Poster: FORESIGHT, A Unified Framework for Threat Modeling and Risk Assessment in Robotics and IoT

ChaeYoung Kim
Seoul Women's University
Department of Information Security
kkimklara@swu.ac.kr

Kyounggon Kim
Naif Arab University for Security Sciences
kkim@nauss.edu.sa

***Abstract*—The integration of robotics and IoT technologies into everyday systems has revolutionized smart environments while introducing critical security and privacy challenges. This paper presents FORESIGHT, a unified framework for threat modeling and risk assessment, that addresses vulnerabilities in autonomous robotics and IoT ecosystems. By categorizing threats into robot-oriented, user-oriented, and environmental domains, FORESIGHT enables comprehensive risk analysis and prioritization of high-risk threats. Using Bayesian networks, the framework evaluates cascading vulnerabilities and interdependencies across system layers. Aligned with international standards such as ISO 13482, IEC 62443, and GDPR, FORESIGHT ensures a structured approach to enhancing the resilience of interconnected human-centered systems.**

***Index Terms*—Threat modeling, Robotics, IoT, Bayesian Networks, ISO Standards, GDPR, Risk Assessment**

1. Introduction

Rapid integration of robotics and IoT technologies has transformed smart environments, introducing opportunities and challenges. Although these advances improve automation and management, they are also identified as the most critical technological component of smart cities [1].

To address these challenges, we propose **FORESIGHT**, a unified framework for threat modeling that systematically addresses vulnerabilities across robot-oriented, user-oriented, and environmental domains. FORESIGHT incorporates international standards (e.g. ISO 13482, GDPR) and employs probabilistic methods like Bayesian networks to quantify and mitigate risks.

2. Related Work and Standards

Cybersecurity in robotics and IoT in smart environments has received increasing attention. Krzykowska-Piotrowska et al. [2] identified communication threats within the R2I model, emphasizing sensory system vulnerabilities. Similarly, Yaacoub et al. [3] recommended various measures to protect robotic ecosystems.

Incorporating international standards such as ISO 13482 and GDPR is crucial. These guidelines ensure compliance and provide a foundation for frameworks like FORESIGHT to address interconnected threats systematically.

3. Proposed Framework : FORESIGHT

3.1. Framework Overview

FORESIGHT, short for **Framework for Operational Risk Evaluation and Security Integration in Generalized Human-centered Technology**, is designed to address the complex cybersecurity and privacy challenges in robotic and IoT ecosystems. The framework offers the following.

- **Comprehensive Threat Identification**: Identifies and categorizes threats systematically across all layers of robotic systems.
- **Contextual Threat Prioritization**: Assigns risk levels to threats based on their likelihood and potential impact.
- **Integrated Security and Privacy Models**: Ensures the coexistence of robust security and privacy mechanisms, aligning with international standards such as ISO 13482 and IEC 62443.

3.2. Layer-Based Analysis

FORESIGHT defines five operational layers within robotic systems:

- **Perception Layer**: Handles data collection through sensors and cameras.
- **Computation Layer**: Processes data using AI models and computational resources.
- **Actuation Layer**: Executes physical actions via motors and servos.
- **Communication Layer**: Facilitates data exchange through network protocols.
- **Control Layer**: Manages decision-making and coordination.

Table 1 consolidates the threats and security measures across these layers, offering a structured view of their interdependencies.

Workshop on Security and Privacy in Standardized IoT (SDIoTSec) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-6-6
https://dx.doi.org/10.14722/sdiotsec.2025.23043
www.ndss-symposium.org

TABLE 1. LAYER-BASED THREATS AND SECURITY REQUIREMENTS IN FORESIGHT FRAMEWORK

Layer	Robot-Oriented Threats	User-Oriented Threats	Environmental Threats
Perception	Sensor spoofing, data manipulation	Unauthorized video/audio collection	Jamming attacks, environmental disruption
Computation	Malware, adversarial ML attacks	Privacy invasion via data analytics	System-wide malware propagation
Actuation	Command injection, hardware sabotage	Unauthorized actuation manipulation	Physical interference, sabotage
Communication	Replay attacks, protocol vulnerabilities	Data interception via communication channels	Network jamming, DoS attacks
Control	Malicious firmware updates, privilege escalation	Unauthorized control access	Exploitation of insecure systems

3.3. Bayesian Network for Threat Analysis

FORESIGHT incorporates Bayesian Networks to quantify cascading vulnerabilities while explicitly accounting for interdependencies among system layers. Threats are represented as nodes, with their interactions—including direct propagation and feedback loops—modeled as edges. This allows the framework to evaluate both immediate and cascading impacts of vulnerabilities.

For instance, a sensor spoofing attack in the Perception Layer may propagate to the Computation Layer, causing erroneous decision-making. Feedback effects, such as incorrect sensor recalibrations or actuator malfunctions, can further amplify risks across interconnected systems.

The total risk, incorporating interdependencies, is calculated as:

$$P(R_{\text{total}}) = \sum_{i=1}^{n} \sum_{j=1}^{m} P(T_i) \cdot P(I_j|T_i) \cdot P(R_k|I_j, D_{ij}), \quad (1)$$

where:

- $P(T_i)$: Probability of threat T_i.
- $P(I_j|T_i)$: Probability of impact I_j given threat T_i.
- $P(R_k|I_j, D_{ij})$: Risk propagation probability given impact I_j and dependency D_{ij} between layers.
- D_{ij}: Dependency factor capturing the influence of I_j on other components or layers.

The dependency factor D_{ij} reflects the strength of the interdependence between system components or layers. For instance, a high D_{ij} value would indicate significant risk amplification due to strong interdependencies. This probabilistic approach allows FORESIGHT to prioritize high-risk threats and account for cascading and feedback effects in dynamic smart environments.

3.4. Incorporating Interdependencies into Risk Assessment

Incorporating interdependencies into risk assessment ensures a more comprehensive evaluation of cascading effects. The refined equation for risk quantification is:

$$R = P(T) \times P(I|T) \times P(R|I, D), \quad (2)$$

where:

- $P(T)$: Probability of threat occurrence.
- $P(I|T)$: Probability of intermediate impact given the threat.
- $P(R|I, D)$: Probability of risk propagation given the impact and dependency D.
- D: Aggregated dependency factor representing interconnections between layers.

By modeling D as a matrix or weighted graph, FORESIGHT evaluates the network-wide risk impact and identifies critical nodes where mitigation measures should be prioritized.

4. Conclusion and Future Work

FORESIGHT provides a unified framework for assessing and mitigating vulnerabilities in robotics and IoT ecosystems. By aligning with international standards such as ISO 13482, IEC 62443, and GDPR, it ensures a holistic approach to security and privacy while enabling systematic risk prioritization and contextual threat analysis. Bayesian Networks further enhance its adaptability by modeling cascading vulnerabilities across system layers.

Future work will focus on:

- **DevOps Integration**: Automating threat modeling for seamless integration into DevOps workflows.
- **Emerging Threats**: Addressing AI-driven attacks and cloud-based vulnerabilities.
- **Predictive Modeling**: Incorporating dynamic threat data into Bayesian Networks for improved accuracy.

These enhancements will position FORESIGHT as a robust framework for safeguarding interconnected technologies against evolving cybersecurity challenges.

References

[1] K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, "Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey," *Sensors*, vol. 23, no. 7, p. 3681, 2023.

[2] K. Krzykowska-Piotrowska, E. Dudek, M. Siergiejczyk, A. Rosiński, and W. Wawrzyński, "Is secure communication in the r2i (robot-to-infrastructure) model possible? identification of threats," *Energies*, vol. 14, no. 15, p. 4702, 2021.

[3] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 21, pp. 115–158, 2022.