ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Volume 12 Issue 12 December 2025

AI-Driven Security Policy Framework for IoT Systems

Tanu Srivastava

Senior Advisory Consultant, IBM Consulting Cybersecurity Services
IBM India Private Limited, India
Email: srivastavtanu@gmail.com

Abstract*— The growing number of Internet of Things (IoT) devices has enabled an extensive and varied network of interconnected devices, generating more vulnerability on cybersecurity and privacy. Traditional, rigid security policies no longer suffice for environments that shift and change quickly and unpredictably. The current work presents an artificial intelligence-driven security policy framework, using machine-learning-based approaches to detect abnormalities, predict threats, and deploy adaptive security controls autonomously. The framework promotes continual monitoring, intelligent threat processing and decreased manual intervention aligned with regulations. The proposed model, by combining AI with policy governance, promotes trust, stability, and scalability for IoT domains, such as smart cities as well as healthcare and industrial settings.

Index Terms*— Artificial Intelligence, Anomaly detection, Deep Learning, Internet of Things, Machine Learning, Network Intrusion Detection System.

I. INTRODUCTION

AI [Artificial Intelligence] is an emerging paradigm in computer science which allows people to perform almost all decision-making, data analysis, and user interaction activities without being reliant on humans. IoT [Internet of Things] includes an ever-growing network of mundane devices around the internet for self-sustaining information sharing and coordinated action. As the IoT deployments increase in quantity and complexity they create voluminous data and work in distributed, resource-constrained contexts. These characteristics present numerous threats to IoT ecosystems cybersecurity-wise. Security policies — formalized rules for the protection of information by either users, devices, or systems — are an important part of maintaining these environments. But traditional security policy is primarily static and manual (for example not much real-time training) and not suitable for quick responses to new patterns of attacks or new patterns of behavior changed in IoT. AI-enabled policy frameworks present a way forward owing to dynamic learning, automated decision-making and agile adaptation. With real-time analytics and automated enforcement, AI strengthens policy execution and provides a stronger and more agile basis for IoT security.

II. RELATED WORK

Past studies related to IoT security have focused on device-level cybersecurity, NIDS detections, and malicious behaviors against IoT. While structured guidance, recommended procedures, and baselines for risk assessment have been created, these frameworks are overwhelmingly manual and often are based on static preset policies for static mechanisms rather than dynamic configurations, even though their widely accepted methodologies were used by other researchers in NIST, ENISA and others. The field of anomaly detection is being studied, in which ML [Machine Learning] based anomaly detection is an emerging field, effectively detecting abnormal traffic, infected sensors, and botnet actions. DL [Deep learning] techniques have also substantially improved accuracy and speed of responses. But these contributions are all on threat detection, not on policy automation. Context-aware policy engines, ontology-based rule models, and semantic reasoning approaches have been examined in policy management literature. Although these are simple policies that improve clarity and prevent policy interpretation conflicts across the board, many of them still need the security administrators themselves to maintain and update the rules. More recent advances propose AI-based security decision systems in which machine learning outputs could be utilized to modify risk scoring or recommendations for policy changes. However, such methods seldom cover the entire life cycle of policy creation, validation, deployment and maintenance. A body of work, focusing on what still remains unexplored, demonstrates limitations of the current state of the art and the necessity for intelligent and fully autonomous AI-powered security policy framework that will evolve with the real time and respond to evolving landscape of the IoT.

III. METHODOLOGY

1. Data Input Layer

Information is continuously collected from IoT devices, communication streams, and system logs, and this presents the most recent version of device behavior and interaction.

2. Feature Preparation

We clean, normalize, and transform raw data to extract important behavioral and protocol-level features that can be used for analytical modeling.

3. Intelligent Analysis Module

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)

Volume 12 Issue 12 December 2025

The refined data is analyzed using a series of supervised, unsupervised and reinforcement learning models which find anomalies, categorize threats and quantify the likelihood of an outcome due to an observed activity.

4. Automated Policy Logic

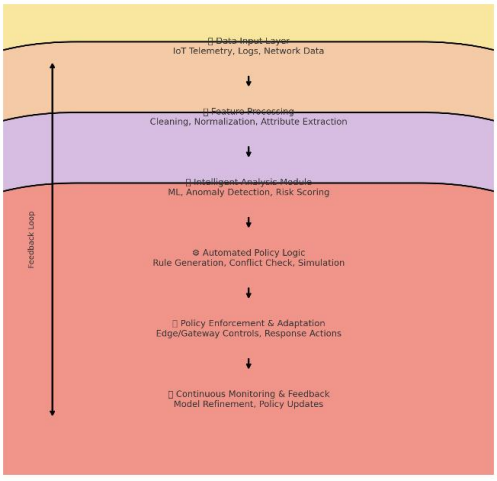
Insights from the AI models are applied for the generation or revision of security rules. Each rule is analyzed for consistency before launch and validated in simulation to avoid conflicts or to avoid unintended consequences.

5. Enforcement and Continuous Adaptation

Validated policies are enforced at least at a very edge or gateway level to control device interaction. Continuous observation pushes new behavioral data back into the learning pipeline, so that both the AI models and security policies can be honed by iteration. This approach allows for an efficient and adaptable security model which can flexibly handle dynamic conditions of IoT systems without the need to heavily depend on manually configured rules.

IV. CONCEPTUAL FRAMEWORK

The conceptual model encompasses five interrelated elements that are intended to support intelligent, adaptive policy management. Data collected by devices, logs, and network interactions goes into a second level called an input layer, which can be processed into structured features appropriate for machine-learning inference. AI algorithms scrutinize the processed data to determine potential threats and anomalies. From analyzing these factors, the automated policy logic produces rules that cater to context, then analyzes them for conflicts and passes them to enforcement points, like the edge gateways. Continuing to check updates policy to be consistent with emerging behavior enables an iterative, learning-on-the-fly approach (both in the sense of a learning environment and policy adjustment—as the best of both worlds): iterative learning.



V. CONCLUSION

As IoT systems grow and sophistication, fixed system security policies can no longer maintain the same security posture over time in case of attacker-changing threat vector and new threats. The purpose of this work is to propose an AI-based security policy framework for a security policy model that includes various aspects of data acquisition, feature mining, feature processing, smart analysis, auto-analysis and rule generation, and real-time implementation, and the enforcement of such policy. The security policy is made up of five functions: data and compliance, feature processing, analysis and analysis, automated rule writing, and enforcement. The framework addresses the challenge of manual involvement, enables continuous learning, and offers improved resilience and scalability of IoT ecosystems. In short, AI embedded through the policy lifecycle can further strengthen the infrastructure of future IoT security models that are autonomous, adaptive and data driven.

REFERENCES

[1] NIST, NISTIR 8259: Recommendations for IoT Device Manufacturers, National Institute of Standards and Technology, 2020.

[2] ENISA, Baseline Security Recommendations for IoT, European Union Agency for Cybersecurity, 2017.

[3] Y. Meidan et al., “Detection of Unauthorized IoT Devices Using Machine Learning Techniques,” IEEE Internet of Things Journal, 2019.

[4] M. A. Khan and K. Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” Future Generation Computer Systems, 2018.