Internet of Things

Programming

Lecture WEEK-11

Advance Topics in IoT-II

Swinburne University of Technology

May 2023

PART I: IoT security

Background

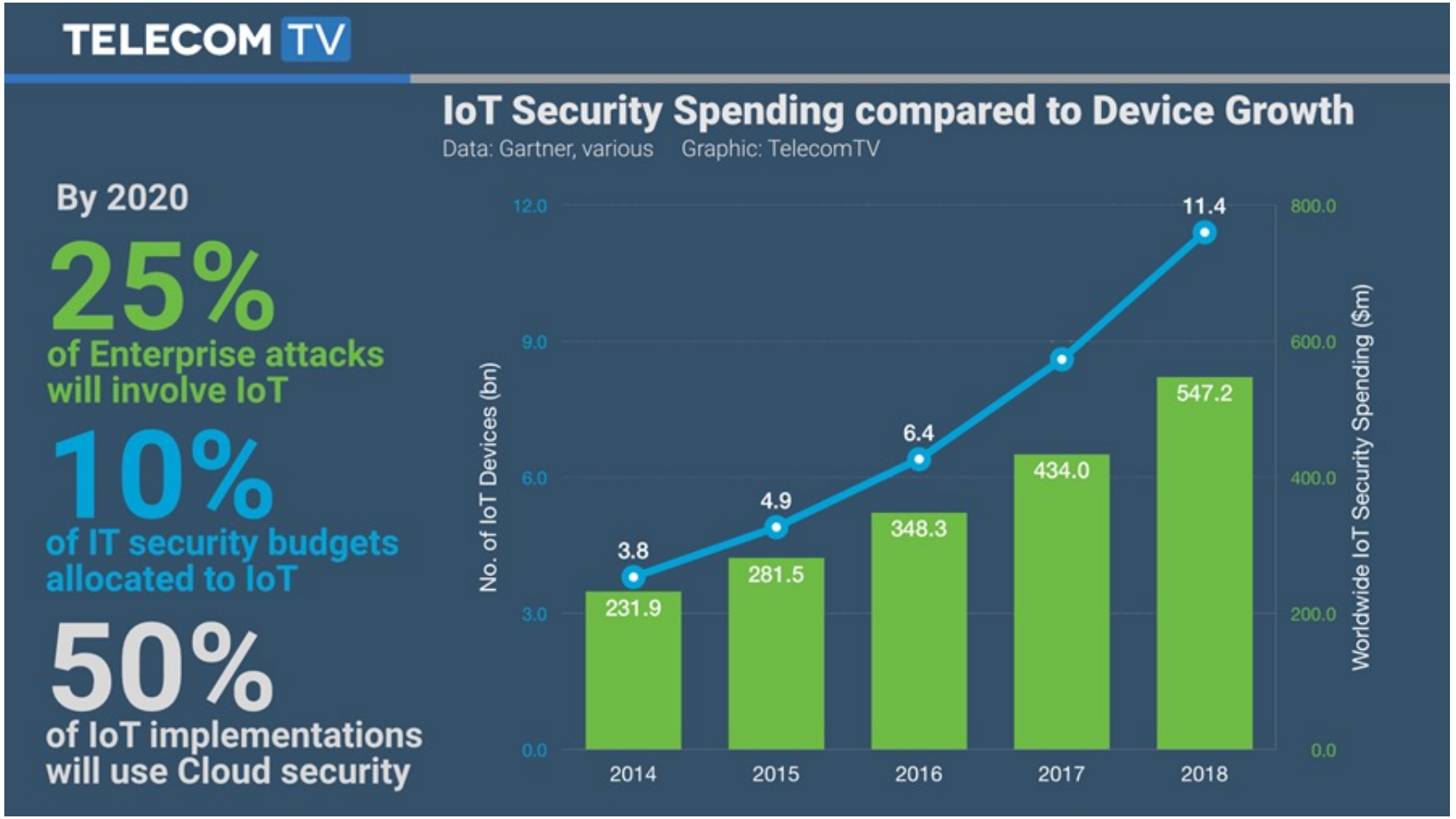
- Growth in the number of connected devices by 21% between 2016 to 2022.
- Multiple IoT ecosystems: constraint sensors to autonomous vehicles.
- Internet which is meant to provide a trustworthy platform.
- IoT therefore needs to be secure.

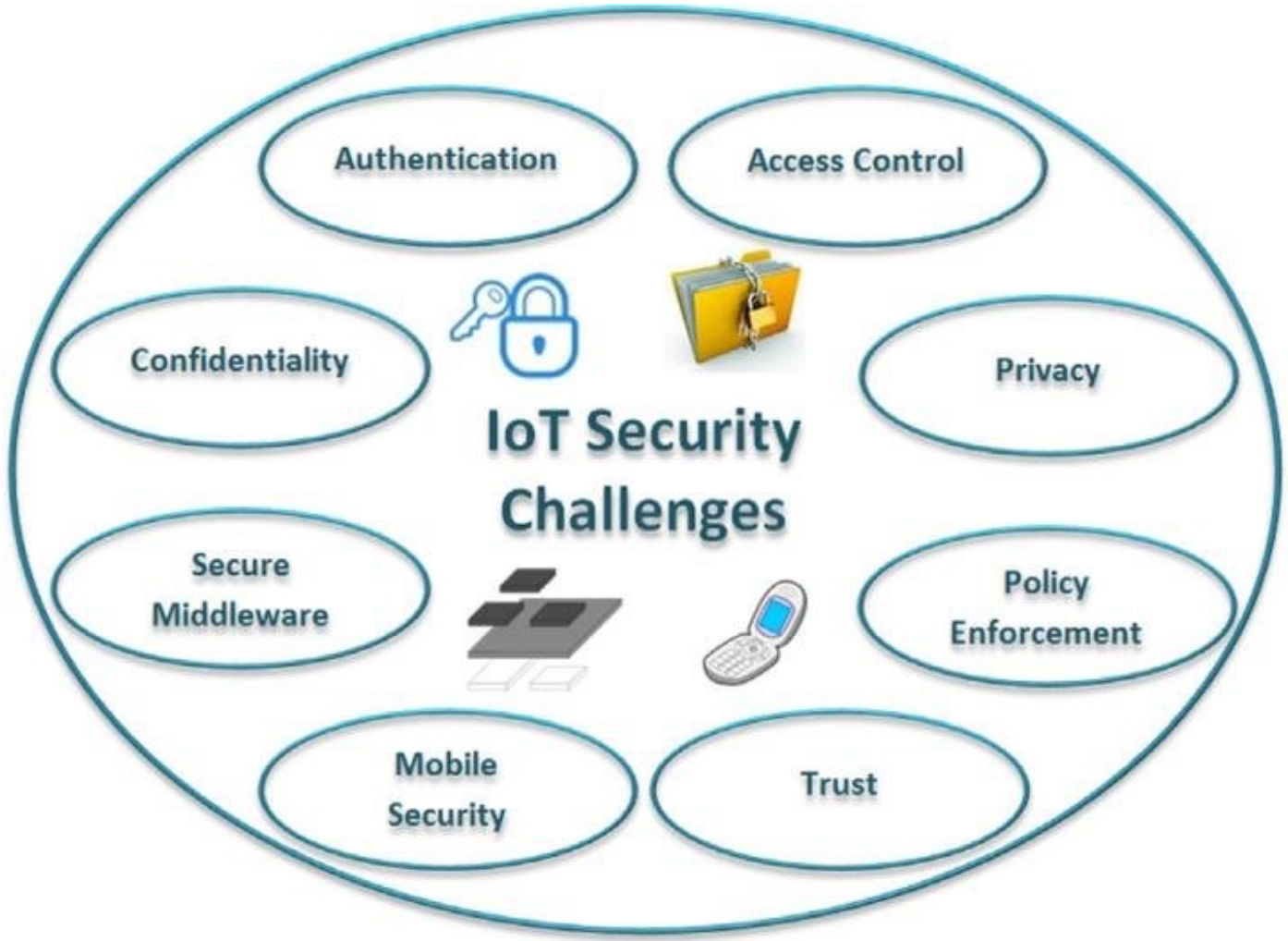
Source: https://www.ericsson.com/en/reports-and-papers/white-papers/iot-security-protecting-the-networked-society

Security in IoT

- Internet-enabled devices (such as, home appliances, connected cars, medical devices, and safety equipment) are usually directly accessible over the Internet. This unprecedented connectivity of IoT devices raises many security and privacy issues.
- There are several aspects of IoT that present security and privacy problems including IoT device communications, constrained resources (e.g., limited battery life), variety (e.g., different types of devices made by multiple manufactures), and the scale, i.e., billions of devices

IoT Security




Authentication
Access Control
Confidentiality
Privacy
IoT Security Challenges
Secure Middleware
Policy Enforcement
Mobile Security
Trust

IoT Security challenges

- Cybersecurity for billion of devices
- Privacy and information security
- Device security
- Trust
- Authentication

Cybersecurity for Billions of devices

- Gartner forecast(2016): more than 25% of all enterprise attackers are estimated to attack Industrial IoT solutions.
- Industrial IoT(IIoT):
  - Autonomous control system
  - One such attack is DDoS
  - More serious issue for the society: as neither the owner nor seller bear the cost of the attack

Privacy and information security in IoT

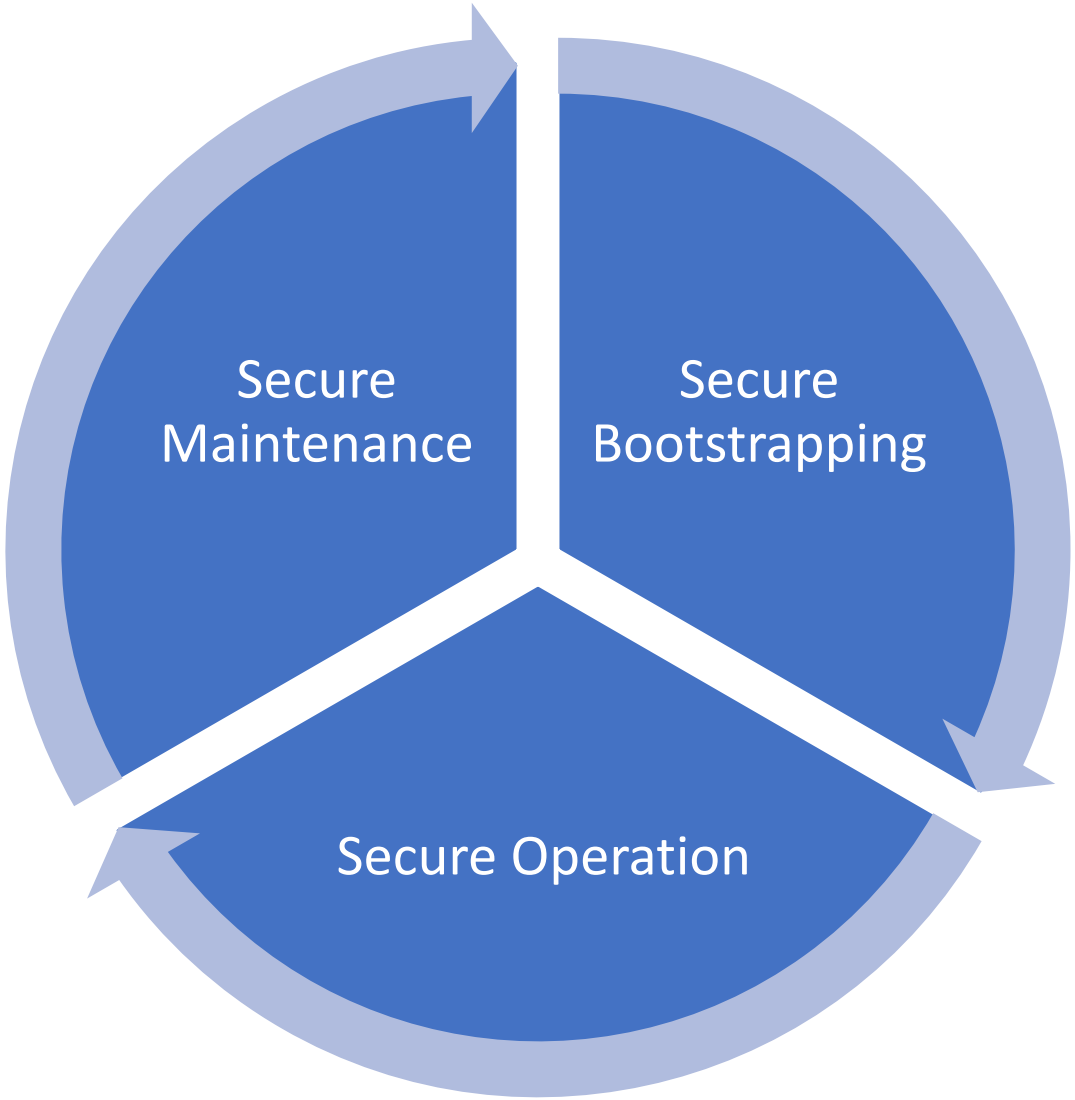
- Privacy in IoT has been widely discussed over the years by researchers and media persons.
- Data related to electricity consumption or room temperature may be seeming harmless
- But with billions of such devices generating potentially lots of sensitive information about people’s movement, activities, and health may create serious privacy issues.

Device security

- IoT device are small devices having limited memory, limited battery life, and limited processing.
- Therefore, ensuring remote firmware updates for securing such constrain devices is a big challenge.

Trust

- In IoT, we use gateways as an intermediate device between sensors and cloud to offload processing.
- These gateways create a new attack surface.
- A trust model breaks down when the security of any of these intermediate nodes is compromised.
- To address this: application layer security, blockchain solutions


Secure
Maintenance
Secure
Bootstrapping
Secure Operation

Secure Bootstrapping

- The life cycle of an IoT device begins when it is installed and activated in a network. Secure bootstrapping denotes the process by which that device can securely join the IoT network.
- In relation to OSI security requirements, this process includes authentication and authorisation of a device.

Secure Operation

- After joining the network, the IoT device starts to operate providing the corresponding services for which it was created. Just as in the bootstrapping stage, the consideration of security mechanisms is necessary at this stage to protect access to resources that are hosted on the device.

Secure Maintenance

- For an IoT device with a lifetime spanning several years, it could be maintained to eventually be upgraded, reconfigured, and consequently commissioned again.
- It can be decommissioned

Existing Security Protocols for the IoT

- IP-based Security Solutions and their Complementary Protocols
  - DTLS
  - EAP
  - PANA
  - DCapBAC
  - Internet Key Exchange version 2 (IKEv2)
- Lightweight Cryptography Solutions (Block Ciphers)
  - CLEFIA
  - HECC
  - NtruEncrypt
- Hardware-assisted Security Solutions (Stream Ciphers)
- Privacy Protection Solutions
  - Elliptic Curve Cryptography

Difference

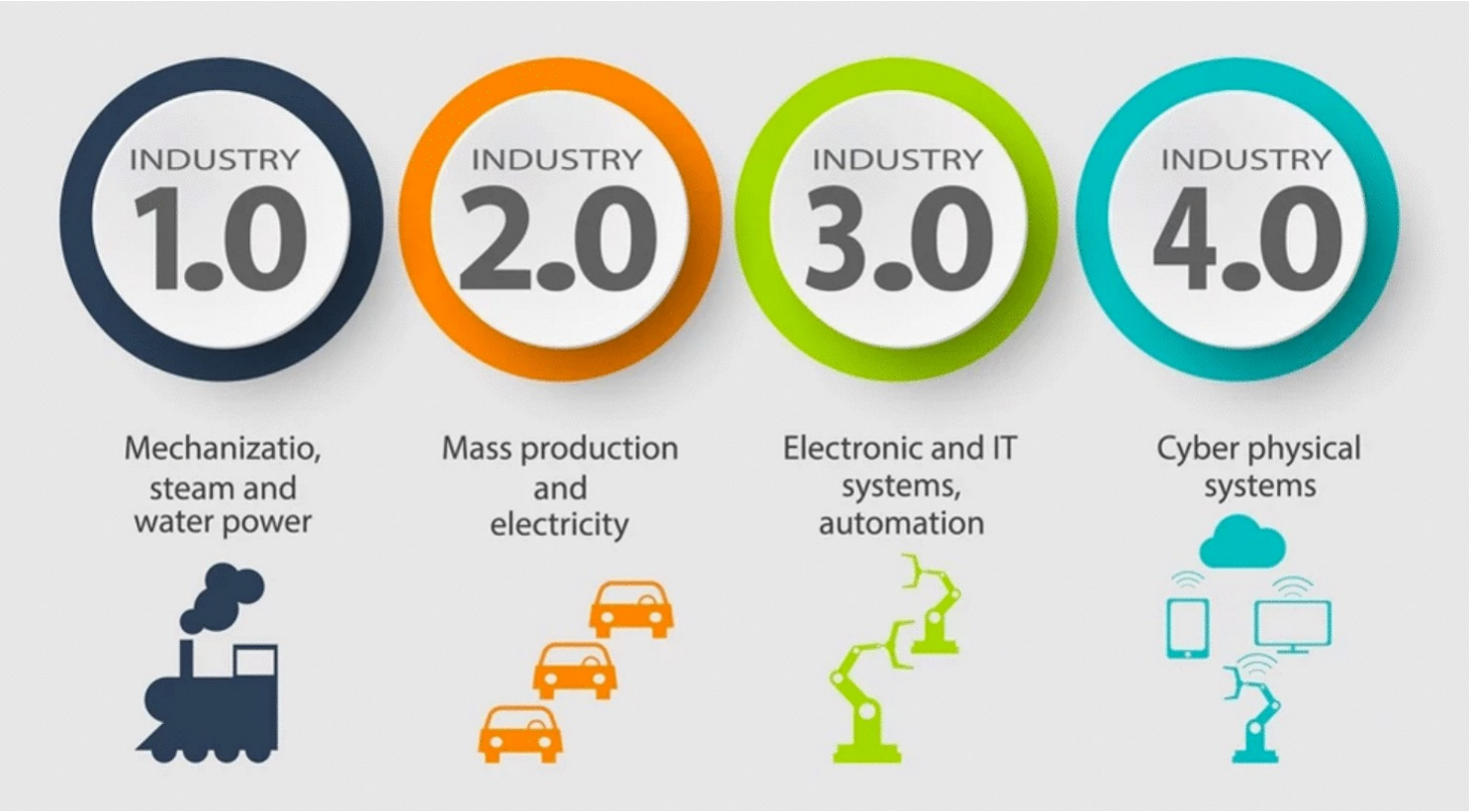
Stream Cipher	Block Cipher
Stream cipher operates on smaller Units of Plaintext	Block cipher operates on larger block of data
Faster than block cipher	Slower than Stream Cipher
Stream cipher processes the input element continuously producing output one element at a time	Block cipher processes the input one block of element at a time, producing an output block for each input block
Require less code	Requires more code
Only one time of key used.	Reuse of key is possible
Ex: One time pad	Ex: DES (Data Encryption Standard)
Application: SSL (secure connection on the web)	Application: Database, file encryption.
Stream cipher is more suitable for hardware implementation	Easier to implement in software.

Aforajayshahnirma.wordpress.com

Question?

PART II: Industry 4.0

Industry 4.0

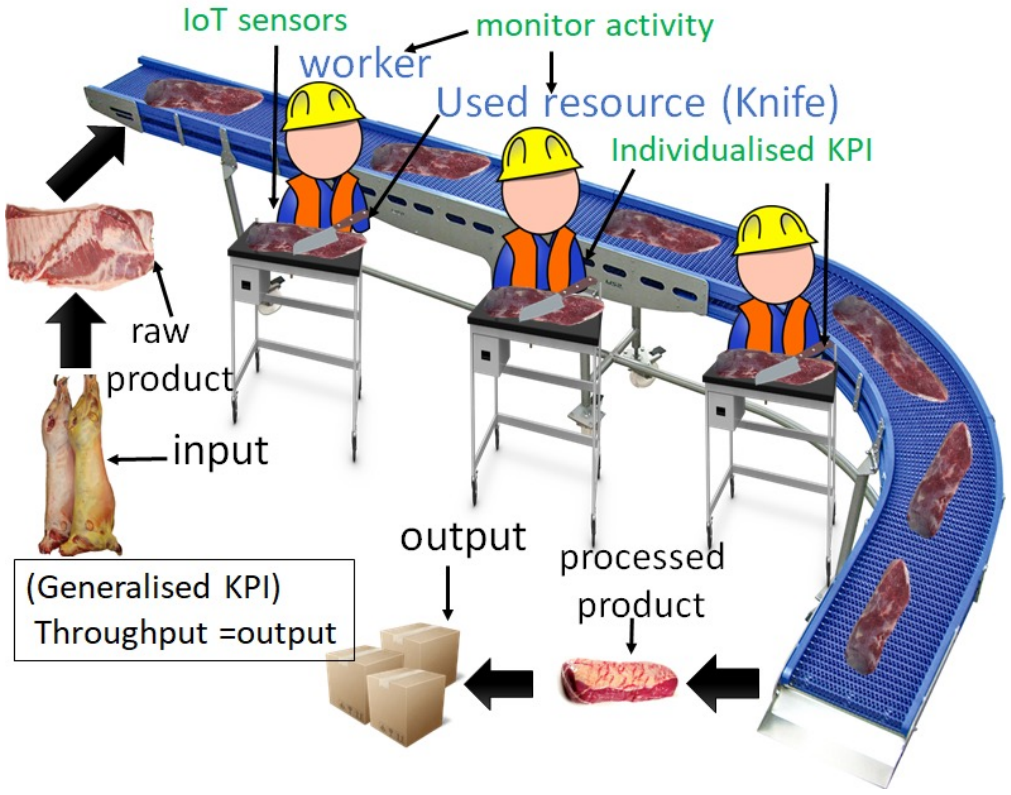

INDUSTRY 1.0
Mechanizatio, steam and water power
INDUSTRY 2.0
Mass production and electricity
INDUSTRY 3.0
Electronic and IT systems, automation
INDUSTRY 4.0
Cyber physical systems


Industry
4.0
Big Data
and Analytics
Cloud
Computing
Cibersecurity
Horizontal &
Vertical
Integration
Robotics
Augmented
Reality
Additive
Manufacturing
Simulation
Internet of
Things (IoT)

Industry 4.0 Solution for Assessing Worker Performance

- Identify one major industry opportunity and develop and trial an IIoT solution in a meat processing plants

Overview of a Meat Processing Plant



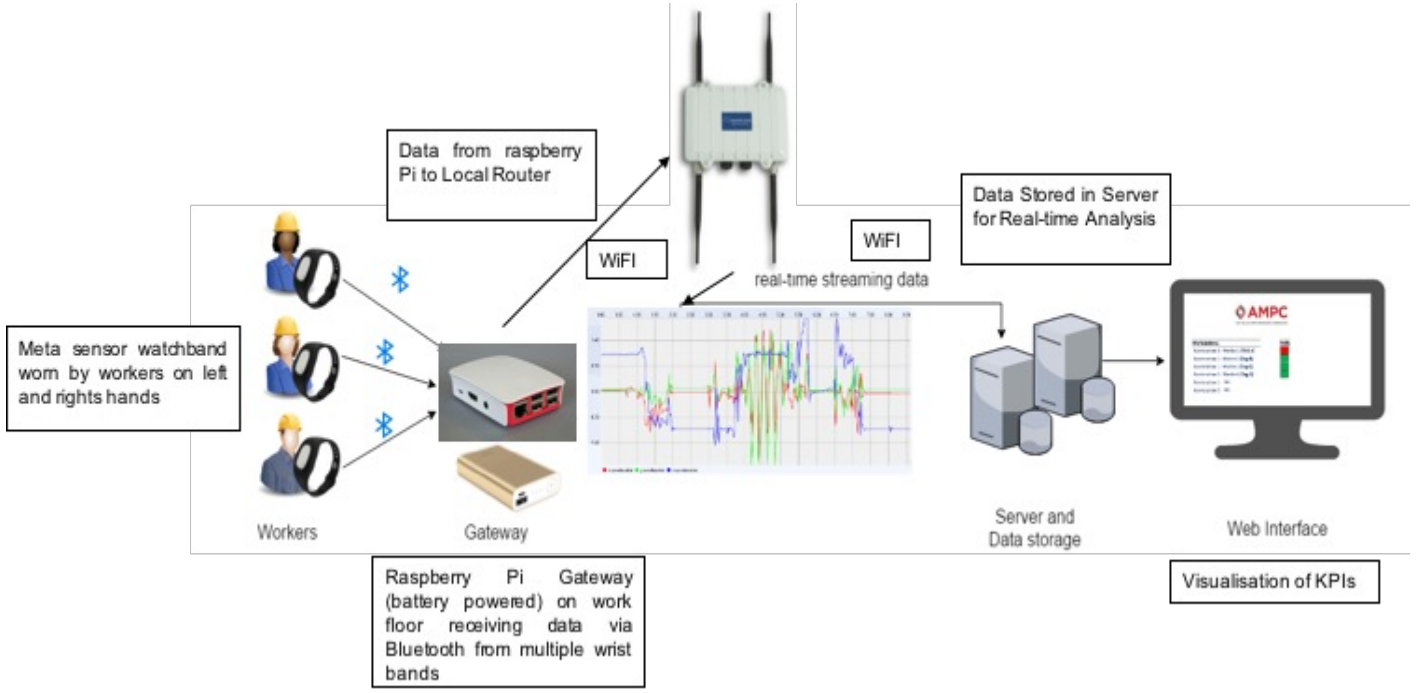
- Each worker works at a workstation where meat pieces come through a conveyor belt.
- A worker grabs and processes the next available piece of meat using a knife

IIoT Solution For Real-time fine grained KPI monitoring

“Real-time fine grained KPI monitoring IIoT solution to support decision making and in turn deliver productivity improvements and reduction in costs.”

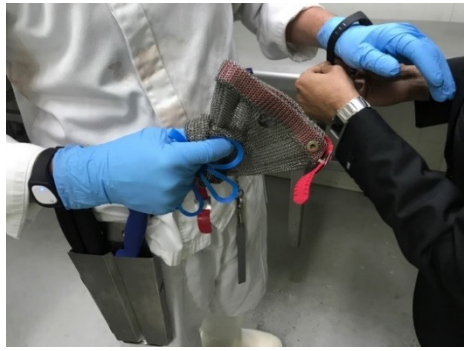
- **IIoT solution for real-time identification of plant worker**
- **IIoT solution for real-time computation of operator efficiency KPI using knife movements**

IIoT solution for real-time computation of operator efficiency KPI



- **Worker Activity**
  - **Productive movement**
  - **Idle**
  - **Aligning**

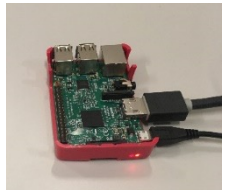
IN-PLANT TRIAL FOR REAL-TIME COMPUTATION OF OPERATOR EFFICENCY KPI

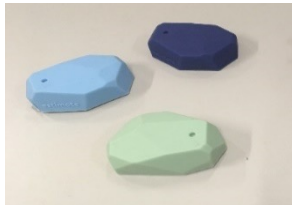




IoT sensors

- Raspberry Pi (Edge computers): For data collection from IoT sensors using BLE.
- Proximity sensor: For worker Identification and associate worker to a workstation for data collection.
- MetaWear Senor: Specific activity recognition from hand and knife movements





Trial design

- Data collected by deploying IoT solution in a one of the largest meat processing plants in Australia.
- Capture real production data from plant workers equipped with the hand acceleration and gyroscope sensors (on both hands)
- Data collected from 4 workers in a period of two working days and four 8-hour shifts.
- The data collection was conducted normal production shifts

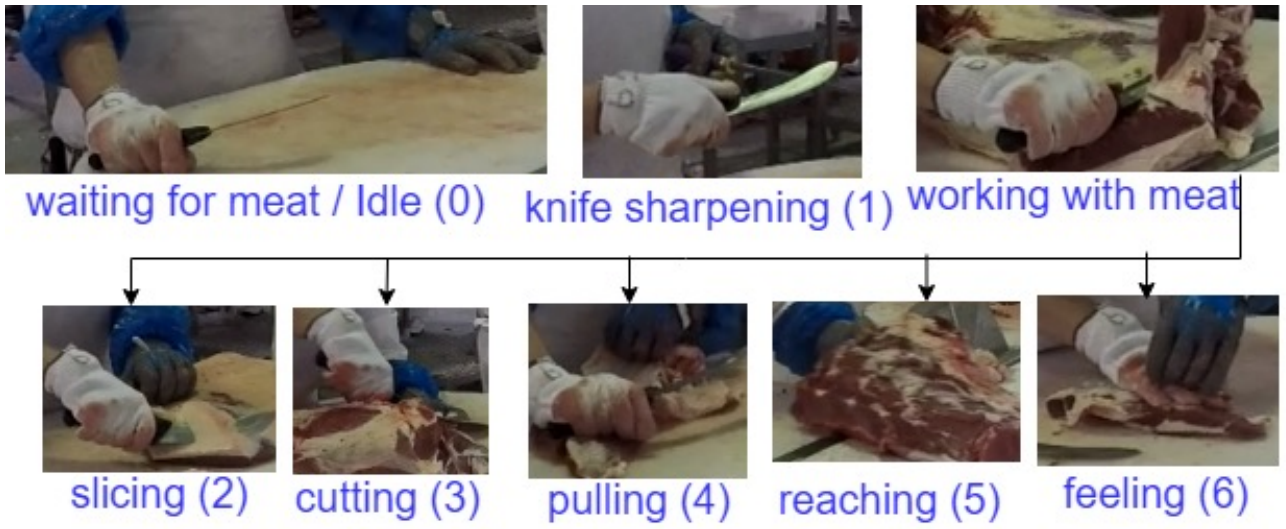
KEY FINDINGS

- Payback in as little as 0.4 years (further reduced where suitable IT infrastructure already exists)
- No negative impact on the plant operations
- No impact on health and safety.
- No interference to worker activity or loss of productivity
- Produced quantitative data to assess productivity and can lead to novel approaches for improving plant productivity (e.g. worker assignment).

More Interesting ML: Activities in Meat Processing

- Wait for next available meat (idle)
- Collecting meat from conveyor belt
- Removing fat from the meat
- Cutting large chunks of meat to suitable delivery-ready pieces.
- Return meat to the conveyor belt after processing
- Knife sharpening

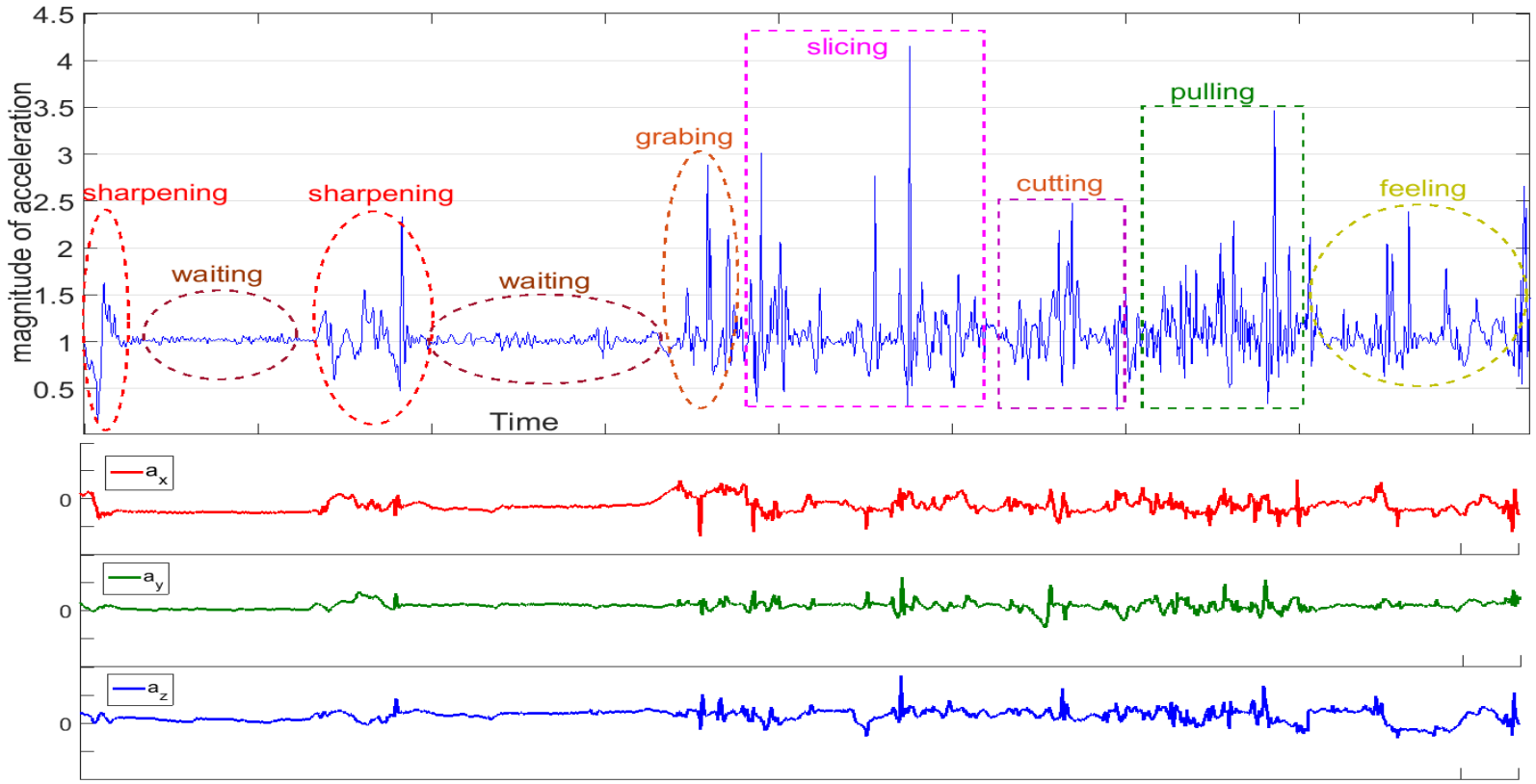
Annotation of activities



(a) A worker's different activities during meat cutting process

(b) Knife sharpness

Visual Representation of Data From Sensors



Feature extraction

- One second window for computing features from acceleration and gyroscope data.
- Extracted motion, orientation and rotation related features
- Total 43 features from acceleration and 32 features from gyroscope data were computed for each hand.
  - Features include statistics such as mean, standard deviations, number of peaks, mean magnitude, roll, pitch etc.
- Total 156 features from both hands

SVM models

- We used SVM with linear kernel as the learning algorithm
- SVMs normally provide better efficiency than other learning algorithms for such activity recognition problems.
  - Individualized SVM model - using features only from corresponding worker (used for one-to-one activity recognition)
  - Generalized SVM model - randomly combining data from multiple workers
  - Simple model - classes are labelled in three categories (labelled as 0 to 2) namely idle, sharpening and working.
  - Detailed model - Seven classes are used (labelled as 0 to 6) according to annotated activities

Learning

- Different models are generated using different subsets of features
  - All features from both hands - 156 features
  - All features only from right hand - 78 features
  - Only acceleration related features from both hands - 86 features
  - Only acceleration related features from only right hand - 43 features
- Right hand mostly used in activities.
- Two-third data is used for training and rest for validation.

Classification accuracy

Features from	No of features	Accuracy for 7 activity classes (%)					Accuracy for 3 activity classes (%)				
		w1	w2	w3	w4	combined	W1	w2	W3	w4	combined
both hands (acc + gyro)	156	70.8	62.97	65.1	64.09	65.87	91.2	92.32	90.12	87.42	89.26
Both hands (acc)	86	73	65.63	68.35	68.34	67.95	93.1	92.61	90.8	90.57	89.94
Right hand (acc)	43	69.8	65.15	61.17	63.86	63.08	90.6	90.62	88.66	86.87	88.56
Right hand (acc + gyro)	78	66.7	59.47	59.82	63.3	62.38	88.6	91.09	87.09	84.28	87.57

Bus Replacement Services for Rail Passenger Service Disruptions

Background

Aims and Objectives

- Address the data needs associated with bus replacement services to evaluate their utilisation
- Primary objectives

  Analyse technological options available to address the current data gap in the performance and patronage of replacement bus services

  Identify a preferred technology option or options to be trialled

  Undertake and assess the trial
- Secondary objectives

  Analyse “value-add” options that could be included in the trial such as:

  A real-time data feedback technology on replacement bus patronage

  The commercialising and partnering opportunities available from:

  i. Having a new data set on “disrupted” passengers;

  ii. That data potentially being available in real-time

Bus Passenger Counting Methods and Technologies

Vision-based commuter tracking and analytics

Floor-based sensing (Sensor Mat)

Mobile sensing

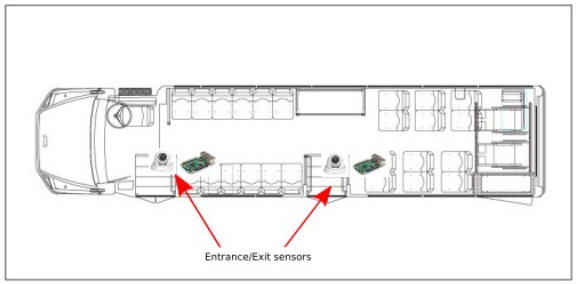
Proximity sensor-based solution

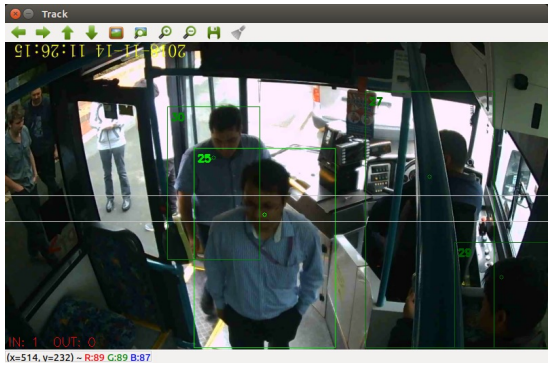
Vision-based commuter tracking and analytics

Solution Description

Visual sensors combined with computer vision and machine learning

On bus solution:





Camera options:

RGB

RGB+Depth

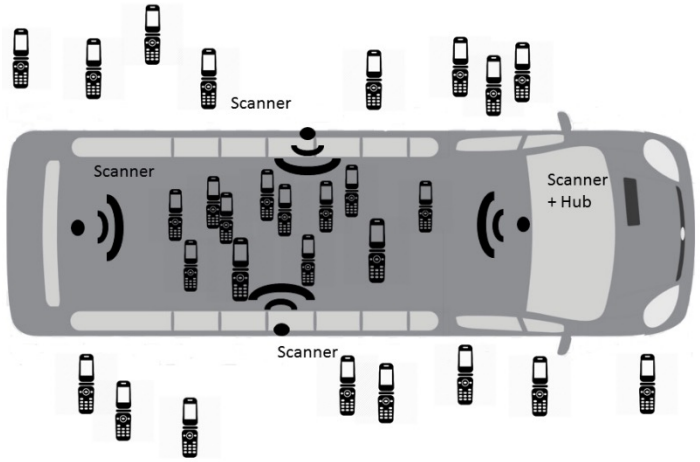
Long Wave IR (thermal)

Floor-based sensing (Sensor Mat)

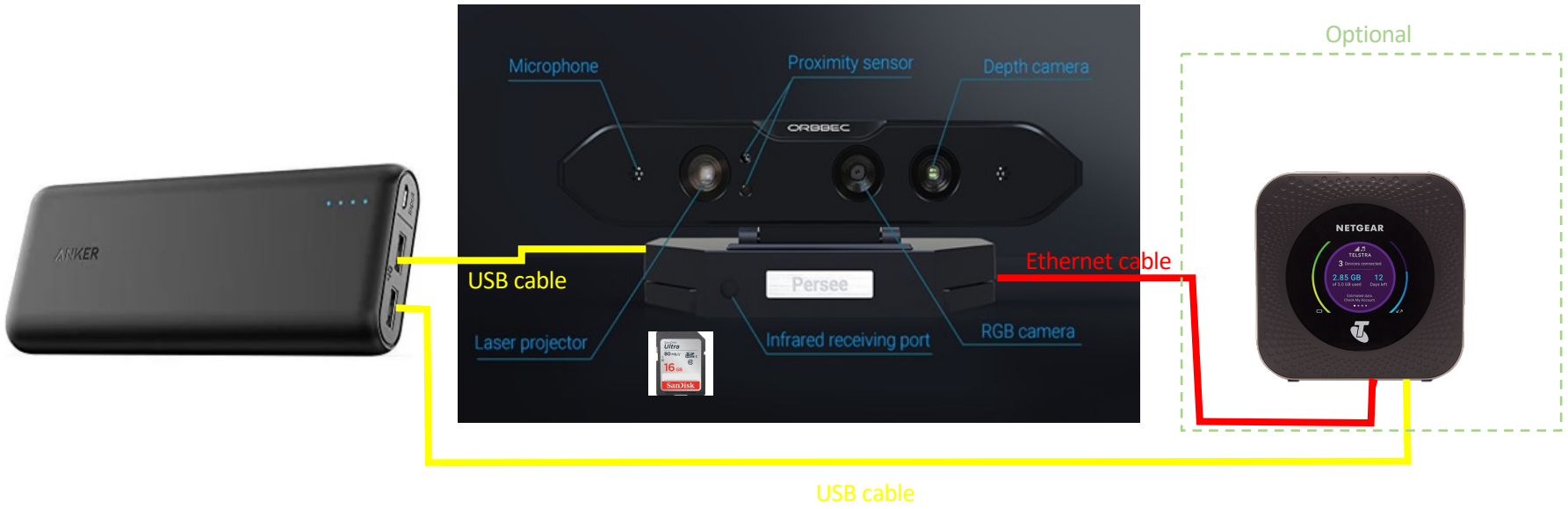
Solution Description

- Force activation (Piezo-resistive) sensing mat at the entrance of the bus
- Count the number of people boarding or alighting the bus as passengers step on them
- Built from rugged rubber-based material, would require minimum maintenance
- The data collected is discrete and no identifiable information of the passengers would be recorded, thus circumventing any privacy issues

Mobile Sensing



Proximity sensor-based solution



Ambient Assisted Living

Helps older people and those with a mild disability remain living at home when they might otherwise be unable to do so
Enable the above via a non-intrusive approach
Provide for unobtrusive assistance and supervision (when required)

Acknowledgement
Thanks to: HalleyAssist
https://halleyassist.com/

A/Prof. Philip Branch

Approach

- HalleyAssist® - **LEARN. SENSE. ASSIST.**
  - Assisted Aged Care technology with easy-to-use interface
  - Non-intrusive home monitoring and support system
  - Monitoring of movement, prolonged inactivity, and sleep pattern
  - Alerts for security breaches and anomalies in the daily routine pattern

Source: HalleyAssist 2019

HalleyAssist

SWINBURNE UNIVERSITY OF TECHNOLOGY

Central Hub

Speakers

Latch Sensor

Motion Sensor

Night Light

Source: HalleyAssist 2019

Source: HalleyAssist 2019

IoT sensors

- A central hub (raspberry pi)
- IoT Sensors located throughout the home connected wirelessly to the hub
  - External door and window sensors to detect in-house mobility
  - Motion and latch sensors that detect movement
  - A speaker that gives reminders for taking medication and fluid intake

Hub

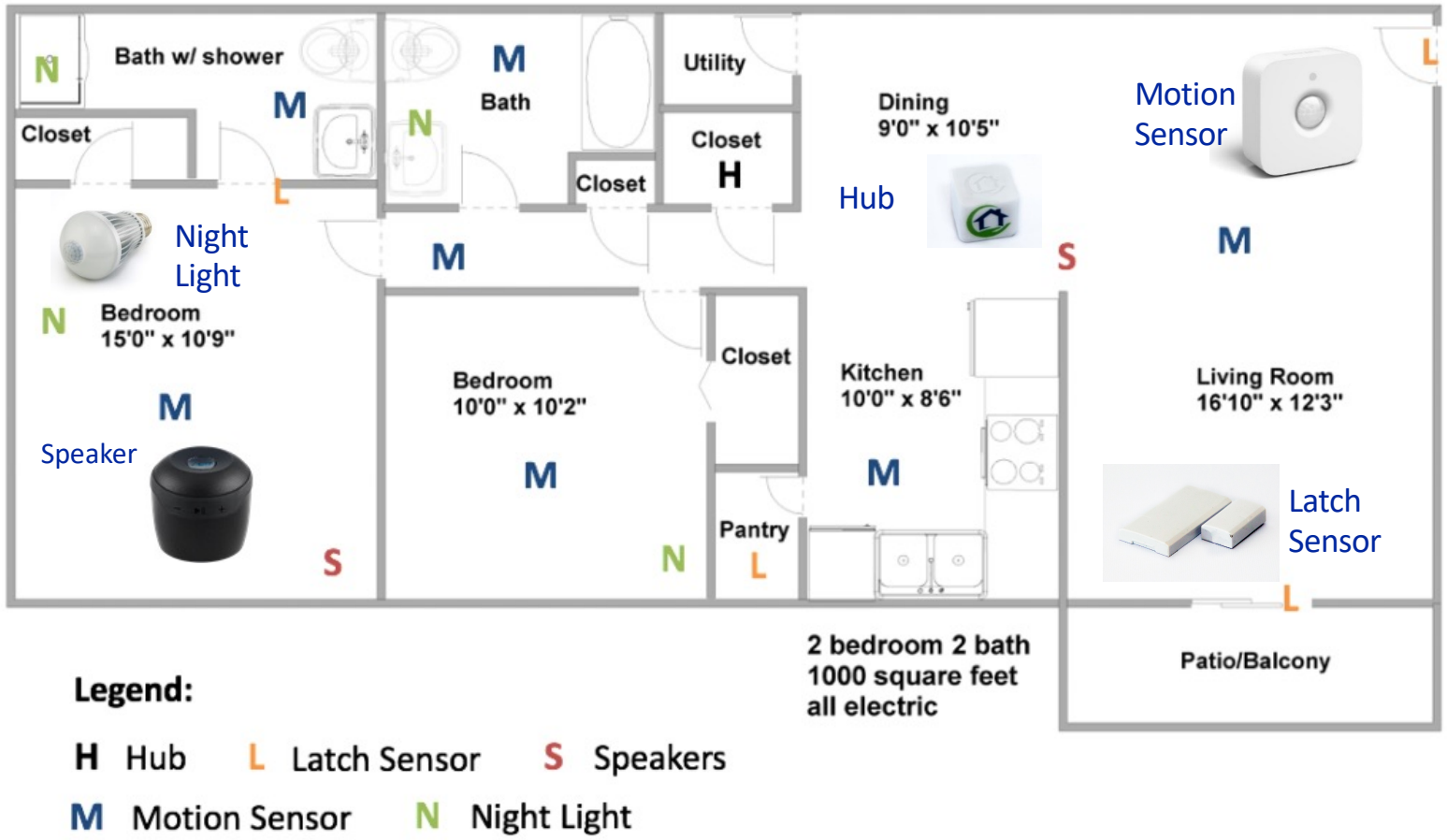
Speaker

Latch sensor

Motion sensor

Source: HalleyAssist 2019

SAMPLE HARDWARE LAYOUT



Source: HalleyAssist 2019

Anomaly detection techniques

- Statistical models learned from sensor data
  - statistics such as mean, standard deviation of individual sensor events or group of sensor events in various time periods
- Markov chain model learned from event sequences
  - based on the probabilities of transitions between a pair of sensors or sensor groups
- Recurrence model
  - using the sequence of sensor activations to understand recurrence patterns in a particular time window
- User-defined rule-based system to detect anomaly

Privacy and security

- All data is stored locally within the central hub
- Processing is also done locally
- Reports are transmitted securely via a messaging service or can be extracted via an App
- All communication is encrypted
- There are NO image or video recordings made

Question?