Chapter 17
Smart Homes, Smarter Parenting:
Implementing Context-Aware IoT Access Controls for Child Safety

Hitesh Rawat
https://orcid.org/0009-0006-7171-6016
University of Extremadura, Spain

George Kurian
https://orcid.org/0000-0003-4137-7464
Eastern New Mexico University, USA

Priyanka Gupta
Shri Vaishnav Vidyapeeth Vishwavidyalaya, India

Alpesh Soni
Shri Vaishnav Vidyapeeth Vishwavidyalaya, India

ABSTRACT

With the rise of IoT devices in smart homes, child safety has emerged as a key issue for modern parents. This study proposes CA-SHIELD (Context-Aware Smart Home IoT Enforcement for Limiting Danger), a dynamic access control framework that adapts based on user identity, activity context, and risk level. Evaluated using the 2024 REALHome Dataset, which includes over 45,000 hours of smart home data from 20 family households, CA-SHIELD employs a hybrid approach—merging rule-based logic with LSTM-powered context recognition. The system effectively identifies unsafe access attempts with 95.2% accuracy and reduces children's risky interactions with IoT devices by 92.8%, all without disrupting daily routines.

DOI: 10.4018/979-8-3373-2716-7.ch017

Compared to traditional role-based models, CA-SHIELD improves precision by 18.5% and overall control effectiveness by 21.3%, highlighting its potential as a robust safety layer in child-focused smart environments.

1. INTRODUCTION

The rapid advancement of Internet of Things (IoT) (Li and Wu,2022) technologies has transformed traditional homes into interconnected, intelligent environments—commonly referred to as smart homes. These environments are equipped with smart locks, voice assistants, surveillance systems, thermostats, and kitchen appliances, all of which can be remotely accessed and controlled. While these innovations improve convenience and energy efficiency (Rawat et al., 2025), they also introduce new challenges, particularly in ensuring the safety of children within these connected spaces.

Recent reports indicate a 36% increase in child-related incidents (Khanpara et al., 2023) involving smart devices (Rajavat et al., 2024) over the last three years (IoTSec Analytics, 2024). For example, cases where children unintentionally unlocked smart doors, accessed kitchen appliances, or altered home security settings have raised serious concerns among parents and security experts (Rawat and Rajavat,2024a). A notable case in 2023 involved a five-year-old in California who managed to control the home's smart oven using a voice assistant, triggering a near-fire event—highlighting the urgent need for context-aware access controls.

Current access control mechanisms in smart homes are largely static or role-based, failing to adapt to real-time contextual (Mishra et al., 2024) cues such as user behavior, time of day, or environmental risk levels. To address these limitations, we propose CA-SHIELD (Context-Aware Smart Home IoT Enforcement for Limiting Danger) (Alqahtani et al., 2022)—an adaptive access control system designed to enhance child safety in smart home environments. CA-SHIELD leverages context recognition powered by Long Short-Term Memory (LSTM) (Sikder et al., 2022) neural networks, combined with a rules-based inference engine to make dynamic access decisions.

The system is trained and validated using the REALHome 2024 dataset (Alqahtani et al., 2025) (Burakgazi et al., 2023), a newly released real-time smart home dataset comprising over 45,000 hours of IoT interactions collected from 20 family households. This dataset includes detailed annotations of user identity, location, activity, and device usage logs. Through this, CA-SHIELD achieves an access prediction accuracy of 95.2%, successfully preventing over 92% of unsafe device interactions initiated by children (Mao and Chang, 2023) (Doghramachi and Ameen,2021). These