Poster: Securing IoT Edge Devices: Applying NIST IR 8259A to a Realtime Animal Detection System

Rahul Choutapally, Konika Reddy Saddikuti, and Solomon Berhe
Department of Computer Science, University of the Pacific, USA
Email: r_choutapally@u.pacific.edu, k_saddikuti@u.pacific.edu, sberhe@pacific.edu

***Abstract*—Urban safety concerns about small animals under vehicles inspired the AniLarm IoT prototype, which uses a Seek Thermal Compact Camera and Raspberry Pi for real-time detection via thermal imaging. The system delivers results through auditory alerts and operates offline. This research evaluates the applicability of NIST IR 8259A standards, focusing on secure authentication, data protection, system integrity, and maintainability in edge IoT applications.**

I. Introduction

Urban environments pose risks to stray animals, such as cats and dogs, that seek shelter under vehicles during adverse weather. These spaces provide warmth and security but can lead to injuries or death when vehicles start, also causing potential vehicle damage [1], [2]. This highlights the need for IoT-based detection systems to improve safety for animals and vehicles (see Fig. 1).

To address this issue, we developed AniLarm, an offline IoT prototype using thermal imaging and machine learning to detect animals under cars. It integrates a Seek Thermal Compact Camera and Raspberry Pi 4 Model B, delivering audible detection results through a Bluetooth speaker for safety and accessibility [3]. While the system captures and deletes images at runtime, privacy concerns may arise [4].

IoT devices face significant security challenges due to their complexity and rapid deployment [5]. Frameworks like NISTIR 8259A offer security baselines to protect device data and ecosystems [6]. This paper evaluates AniLarm's compliance with NISTIR 8259A to address its security and privacy challenges.

II. Related Work

NIST cybersecurity frameworks address IoT security challenges across domains. For example, applying NIST standards to smart inverters highlighted vulnerabilities in communication links and updates, leading to improved security via secure configurations and access controls [7]. Similarly, NISTIR 8228 ensured compliance with regulations like HIPAA for Medical IoT devices while managing risks [8].

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.2025.23054
www.ndss-symposium.org

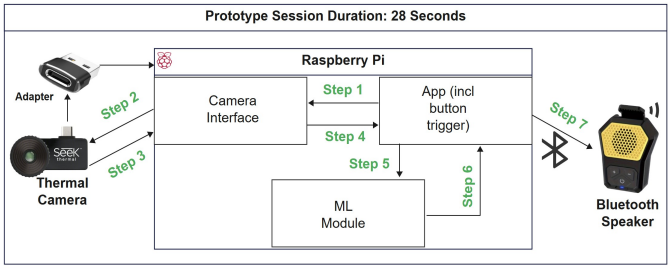

Fig. 1. Security Architecture Diagram

NISTIR 8259 emphasizes secure configurations and software updates during IoT design to reduce user burdens and align devices with organizational goals [9]. By tailoring IoT Core and Non-Technical Baseline profiles, NISTIR 8259C demonstrated how sector-specific needs could be addressed through minimal securability principles [10].

This study applies NISTIR 8259A to AniLarm, an IoT prototype for real-time animal detection in resource-constrained environments. AniLarm uses secure configurations, AES-256 encryption, and Bluetooth auditory feedback to meet NIST requirements, addressing authentication, data protection, access control, updates, and incident detection. This work demonstrates practical security for safety-critical applications and fills gaps in existing research.

III. Methodology

This section reviews the six key NIST IR 8259A requirements and their impact on AniLarm's system components [5], [11]. The methodology maps each requirement to corresponding hardware, software, and connectivity components for identifying gaps while accomplishing compliance with IoT security standards. The prototype applies the NIST IR 8259A standard to protect two key IoT data components: captured images and user notifications.

A. NIST IR 8259A Requirements

The key security requirements for device compliance are:

Requirements: Req 1: Device Identification – Devices must have unique identifiers for management and security. **Req 2: Secure Configuration** – Devices must provide secure default settings and allow configurable security improvement. **Req 3: Data Protection** – Sensitive data must be protected using encryption to ensure confidentiality and integrity. **Req 4: Access Control** – Access must be restricted to authorized

TABLE I
RESULT: NIST IR 8259A REQUIREMENTS AND PROTOTYPE COMPONENT IMPLEMENTATION MAPPING

ID	Name	Type	Req 1: Device ID	Req 2: Secure Config	Req 3: Data Protection	Req 4: Access Control	Req 5: SW Updates	Req 6: CIDR
Comp 1	Image Captured	Data	-	-	-	-	-	**No**
Comp 2	User Notification	Data	-	-	-	-	-	**No**
Comp 3	Seek Camera	Hardware	Yes	**No**	Yes	**No**	-	**No**
Comp 4	Raspberry Pi 4 Model B	Hardware	Yes	**No**	**No**	**No**	-	**No**
Comp 5	Raspberry Pi 4 SD Card	Hardware	Yes	**No**	**No**	**No**	-	**No**
Comp 6	Speaker Device	Hardware	Yes	**No**	**No**	**No**	-	**No**
Comp 7	Trigger Button	Software	-	Yes	**No**	Yes	Yes	**No**
Comp 8	Raspberry Pi OS	Software	-	Yes	**No**	Yes	Yes	**No**
Comp 9	Image Classification Module	Software	-	**No**	**No**	**No**	Yes	**No**
Comp 10	Web Server App	Software	-	Yes	**No**	Yes	Yes	**No**
Comp 11	Camera Interface	Software	-	**No**	**No**	**No**	Yes	**No**
Comp 12	USB-C Cable	Connectivity	Yes	**No**	**No**	**No**	-	**No**
Comp 13	Speaker BLE 4.0	Connectivity	-	Yes	Yes	**No**	-	**No**
Comp 14	HTTP Web Server	Connectivity	-	Yes	**No**	Yes	-	**No**

Fig. 2. AniLarm IoT Prototype for Small Animal Detection

users and systems. **Req 5: Software Updates and Patching** – Devices must support updates to address vulnerabilities. **Req 6: Cyber Incident Detection and Response (CIDR)** – Devices must detect and respond to security incidents effectively.

B. Evaluating Requirements and Prototype Components

The compliance of each component with NIST IR 8259A is assessed as: **Yes** (fully compliant), **No** (not compliant), or **-** (not applicable) to identify strengths, weaknesses, and guide improvements (see Table I).

IV. RESULTS AND DISCUSSION

This section summarizes the implementation, testing, and compliance outcomes of the AniLarm prototype based on NIST IR 8259A requirements, as well as its performance and accuracy metrics. Figure 2 shows the AniLarm prototype, which processes data locally within 28 seconds, achieving 97.83% accuracy in identifying small animals. Images are deleted after processing or if no connection exists. The hardware uses unique IDs, but CIDR requirements were omitted due to functional constraints. Software includes access control, offline operation, and data encryption, with Bluetooth 4.0 providing encryption, though connectivity security is limited.

Compliance with NIST IR 8259A varies across components. While software components like the Web Server App and Raspberry Pi OS meet secure configuration, access control, and software update requirements, hardware components such as the Seek Camera and Raspberry Pi SD Card have gaps in data protection and access control. The system also lacks CIDR compliance, requiring customized implementation for resource-constrained offline devices. Despite offline operation reducing internet-based threats, hardware and connectivity vulnerabilities must be addressed for full compliance across all system layers in safety-critical applications (see Table I).

V. CONCLUSION

The AniLarm system, guided by NIST IR 8259A, shows how IoT edge devices can be secured for safety-critical applications, though gaps remain in CIDR and hardware access control. Future work will focus on lightweight CIDR mechanisms, improved hardware security, and evaluating a more comprehensive end-to-end data security approach.

REFERENCES

[1] "What ratan tata said about stray animals' safety during monsoon." https://www.news18.com/business/what-ratan-tata-said-about-stray-animals-safety-during-monsoon-8255647.html. [Accessed 08-09-2024].

[2] "How to keep cats from under your car." https://vetexplainspets.com/how-to-keep-cats-from-under-your-car/. [Accessed 08-09-2024].

[3] R. Sedouram and D. V. Klein, "Safer audio consumption while driving." Technical Disclosure Commons, April 2023.

[4] A. C. L. U. (ACLU), "Know your rights: Photographers." https://www.aclu.org/issues/free-speech/photographers-rights, 2023. Accessed: 2023.

[5] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "Iot device cybersecurity capability core baseline," 2020.

[6] B. Sereda and J. Jaskolka, "An evaluation of iot security guidance documents: A shared responsibility perspective," *Procedia Computer Science*, vol. 201, pp. 281–288, 2022.

[7] J. McCarthy, J. Marron, D. Faatz, D. Rebori-Carretero, J. Wiltberger, and N. Urlaub, "Cybersecurity for smart inverters: Guidelines for residential and light commercial solar energy systems," tech. rep., National Institute of Standards and Technology, 2024.

[8] T. P. Dover, "Evaluating medical iot (miot) device security using nistir-8228 expectations," *arXiv preprint arXiv:2104.03283*, 2021.

[9] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, *Foundational Cybersecurity Activities for IoT Device Manufacturers*. US Department of Commerce, NIST, 2020.

[10] M. Fagan, J. Marron, K. Brady, B. Cuthill, K. Megas, and R. Herold, "Creating a profile using the iot core baseline and non-technical baseline," tech. rep., National Institute of Standards and Technology, 2020.

[11] R. Choutapally, K. R. Saddikuti, and S. Berhe, "Anilarm: Offline ai for small animal detection under cars using thermal camera," in *Submitted to IEEE Conference on Artificial Intelligence*, 2025.