Voice Interfacing and Control of Home IoT Networks

Our Mentor: Prof. Prasad Honnavalli

Shashank Prabhakar	01FB16ECS356
Shrey Tiwari	01FB16ECS368
Sumanth V Rao	01FB16ECS402

November 27th, 2019

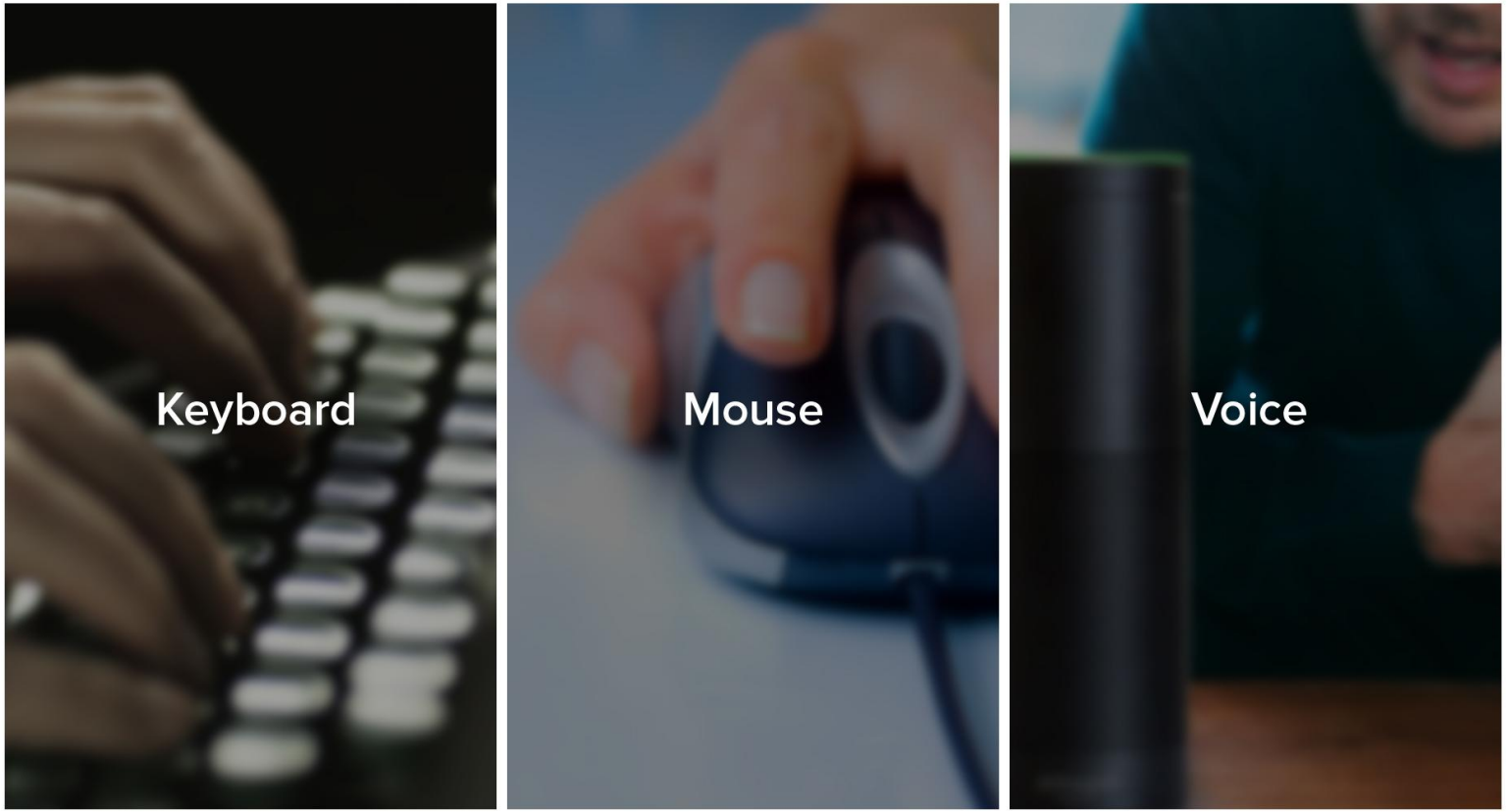
Table of contents

Motivation

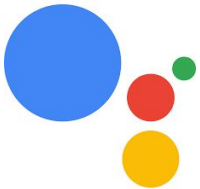
Current IoT Home Automation Landscape

- **High Cost**
  Expensive products and high installation/modification charges
- **No Interoperability**
  Products are tied to their specific platforms
- **Low on security**
  Many attack surfaces for IoT networks
- **Fragmented**
  Solutions and technologies that are incomplete and specific
- **Mutually exclusive ecosystems**
  Market is dominated by a few companies and they have different sales channels.

Voice is the way ahead



Project Abstract and Scope



Google Assistant

Amazon Alexa

- Our project aims to build an intuitive and robust solution for automation and control of home IoT networks.
- **Architect** a **platform agnostic** solution to overcome existing gaps and meet the performance and cost constraints
- **Security by design**: Use STRIDE Threat Modelling approach to identify vulnerabilities in the network and devise appropriate countermeasures
- Make appropriate **design choices** to incorporate the same in the architecture

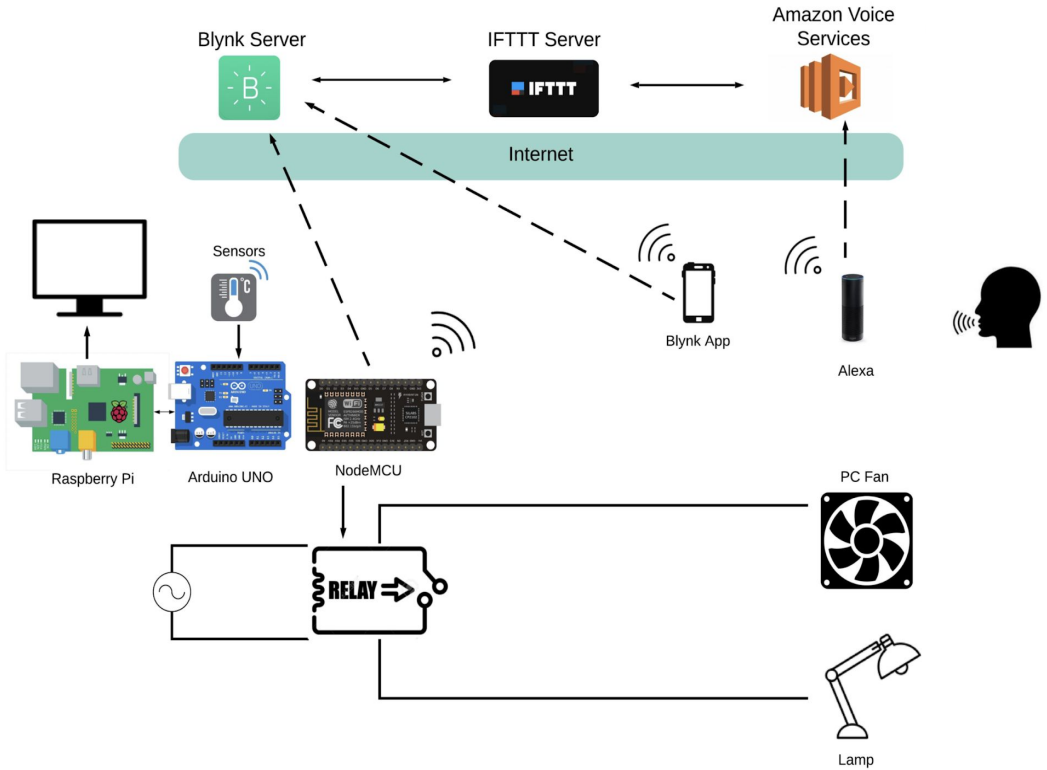
Non-functional Requirements

- ***Cost-effectiveness***
  The solution should be cheap. Must integrate with existing infrastructure.
- ***Security***
  The network should have security by design.
- ***Scalability***
  The design should not have any choke points. It must be easy to add more devices.
- ***Manageability***
  The interfacing with the network should be seamless and intuitive.
- ***Configurability***
  It should be possible to update and configure the network over the air.

Literature Survey

- Y. Igarashi, M. Hiltunen, K. Joshi, and R. Schlichting, ``**An Extensible Home Automation Architecture based on Cloud Offloading**", In 18th International Conference on Network-Based Information Systems, 2015.
- D. Greenstreet and J. Smrstik, Texas Instruments, ``**Voice as the user interface – a new era in speech processing**", May 2017.
- V. Stangaciu, V. Opârlescu, P. Csereoka, R. D. Cioargă, and M. V. Micea. ``**Scalable Interconnected Home Automation System**", In 21st International Conference on System Theory, Control and Computing (ICSTCC), 2017.
- D. Kumar, R. Paccagnella, P. Murley, E. Hennenfent, J. Mason, A. Bates, and M. Bailey, ``**Skill Squatting Attacks on Amazon Alexa**", In 27th USENIX Security Symposium, ISBN 978-1-931971-46-1, Aug., 2018.
- Booz Allen Hamilton, ``**2019 Cyber Threat Outlook**", 2019.
- J. Cichonski, J. Marron, and N. Hastings, ``**Security for IoT Sensor Networks**", National Institute of Standards and Technology, February 2019.
- C. Withanage, R. Ashok, C. Yuen, and K. Otto, ``**A Comparison of the Popular Home Automation Technologies**", In IEEE Innovative Smart Grid Technologies, 2014.
- R Style Labs, ``**Building Intelligent Connected Home Solutions: Challenges and Ways to Overcome Them**", 2019.
- M. Fagan, M. Yang, A. Tan, L. Randolph, and K. Scarfone, ``**Security Review of Consumer Home Internet of Things (IoT) Products**", National Institute of Standards and Technology, U. S Department of Commerce Tech. Report, October 2019.

Previous Architecture



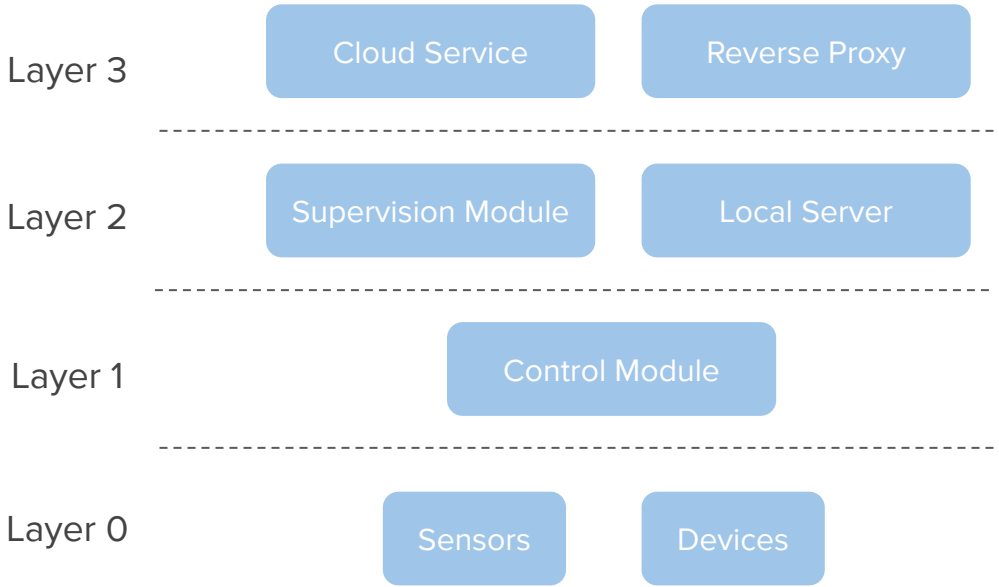
Advantages

- Simple
- Cost effective
- Secure

Disadvantages

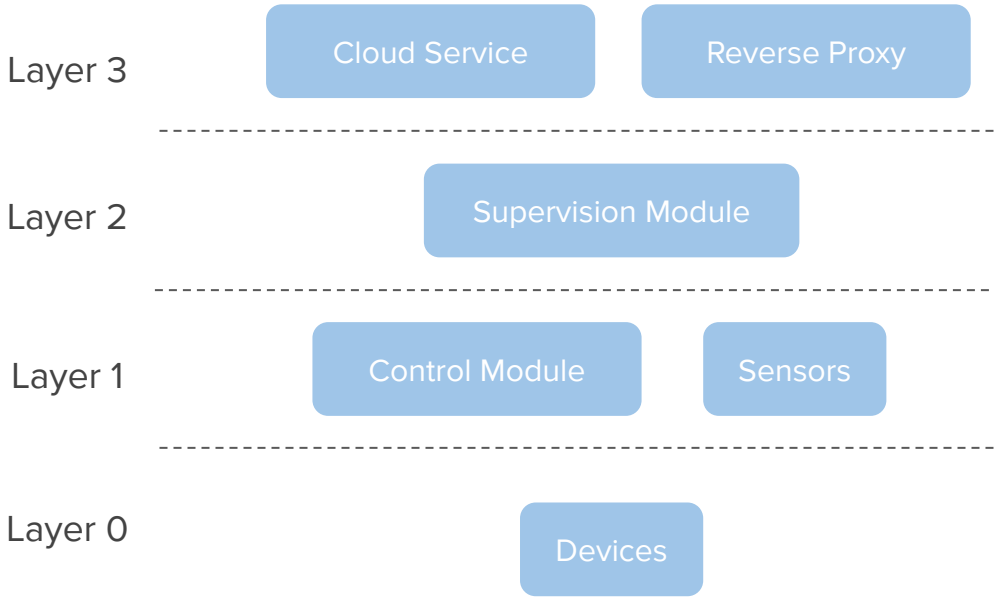
- High latency
- Limited capabilities
- Low configurability
- Platform dependence

Proposed Architecture - High Level View



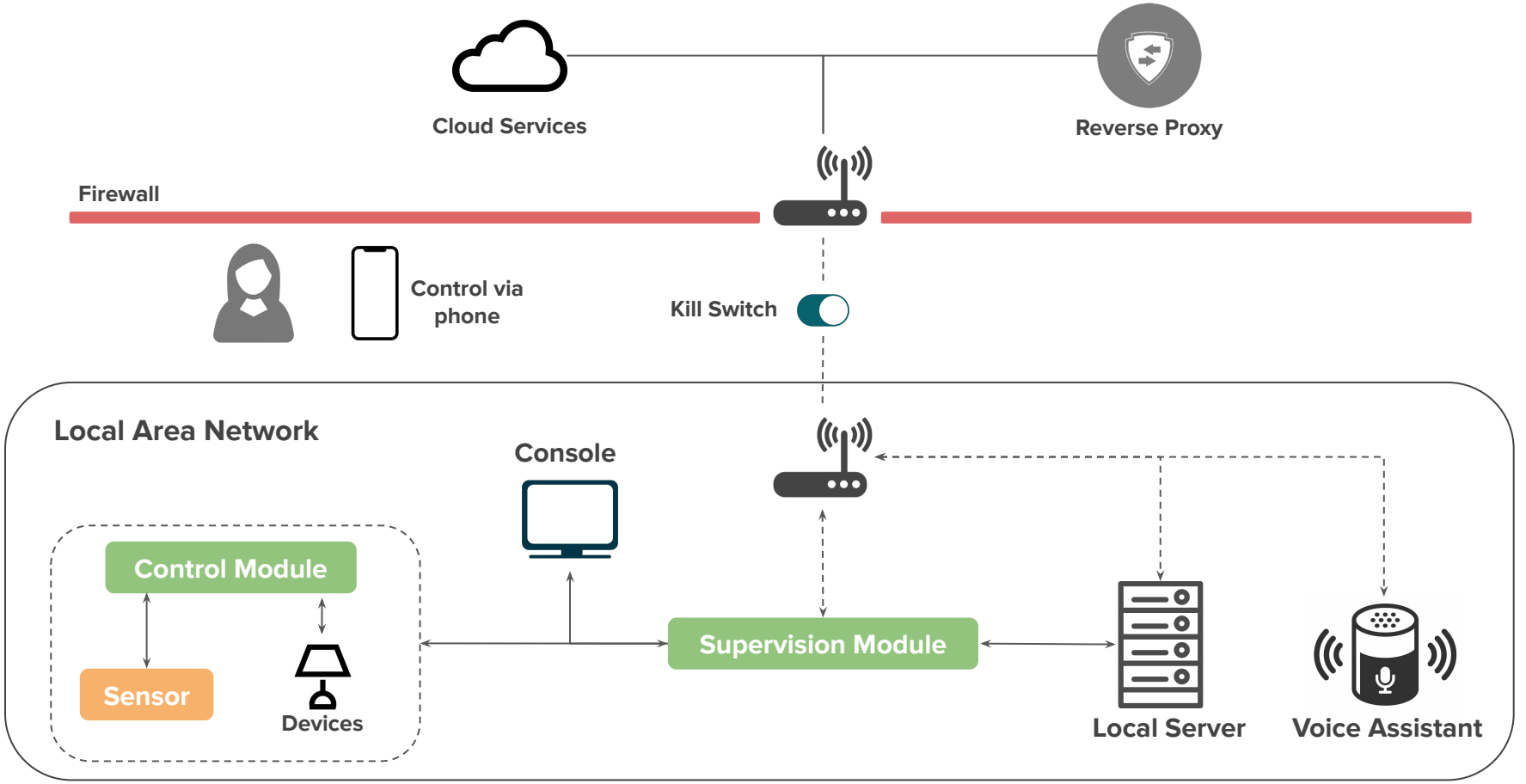
- **Control Module**
  Wifi enabled boards to control the IoT network
- **Supervision Module**
  Manages the control modules and the data
- **Local Server**
  Endpoint for the outputs from voice assistant services

Proposed Architecture - High Level View



- **Control Module**
  Wifi enabled boards to control the IoT network
- **Supervision Module**
  Manages the control modules and the data
- **Cloud Server**
  Endpoint for the outputs from voice assistant services

Architecture - Iteration 1



Use and Misuse Cases

USE CASES	MISUSE CASES	COUNTERMEASURES
Control and interface with devices using voice commands	Skill Squatting	Certification systems and verification of skills
Control and interface with devices using the web application	Unauthorized access and control of an IoT device using voice commands	Voice recognition and unique passphrases
Ability to perform compound actions	Information leakage from IoT home monitor to outsiders or guests	Access Control
Adding, removing and discovery of devices	Use home IoT network as Botnet to launch DDoS attack	Firewalls and Intrusion Prevention Systems
Adding and deleting users of the devices	Privacy breach by exploiting vulnerabilities of voice assistant	Kill Switch
Control third party devices	Gain access IoT network via voice commands when not at home	Disabling voice interfacing subsystems in the absence of the owner

Threat Modelling - STRIDE

Threat modelling works to **identify**, **communicate**, and **understand** threats and **mitigations** within the context of protecting something of value

- S — SPOOFING
- T — TAMPERING
- R — REPUDIATION
- I — INFORMATION DISCLOSURE
- D — DENIAL OF SERVICE
- E — ELEVATION OF PRIVILEGE

Threats and Countermeasures - Spoofing

Threat	Countermeasure
An attacker can reuse a password	• Periodic changing of passwords
An attacker can anonymously connect to the network	• Secure communication protocols (WPA2 - PSK) • Session cookies
Response spoofing from the server	• Security by Obscurity - Reverse Proxy • Nonce • Encryption
System ships with default passwords	• Software authentication architecture - force change default passwords

Threats and Countermeasures - Tampering

Threat	Countermeasure
Distributed '***Access Control***' rules	• Centralized Home Hub
An attacker can replay data without detection	• Nonce - timestamps and sequence numbers
An attacker can directly modify or write to a data store	• Secure communication protocols • Access control

Threats and Countermeasures - Repudiation

Threat	Countermeasure
The system has no logs	• Logging software
An attacker can alter log messages on the network	• Heartbeat option for logging system
An attacker can edit logs and there's no way to tell	• Secure communication • Access control

Threats and Countermeasures - Information Disclosure

Threats	Countermeasure
An attacker can see error messages with security-sensitive content	• Default error messages
An attacker can act as the man in the middle	• Encryption • Certification
The attacker can discover the fixed key being used for encryption	• Periodic change of keys • Secure storage of keys

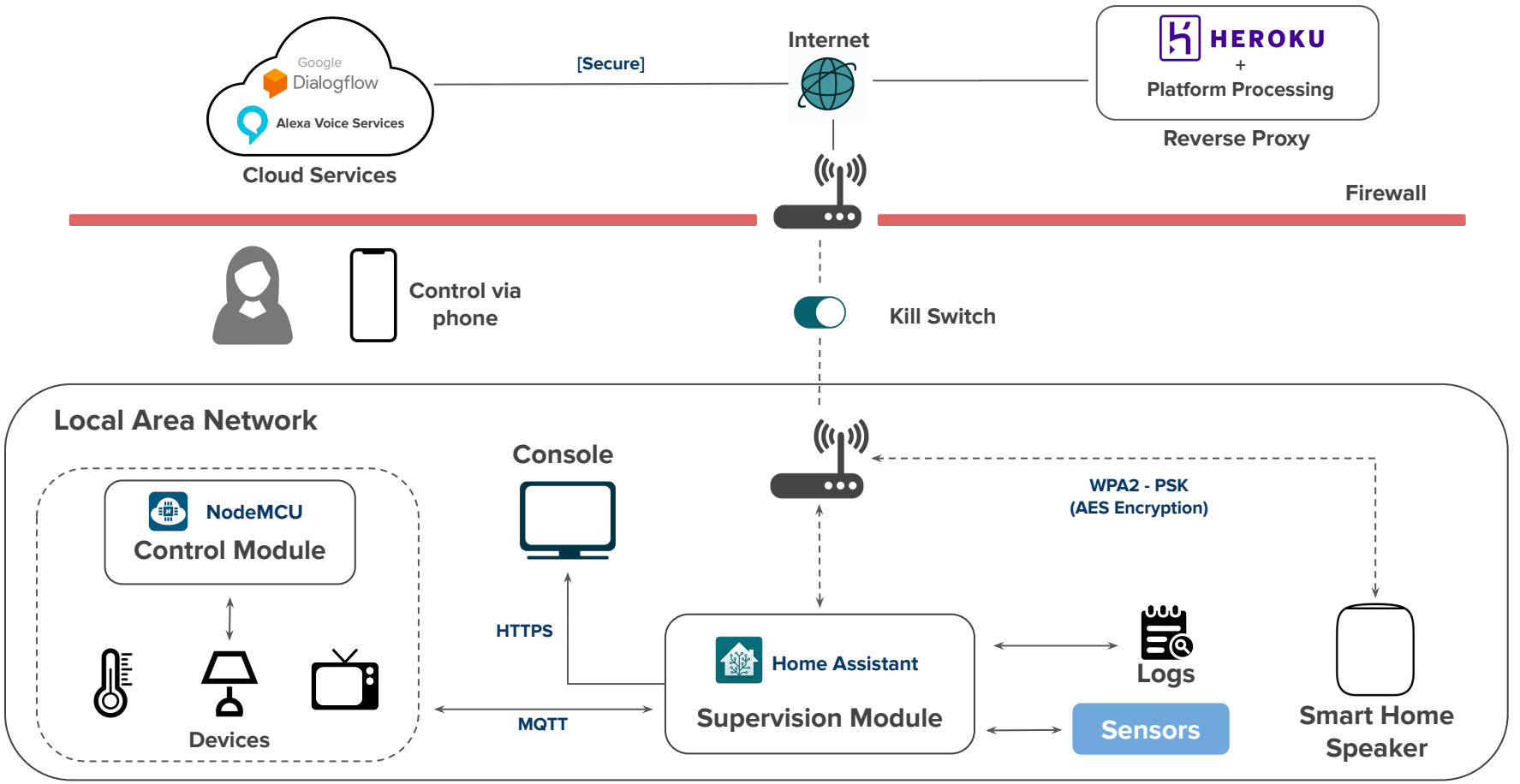
Threats and Countermeasures - Denial of Service

Threat	Countermeasure
An attacker can render your authentication system unusable	• Security by obscurity - Reverse Proxy
An attacker can make your network unstable	• Rate limiting on requests per device
An attacker can block functionality	• Rate limiting on requests per device • Intrusion Detection Systems

Threats and Countermeasures - Elevation of Privilege

Threats	Countermeasure
A single person holds all the access rights	
You include user-generated content within your page, possibly including the content of random URLs (XSS)	• Handled by protocols and structured communication standards.
An attacker can inject a command that will run at a higher privilege level	• Code filtering • Network segmentation

Architecture - Incorporating Design Choices



Design Choices

Home Assistant

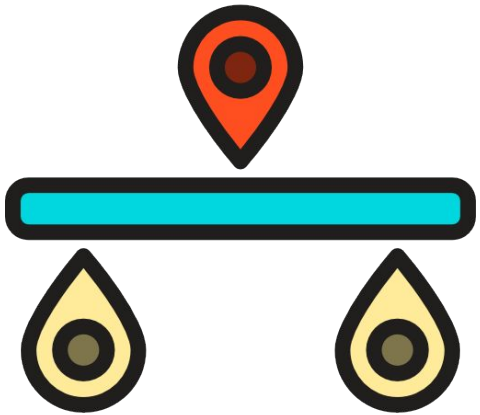
- **Publisher-Subscriber** communication model
  Implement the communication using the '***Message Queuing Telemetry Transport***' protocol

  Properties:
  - Scalable
  - High Availability and Redundancy
  - Retains messages for sessions
  - Connection State change monitoring

  Security:
  - Certificates
  - TLS
  - Authentication (username and password)

- **Heroku** as the **Reverse Proxy**

- **Home Assistant** as the home hub



Implementation - Semester 8

- **Hardware**
  - Rewiring and connecting devices
  - Designing **Two-Way** switching
- **Skills Development**
  - Create and deploy skills on both platforms
- **System Integration**
  - Hardware and software integration
- **Software and Penetration Testing**
- **Research paper**

PES UNIVERSITY

Thank you