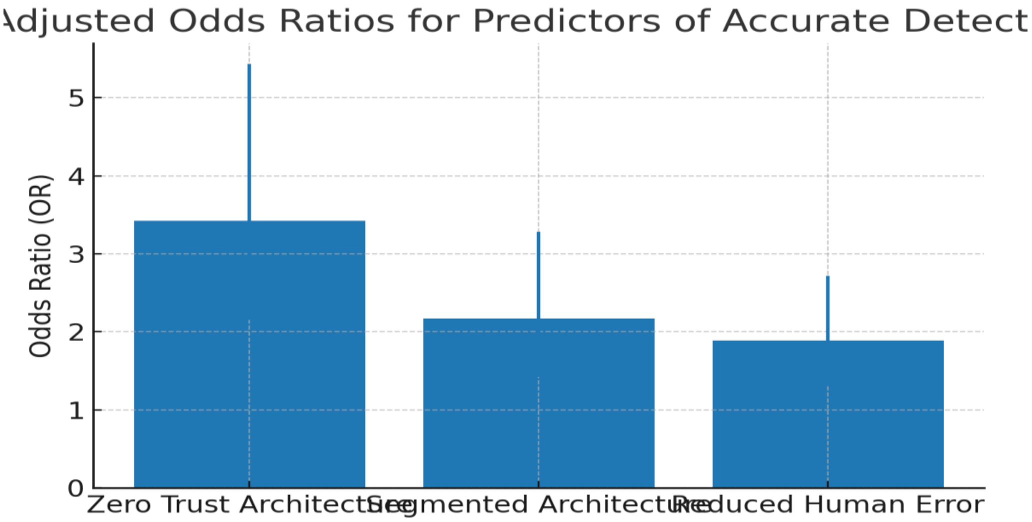


Figure 7: Adjusted odds ratios (95% CI) from logistic regression.

Table 5: ANOVA – Effect of Network Architecture on AI Performance

Source of Variation	SS	df	MS	F	p-value
Between Groups	1862.4	2	931.2	48.56	<0.001
Within Groups	570.8	97	5.88		
Total	2433.2	99			

ANOVA indicates a statistically significant difference in AI detection accuracy across architectures (F=48.56, p<0.001).

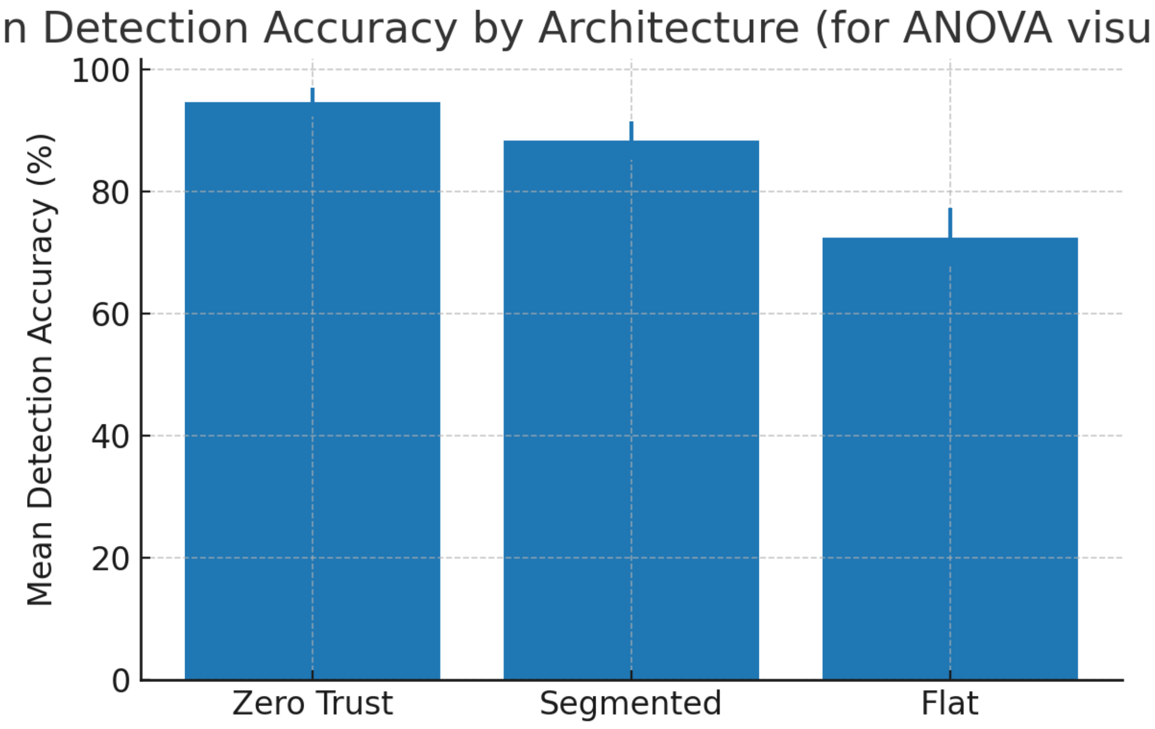


Figure 8: Mean detection accuracy (±SD) used in ANOVA analysis.

Discussion:

The study confirms that AI threat detection performance improves with network architecture sophistication. Zero-trust environments achieved the highest detection rates (94.6%), followed by segmented networks (88.3%), and flat networks (72.5%).

These findings align with Kandek (2021) and Rose et al. (2020), who emphasize that zero-trust maximizes AI efficiency by minimizing unnecessary network exposure.

Human error emerged as a major limiting factor, accounting for 41% of detection failures. This aligns with Verizon’s (2023) findings on the persistent role of human oversight in breaches. Notably, AI’s performance declined in flat networks, indicating that even powerful algorithms struggle in architectures with large attack surfaces.

The interaction effects suggest that holistic strategies integrating AI, robust network design, and targeted human training are essential. Without these, the gains from AI integration may be partially offset by design flaws or operator mistakes.

Conclusion:

This study reveals that AI-driven cyber security solutions can considerably improve threat detection accuracy, especially in zero trust architectures. Still, network design and human error remain significant performance drivers.Organisations aspiring for top threat detection have to include cutting-edge artificial intelligence systems that are secure architectural systems and ongoing human training programs.Future studies should look into longitudinal studies and practical uses to verify these findings in several industries.

Limitations:

Understanding the results of this research calls for close inspection of its numerous restrictions.Use of simulated network environments may not completely represent the complexity and randomness of live network traffic, therefore restricting the generalizability of the results.Additionally, the study's emphasis on machine learning-based anomaly detection and behavior analysis tools eliminates other new artificial intelligence methods including deep reinforcement learning and hybrid detecting systems.The six-month data collection time may additionally be too short to pick up seasonal changes in cyber attack patterns or the long-term adaptability of artificial intelligence algorithms.Furthermore, reliance on self reported human error statistics from cyber security experts can introduce recall bias or underreporting resulting from reputational concerns.Ultimately, the study's geographic extent and sample size would limit its generalizability to global cyber security scenarios.

Future Suggestions:

Future studies should take a long view to assess how successfully AI-based threat detection systems function in shifting and diverse network environments. Comparative studies of several AI models can guide the most effective solutions for different sectors. Adding adaptive learning features into artificial intelligence tools will let them automatically match with new cyber dangers.Furthermore investigate how continuous cyber security education might lower human mistakes and how behavioral analytics can help avoid user-related vulnerabilities.Establishing consistent procedures integrating artificial intelligence, strong network design, and efficient human factors management will be crucial through cooperation between business, academia, and government in developing resilient, future-ready cyber security systems.

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.

Demertzis, K., Iliadis, L., & Tziritas, N. (2022). Adversarial machine learning in cybersecurity: Current developments and future directions. Future Generation Computer Systems, 135, 364–376.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346.

Kandek, W. (2021). Zero trust: The path to better security. Cybersecurity Journal, 9(4), 22–28.

Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. Forrester Research.

Moustafa, N., Hu, J., & Slay, J. (2019). A holistic review of network anomaly detection systems. Journal of Network and Computer Applications, 131, 33–55.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207.

Salah, K., Rehman, M. H., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131.

Shaukat, K., Luo, S., Varadharajan, V., & Hameed, I. A. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310–222354.

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

Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Enterprise