McGill University – INTG 215

Project Outline

Integrated Smart-Home Security Gateway for Consumer IoT Protection

Team Members

Charles de Bettignies (MC GILL ID)
Thomas Joliveau (MC GILL ID)
Raphaël Lemarié (MC GILL ID)
Tianhe Li (MC GILL ID)
Noé Manwaring–Favennec (MC GILL ID)

NE PAS METTRE LES ID MC GILL TANT QUE CE N'EST PAS DEMANDÉ CE DOCUMENT EST PUBLIC POUR LE MOMENT.

Montreal, QC

Due Date: November 26, 2025

1. Executive Summary

2. Background & Context

Over the past decade, the Internet of Things (IoT) witnessed dramatic expansion in scope, connectivity, and impact. IoT evolved from basic experimental concepts into an ambitious technology present in industries, cities, and homes, with promised revolutions on electronic equipment systems. Looking ahead, IoT is predicted to bring even greater utility to housing electronics, transforming smart homes from the fundamental perspectives with singular benefits including real-time automation, energy optimization, and predictive maintenance.

By 2024, the number of connected IoT devices will have sharply increased to over 18.5 billion, marked as a symbol of significant market evolution, technological advancements, and enhanced interoperability of IoT devices. Adoption of new wireless technologies such as LTE-M, NB-IoT, and the introduction of 5G RedCap enabled affordable, low-latency connections suitable for a vast array of devices globally, which provides faster and more reliable communication for IoT and electronic ecosystems. Besides the improvements of connectivity, the proliferation of sensors and embedded systems has also expanded IoT's reach, while the rapid evolution of Artificial Intelligence (AI) further empowered these devices to become smarter and more autonomous.

Beside the industrial application that's already fully demonstrated, IoT devices are predicted to be utilized among housing electronics, forming the foundational infrastructure for future smart homes. The interconnection of various home elements and equipment including lighting, heating, ventilation, air conditioning and security systems are enabled by IoT technologies. It provides the promised potential in improving enhanced energy efficiency, convenient automation, and improved living comfort by the employment of intelligent sensors combined with machine learning, allowing predictive maintenance and adaptive environmental control. The implementation of IoT devices for housing allows homeowners to remotely monitor and manage devices through automated systems.

Furthermore, ongoing standardization efforts and integration with renewable energy systems such as solar panels and heat pumps provides further possibilities regarding the integration between Internet of Things (IoT) with residential electronics. All provide a sustainable and smarter resource management for housing electronics.

In summary, significant progress was made within the field of IoT devices over the past decade, with the notable improvements in the device connectivity, technology complexity, and moreover the standardization. The foundation for IoT to revolutionize residential electronics, while enabling the creation of a highly interconnected, smart, and energy efficient housing environment is obtained. This development has led to a promised convenient and controllable housing

network, which contributes to sustainable living and more responsive home management. It has highlighted the crucial role of the IoT within future residential technologies and frameworks.

3. Problem Statement & Opportunity Identified

The Internet of Things (IoT) is growing very rapidly in the residential sector; this has created a great market opportunity. There is an explosive growth in device adoption; however, this growth is inherently restrained by a critical problem: the lack of a trustworthy security and privacy framework for connected devices. This lack is caused by a widespread design decision to prioritize convenience and connectivity over robust protection which undermines user adoption. Our main finding, as expanded upon in the market research summary, is that users are deeply concerned about data collection and device hijacking. While some security options exist, they are usually complex and designed for users with a high technical knowledge of IoT networks. This constitutes a technical barrier that makes security inaccessible to the average IoT consumer. This shows a discrepancy between customer's expectations of trustworthiness and the technology currently available to them and constitutes a clear market need.

4. Proposed Solution or Innovation

4.1 Plug & Play Architecture

4.2 Cross-Protocol Intelligence & Compatibility

4.3 Local Privacy

5. Market and User Research Summary

5.1 Market Opportunity

5.2 Target User

5.3 Competitor Analysis

5.4 The Opportunity

5.5 Key Trends & External Factor

6. Feasibility Analysis

7. Implementation Roadmap

8. Team Roles & Contributions

9. Challenges & Limitations

References