

# Securebox: Platform for Safeguarding Network Edge

Ibbad Hafeez\*, Aaron Yi Ding§, Lauri Suomalainen\*, Sasu Tarkoma\*

\* Department of Computer Science, University of Helsinki, Finland

§ Department of Informatics, Technical University of Munich, Germany

## Background and Motivations

- Billions of smart devices in residential and corporate networks
- IoT devices with limited support are inherently vulnerable
- Security and management in IoT ecosystem is critical
- SDN design brings programmability and extensibility
- Cloud resources for scalability, flexibility & cost efficiency
- Potential of combining SDN and cloud-based security services

## Challenges

- Lack of support to run end-host based security applications
- Complex cross-device dependencies and interactions
- High cost and less scalability of traditional network security solutions e.g., firewall, IDS/IPS.s
- Need for automation in network security and management
- Balance between cost and performance

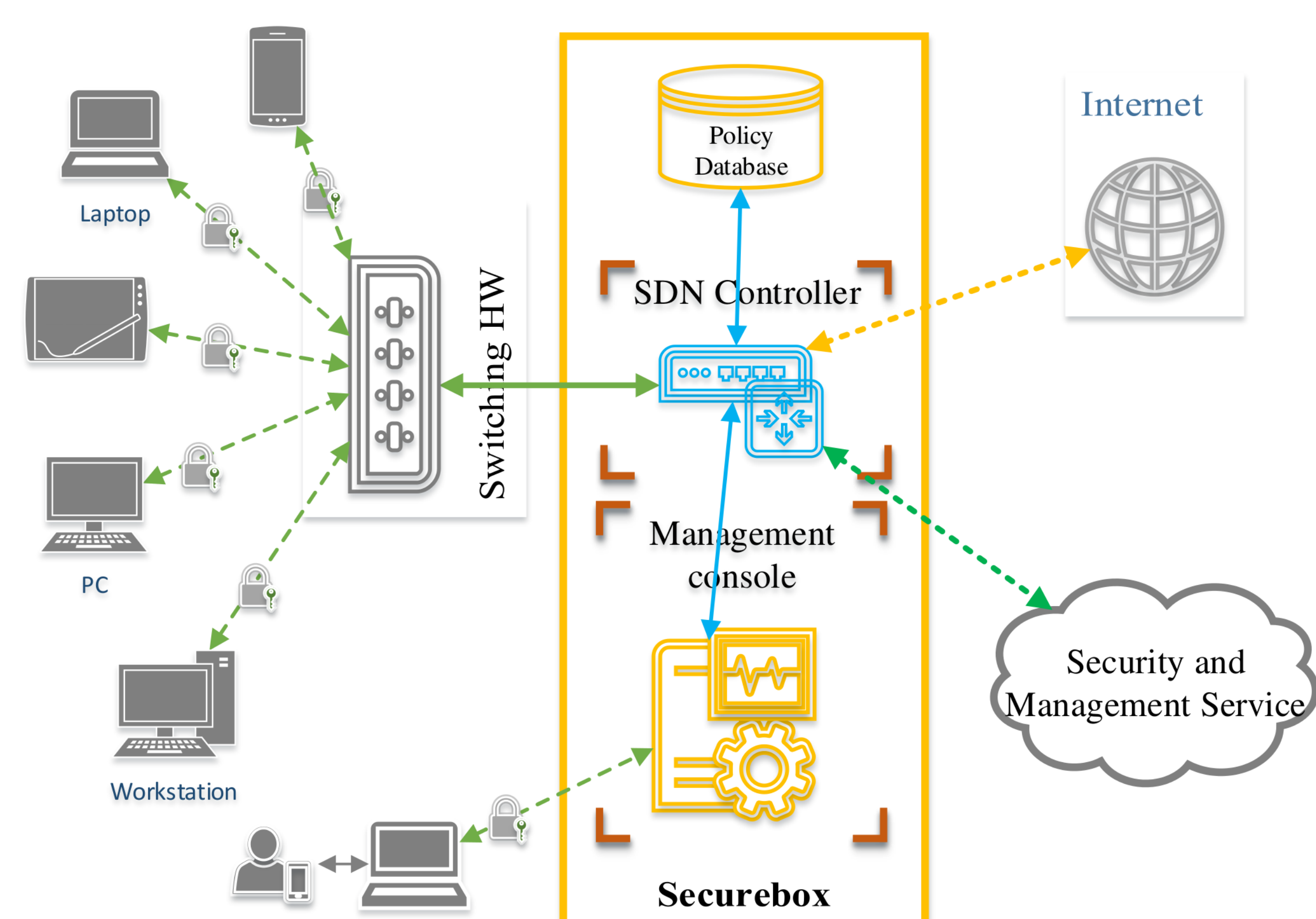
## Research Questions

- How to secure IoT ecosystem
- How to develop self-adaptive edge networks
- How to build responsive, deployable and extensible platform
- What are limitations and overhead for our outsourcing security and management to third party.

## Key Components

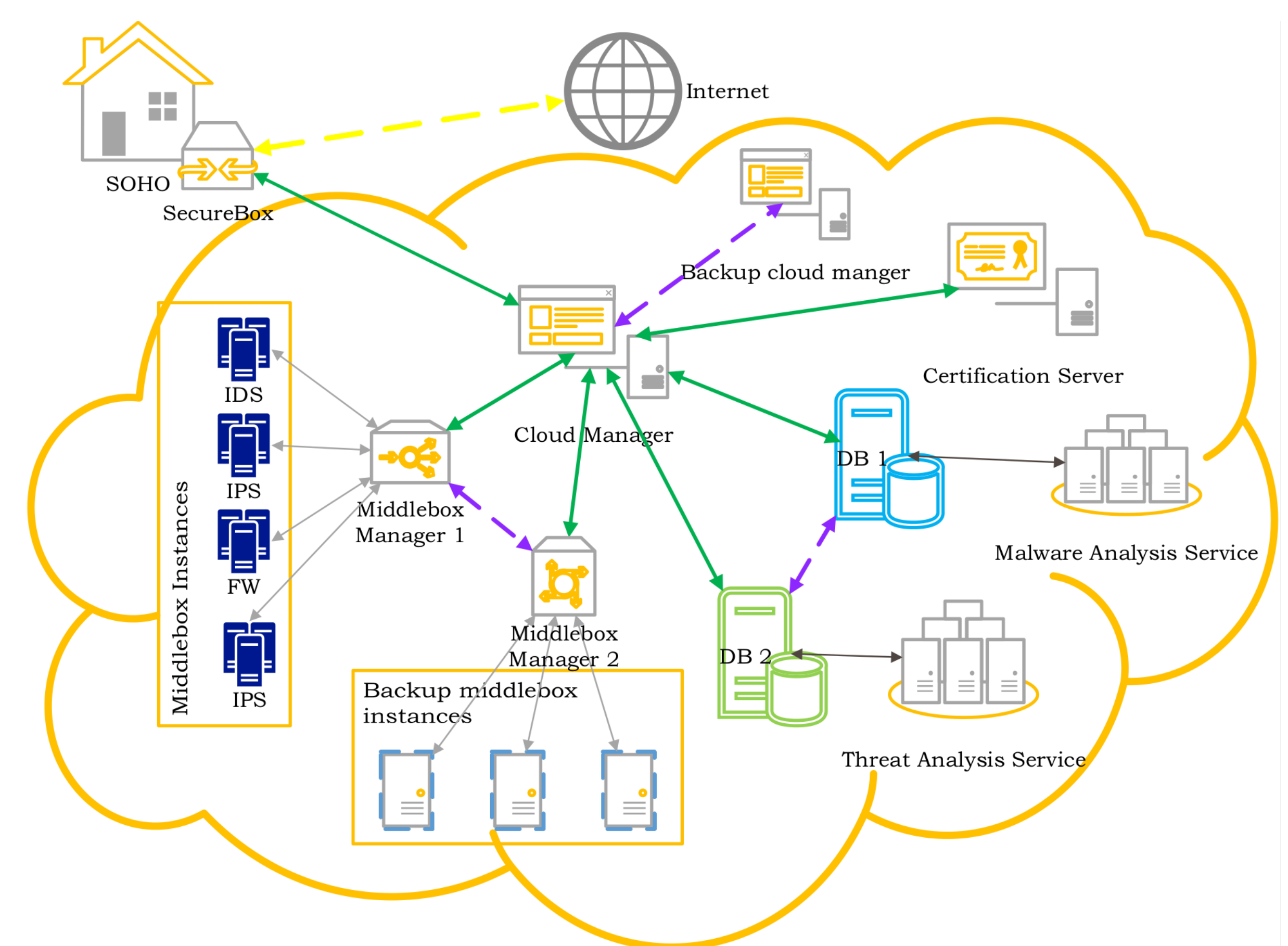
- Redesigned gateway for edge networks
- Service backend for managing gateways at the edge.

## Gateway Design



Security Gateway Design

## Security and Management Service Design



Security and Management Service

## Prototype Implementation

- OF-enabled access point based on Raspberry-PI running Floodlight SDN controller, Open vSwitch.
- SMS deployed using Kubernetes and with lightweight services running as Docker Containers

## System Highlights

- Easy of deployment and management.
- Cost efficiency with transparency and control for users.
- Openness – standardized protocol and open-source platform
- Programmability – extensible for integrating security services
- Adaptive – on demand and elastic
- Collaborative analytics for mitigating security threats

## Use Cases

- “Everything in a box” for security enhancement of smart home
- Detect and diagnose attacks for enterprise/campus scenarios
- Outsource security functionality
- Risk assessment of network environment

## Future Work

- Enhance network and cloud managers
- Support more security services with Docker and VM
- Extensions for multiple scenarios – wired and wireless
- Hierarchical management framework
- Minimize the latency of security operations
- Protect activities inside home network environment