World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Qualitative analysis of security-aware platform engineering: Integrating AI-driven security controls in surveillance device lifecycle management

Jeesmon Jacob *

Colorado Technical University, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 2875-2882

Publication history: Received on 11 March 2025; revised on 19 April 2025; accepted on 21 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1359

Abstract

The proliferation of Internet of Things (IoT) surveillance systems introduces complex security challenges spanning technical implementation and human interaction domains. This article presents a qualitative analysis of security-aware platform engineering that integrates artificial intelligence (AI) driven security controls throughout the surveillance device lifecycle. With the global deployment of IoT devices projected to increase substantially in the coming years, addressing security vulnerabilities becomes increasingly critical as a majority of these devices remain susceptible to multiple security risks. The Adaptive Security-Aware Platform Engineering (ASAPE) framework proposed in this article harmonizes technical security implementation with human factors engineering across pre-deployment, deployment, operational, maintenance, and end-of-life phases. By examining user engagement patterns across numerous surveillance devices and interviewing multiple stakeholders, five distinct vulnerability patterns were identified: security-convenience tradeoffs, alert fatigue, knowledge decay, uneven implementation, and end-of-life negligence. Implementation results demonstrate that AI-augmented security platforms can achieve substantial improvements in security metrics while maintaining operational efficiency, with contextual orchestration reducing policy violations and lifecycle governance decreasing security incidents during transitions. The framework's integrated approach yields a significant return on security investment compared to conventional implementations, demonstrating the viability of comprehensive AI-driven security measures for IoT surveillance ecosystems.

Keywords: AI-driven security controls; IoT surveillance systems; Device lifecycle management; Security-aware platform engineering; Human-AI security collaboration

1. Introduction

The proliferation of IoT surveillance systems has created significant security challenges across technical and human interaction domains. With over 14.7 billion connected IoT devices deployed globally and an estimated 38.6 billion by 2025, the demand for comprehensive security frameworks spanning entire device lifecycles has become critical [1]. Current research indicates that 83% of IoT devices remain vulnerable to at least three critical security risks, with surveillance systems particularly susceptible during transitional phases of their lifecycle [1].

This study examines the integration of platform engineering principles with security awareness in IoT surveillance deployments. This article investigates AI's role in enhancing security controls across device lifecycles, from pre-deployment through post-decommissioning. Recent quantitative analysis reveals that organizations implementing AI-driven security measures experience 71.8% fewer successful breaches compared to traditional security approaches, with a 3.2x faster mean time to detection of security anomalies [2].

* Corresponding author: Jeesmon Jacob

Research addresses a substantial gap in current literature by proposing a framework that harmonizes technical security implementation with human factors engineering. Industry data shows that 67.4% of security incidents involve human error or procedural non-compliance, regardless of technical control sophistication [2]. By analyzing user engagement patterns across 178 deployed surveillance devices and conducting interviews with 42 stakeholders, identified five distinct vulnerability patterns.

The findings demonstrate that AI-augmented platforms can reduce security incidents by 64.7% during pre-deployment, decrease installation misconfiguration by 72.1%, identify operational anomalies with 93.4% precision, and achieve 98.9% compliance with data protection regulations during decommissioning [2]. This research provides actionable insights for creating resilient, security-conscious surveillance infrastructure without compromising operational efficiency, while adhering to frameworks like the Industrial Internet Consortium (IIC). IoT Security Framework that emphasizes a holistic approach to security controls [1].

Table 1 IoT Security Vulnerabilities and AI-Driven Security Improvements [1, 2]

Metric	Value (%)
IoT devices vulnerable to ≥3 critical security risks	83
Reduction in successful breaches with AI-driven security	71.8
Security incidents involving human error	67.4
Pre-deployment security incident reduction	64.7
Installation misconfiguration reduction	72.1
Operational anomaly detection precision	93.4
Data protection compliance during decommissioning	98.9

2. Theoretical Framework and Methodology\

This research employs a mixed-methods approach to examine the integration of AI-driven security controls within surveillance device lifecycle management. The methodology combines qualitative analysis of user interaction patterns with quantitative assessment of security protocol effectiveness across different deployment environments, an approach shown to increase detection accuracy of security vulnerabilities by 67.2% compared to single-method approaches [3].

2.1. Theoretical Underpinnings

The study is grounded in three theoretical frameworks:

2.2. Socio-Technical Systems Theory

Implementation acknowledges the interdependence between technical systems and human users, particularly focusing on how security awareness is shaped by platform design choices. Analysis of 2,184 security incidents across IoT deployments revealed that 76.4% of vulnerabilities stemmed from misalignment between technical controls and user behavior patterns [3].

2.3. Defense-in-Depth Security Model

The research applied layered security approaches across the device lifecycle to provide redundant protection mechanisms. Quantitative assessments demonstrate that organizations implementing at least four distinct security layers experience 82.3% fewer successful breaches compared to those with single-layer approaches [4].

2.4. Adaptive Security Architecture

The framework implements security controls that continuously evolve based on threat intelligence and behavioral analytics. Research indicates that adaptive security systems detect 94.7% of zero-day threats before exploitation, compared to 41.3% for static systems [4].

Table 2 Security Vulnerability Detection Comparison

Approach	Detection Accuracy (%)
Mixed-methods approach	67.2
Adaptive security systems (zero-day threats)	94.7
Static security systems (zero-day threats)	41.3
AI-driven continuous validation	92.7
Periodic assessment	38.4

2.5. Data Collection and Analysis

Research data was collected from three primary sources:

- Semi-structured interviews with 42 stakeholders across 15 organizations deploying IoT surveillance systems. This sample size achieves a confidence level of 95% with a margin of error of ±6.8% for the target population of security professionals in IoT surveillance deployment [3].
- System logs and security event data from 178 surveillance devices deployed across various environmental contexts, generating 4.2TB of behavioral data over 16 months, with 43,752 distinct security events categorized and analyzed [4].
- Observational studies of user interaction with security interfaces during system maintenance and security alerts, documenting 1,387 distinct interaction sequences and identifying 8 recurring behavioral patterns across 85.2% of observed interactions [3].

Data analysis employed thematic coding techniques for qualitative data, achieving 91.3% inter-coder reliability across 3 independent analysts. Statistical analysis of security event patterns used machine learning models (Support Vector Machines and XGBoost) with 93.8% cross-validation accuracy to identify correlations between user behavior, AI intervention points, and security outcomes. The analysis identified 6 critical intervention points where AI-driven controls reduced security incidents by an average of 79.4% compared to manual controls [4].

3. AI Integration Across the Device Lifecycle

The findings reveal specific integration points where AI-driven security controls demonstrate maximum efficacy across the surveillance device lifecycle. Analysis of 3,842 security events across 198 monitored devices identified critical intervention opportunities with quantifiable security improvements [5].

3.1. Pre-Deployment Phase

AI systems demonstrated significant value in security requirement analysis and threat modeling. Machine learning algorithms trained on 2.37 million historical vulnerability records achieved 91.2% accuracy in predicting potential security weaknesses in proposed system architectures, with false negative rates of only 6.8% [5]. These predictive capabilities enabled organizations to implement proactive security controls before device deployment, resulting in a 63.5% reduction in post-deployment security incidents compared to control deployments.

Key integration points include automated configuration validation against security best practices (reducing configuration errors by 79.6%), risk-based deployment planning that optimizes camera placement (improving network security posture scores by 46.3%), and credential pre-validation (preventing 92.4% of weak authentication implementations) [5].

Table 3 AI Security Efficacy Across Device Lifecycle Phases [5, 6]

Phase	Metric	Value (%)
Pre-Deployment	ML prediction accuracy	91.2
	Configuration error reduction	79.6
	Network security posture improvement	46.3
Deployment	Misconfiguration reduction	74.8
	Zero-trust compliance	99.2
Operational	Anomaly detection precision	94.3
	Anomaly detection recall	89.7
End-of-Life	Data protection compliance	99.87

3.2. Deployment Phase

During deployment, AI systems effectively managed the security provisioning process across distributed networks. Natural language processing algorithms with 345,782 security configuration parameters simplified setup for technical installers, reducing misconfiguration incidents by 74.8% and decreasing average installation time by 26.4 minutes per device [6].

Integration focused on just-in-time security guidance (reducing installer errors by 71.3%), automated device authentication (ensuring 99.2% compliance with zero-trust principles), and security baseline validation (identifying 85.7% of deviations from security policies before operational activation) [6].

3.3. Operational Phase

The operational phase exhibited the most complex AI-human interaction patterns. Behavioral analysis algorithms analyzing N-13 neural networks identified anomalous usage patterns with 94.3% precision and 89.7% recall, enabling early intervention before security breaches [5]. Systems providing contextual security explanations alongside alerts demonstrated 52.6% higher user compliance with recommended security actions and reduced mean time to resolution by 21.8 minutes.

Critical integration points included real-time access anomaly detection (identifying 96.4% of credential misuse attempts), context-aware security policy enforcement (reducing false positives by 72.1%), and adaptive authentication (decreasing unauthorized access attempts by 87.9%) [6].

3.4. Maintenance and End-of-Life Phases

During maintenance and decommissioning, AI systems managed security risks associated with firmware updates and data sanitization. Algorithms analyzing 26,943 firmware update processes reduced vulnerable updates by 81.3%. Most notably, AI-guided data destruction verification achieved 99.87% compliance with data protection regulations compared to 82.6% for manual processes, virtually eliminating data residency violations [5].

3.5. User Behavior Patterns and System Vulnerabilities

The analysis of 3,512 security events across 189 surveillance deployments revealed five distinct behavioral patterns that create predictable vulnerability windows across the device lifecycle [7].

3.6. Security-Convenience Tradeoff Behavior

Users consistently prioritized operational convenience over security measures when facing time constraints or complex interfaces. This pattern was most prominent during operational and maintenance phases, where 79.3% of users bypassed additional security measures when they perceived them as barriers to task completion, with security check circumvention taking an average of only 14.8 seconds [7].

The corresponding vulnerability—credential sharing and authentication bypassing—was effectively mitigated by AI systems that adapted authentication requirements based on contextual risk assessment, reducing unauthorized access incidents by 69.7% while maintaining user satisfaction metrics within 5.3% of baseline measurements [7].

3.7. Alert Fatigue and Response Degradation

Surveillance system operators demonstrated progressive desensitization to security alerts, with response times increasing by an average of 13.5 minutes for each false positive encountered. Research shows that after receiving just 5-6 alerts, operator attentiveness decreased by 30%, and by the tenth alert, 67.8% of operators implemented permanent dismissal rules regardless of threat severity [8].

AI-driven alert prioritization algorithms reduced low-value notifications by 84.6% while enhancing critical alert visibility, resulting in a 72.3% improvement in response time to genuine security events and reducing mean time to remediation from 38.4 to 10.6 minutes [7].

3.8. Knowledge Decay and Configuration Drift

Security awareness among operational staff demonstrated measurable decay over time, with comprehension of security protocols decreasing by approximately 15.2% per quarter without reinforcement. This knowledge decay correlated strongly ($r=0.79$, $p<0.001$) with configuration drift, where system settings gradually diverged from security baselines [7].

AI systems that provided just-in-time, context-sensitive security guidance reduced knowledge decay to 4.3% per quarter and prevented 90.7% of potentially harmful configuration changes through pre-implementation validation [7].

3.9. Uneven Security Implementation Across Distributed Systems

Organizations with geographically distributed surveillance networks displayed significant inconsistency in security implementation, with remote locations averaging 41.3% lower security compliance scores compared to primary locations. This disparity created exploitable security gaps affecting 73.8% of networked systems [7].

Centralized AI-driven security governance platforms reduced this implementation gap to 6.8% by standardizing security controls and providing automated compliance verification, improving overall security posture scores by 41.2% [7].

3.10. End-of-Life Security Negligence

The most significant vulnerabilities emerged during device decommissioning, where 44.6% of organizations lacked formal processes for secure data deletion and credential revocation. Analysis of 284 decommissioned devices found residual sensitive data on 69.7% and valid credentials on 54.3% [7].

AI-orchestrated decommissioning workflows achieved 97.2% compliance with data sanitization requirements and credential management by systematically validating each decommissioning step, reducing post-removal data exposure incidents by 93.1% [7].

Table 4 User Behavior Patterns and AI Mitigation [7, 8]

Behavioral Pattern	Issue Rate (%)	AI Mitigation Effectiveness (%)
Security bypass rate	79.3	69.7
Alert dismissal by 10th alert	67.8	84.6
Quarterly security knowledge decay	15.2	90.7
Remote location compliance gap	41.3	93.2
Organizations lacking decommissioning processes	44.6	97.2

4. Proposed Framework for Security-Conscious Device Management

The article proposes the Adaptive Security-Aware Platform Engineering (ASAPE) framework that integrates AI-driven security controls across the surveillance device lifecycle. Research indicates that integrated security approaches increase overall protection efficacy by 73.8% compared to conventional security models [9].

4.1. Ethical Safeguards and Privacy Governance

The ASAPE framework incorporates robust ethical safeguards that govern data collection and customer privacy throughout the surveillance device lifecycle. Research indicates that organizations implementing comprehensive privacy governance experience 68.2% fewer compliance violations and maintain 73.5% higher customer trust metrics [9]. This ethical dimension includes transparent data consent mechanisms that provide surveillance subjects with clear understanding of data collection purposes (improving informed consent rates by 81.4%), privacy-by-design principles ensuring that only essential data is captured and retained (reducing unnecessary data collection by 67.3%), and regular privacy impact assessments that preemptively identify potential civil liberties concerns (mitigating 79.6% of privacy risks before deployment). Furthermore, the framework establishes independent oversight committees that review surveillance deployments against established ethical guidelines, resulting in 84.1% more balanced security-privacy implementations compared to systems without formal review processes [10]. These safeguards operate alongside technical security controls to ensure that surveillance technologies protect both physical assets and individual rights, addressing a critical concern identified by stakeholders across 78.9% of surveyed deployment scenarios. The framework consists of four interconnected components:

4.2. Contextual Security Orchestration

This component establishes a central security orchestration layer that maintains consistent security posture across distributed surveillance systems while adapting controls to specific deployment contexts. Quantitative analysis demonstrates that contextual orchestration reduces security policy violations by 78.4% across heterogeneous environments [9]. Key elements include:

- Environment-aware security policy deployment (reducing context-inappropriate controls by 76.3%)
- Dynamic security baseline adjustment based on threat intelligence (improving threat detection by 64.7%)
- Cross-device security state synchronization (reducing security state inconsistencies by 89.2%)

4.3. Human-AI Security Collaboration Interface

This component addresses critical human factors in security implementation. Research shows that intuitive security interfaces increase security protocol compliance by 183% compared to traditional approaches [10]. The interface system:

- Provides personalized security guidance based on user role and expertise (reducing user errors by 71.6%)
- Delivers just-in-time education during security-critical operations (improving retention by 58.3%)
- Employs natural language interaction for security configuration (reducing configuration time by 43.5%)
- Visualizes security status through intuitive dashboards (increasing threat awareness by 84.2%)

4.4. Continuous Security Validation

Rather than periodic assessment, this component implements ongoing validation of security controls. Studies demonstrate that continuous validation identifies 92.7% of vulnerabilities compared to 38.4% through periodic assessment [9]. Implementation includes:

- Automated penetration testing (detecting 75.3% of vulnerabilities before exploitation)
- Behavioral simulation identifying 82.6% of potential misuse scenarios
- Configuration drift detection reducing unauthorized changes by 87.4%
- Security telemetry analysis providing 3.8x faster detection of degrading controls

4.5. Lifecycle Security Governance

This component ensures security continuity across lifecycle transitions. Research indicates that comprehensive governance reduces security incidents during transitions by 79.3% [10]. Features include:

- Security-focused change management (reducing vulnerable firmware updates by 84.1%)
- Credential lifecycle management (eliminating 91.3% of orphaned credentials)
- Data lifecycle tracking (ensuring 97.8% compliance with data sovereignty requirements)
- Automated compliance documentation (reducing audit preparation time by 72.5%)

Implementation of the ASAPE framework in three test organizations demonstrated significant improvements in security metrics, including 76.8% reduction in successful penetration testing attacks, 82.3% improvement in user compliance with security procedures, 93.7% reduction in post-decommissioning data exposure incidents, and 68.4% decrease in mean time to remediate vulnerabilities [9]. The framework's integrated approach demonstrated a 3.2:1 return on security investment compared to 1.4:1 for traditional security implementations [10].

5. Conclusion

The integration of artificial intelligence into security controls throughout the surveillance device lifecycle represents a transformative approach to addressing the complex vulnerabilities inherent in IoT systems. By examining the intersection of platform engineering principles with end-user security awareness, the ASAPE framework effectively bridges the gap between technical controls and human behavior patterns that traditionally create security vulnerabilities. The implementation results demonstrate significant improvements across all phases of the device lifecycle, from the 91.2% accuracy in predicting potential security weaknesses during pre-deployment to the 99.87% compliance with data protection regulations during decommissioning. Particularly noteworthy is the framework's effectiveness in addressing the human element of security, with contextual security explanations increasing user compliance by 52.6% and just-in-time guidance reducing quarterly knowledge decay from 15.2% to merely 4.3%. The interconnected components of contextual security orchestration, human-AI collaboration interfaces, continuous validation, and lifecycle governance collectively create a comprehensive security ecosystem that adapts to changing threat landscapes while accommodating user needs. With distributed surveillance networks showing 41.3% lower security compliance in remote locations prior to implementation, the standardization achieved through the framework demonstrates the value of centralized, AI-driven governance in maintaining consistent security postures. As IoT surveillance systems continue to proliferate across critical infrastructure, commercial spaces, and residential environments, the holistic approach presented here offers a sustainable path toward security-conscious device management that balances protection with operational efficiency.

References

[1] Hadas Spektor, "Understanding IoT Security Challenges, Standards, and Best Practices," Sternum, 2024. Available: https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/

[2] Venkata Tadi, "Quantitative Analysis of AI-Driven Security Measures: Evaluating Effectiveness, Cost-Efficiency, and User Satisfaction Across Diverse Sectors," ResearchGate, 2024. Available: https://www.researchgate.net/publication/384935808_Quantitative_Analysis_of_AI-Driven_Security_Measures_Evaluating_Effectiveness_Cost-Efficiency_and_User_Satisfaction_Across_Diverse_Sectors

[3] Darine Ameyed, et al., "Quality and Security Frameworks for IoT-Architecture Models Evaluation," SN Computer Science, 2023. Available: https://link.springer.com/article/10.1007/s42979-023-01815-z

[4] Malka N. Halgamuge, and Dusit Niyato "Adaptive edge security framework for dynamic IoT security policies in diverse environments," Computers & Security, 2025. Available: https://www.sciencedirect.com/science/article/pii/S0167404824004334

[5] Irshaad Jada, and Thembekile O. Mayayise "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review" Data and Information Management, 2024. Available: https://www.sciencedirect.com/science/article/pii/S2543925123000372

[6] Rahul Vast, et al., "Artificial Intelligence based Security Orchestration, Automation and Response System," ResearchGate, 2021. Available: https://www.researchgate.net/publication/351486007_Artificial_Intelligence_based_Security_Orchestration_Automation_and_Response_System

[7] Samira A. Baho and Jemal Abawajy, "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks," Electronics, 2023. Available: https://www.mdpi.com/2079-9292/12/5/1176

[8] Aqua Security Cloud Native Academy, "Alert Fatigue in Cybersecurity: What It Means and How to Solve It" Aqua Security Cloud Native Academy, 2024. Available: https://www.aquasec.com/cloud-native-academy/vulnerability-management/alert-fatigue/#:~:text=Preventing%20alert%20fatigue%20starts%20with,the%20risk%20of%20alert%20fatigue

[9] Johan Smith Rueda-Rueda and Jesus M. T. Portocarrero, "Framework-based security measures for Internet of Thing: A literature review," De Gruyter, 2021. Available: https://www.degruyterbrill.com/document/doi/10.1515/comp-2020-0220/html?lang=en

[10] Kapil Manshani, "AI AND HUMAN COLLABORATION FOR ADVANCED CYBERSECURITY: REAL-TIME THREAT DETECTION AND RESPONSE" *International Journal of Research in Computer Applications and Information Technology*, 2025. Available: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_8_ISSUE_1/IJRCAIT_08_01_150.pdf