TNE30009/TNE80009

Case Study

1. Introduction

In this case study you will carry out a risk assessment, formulate policies and outline how to they can be implemented for the Ambient Assisted Living System (AALS) described in the attached paper.

This is an individual assignment. It is to be your work only. You can consult with others but do not share completed or partially completed work. Doing so is potentially enabling plagiarism

The report is due at the end of the second week of the exam period.

The system is an Ambient Assisted Living system for aged and disabled care. The attached paper describes the system.

2. Project requirements

You are required to:

1. Identify the major security risks associated with the system and perform a risk analysis. The number of major risks is to be four. You must use the Delphi method discussed in class to rank the risks.
2. Write security policies that address the risks identified in the risk analysis.
3. Specify how each policy will be implemented. Explain what technologies and procedures will be deployed and how they will be used. Briefly outline the capabilities of the technologies to be implemented.

In preparing this work you will need to make a number of assumptions regarding the organisation. You are welcome to check your assumptions with the convenor. When you prepare your work you will need to document your assumptions.

3. Report

You can choose what format you use for the report but IEEE is preferred. Sections are to be numbered. Diagrams are to be labelled. Any references used are to be listed in a Reference section.

The report is to be no more than 15 pages. Below is the rubric for assessment. The report will be graded as Pass, Credit, Distinction, High Distinction or Not passed. Marking criteria are listed below. Referencing is to be IEEE or Author-Date.

The report is to have the following sections:

1. Title including author name and email.
2. Executive summary.

   A short summary of the report including recommendations.
3. Introduction.

   Overview of the system and security issues it and similar systems face.
4. Risk analysis.

TNE30009/TNE80009

Case Study

Identify and rank the security threats faced by the organisation using the method discussed in class.

This is to include an identification of the relevant organisation's assets. Threats faced by the organisation are to specify what assets are at risk.

5. Policy Formulation

   This is to consist of policy statements that address the threats identified in the previous section. Four of the most urgent threats are to be addressed. Policy statements are high level statements of security goals.

6. Implementation of security programme.

   Specify how each policy will be implemented. Specify what technologies are to be used and where and how they will be deployed. Outline any manual controls to be adopted.

7. Summary including recommendations.

   This will consist of a bullet point list of recommendations.

8. References

   Use IEEE or Author-Date.

In the above sections you MUST DOCUMENT ANY ASSUMPTIONS YOU MAKE.

4. Assessment

Assessment will be based on how thoroughly and clearly the risk analysis, the security programme and the implementation are described. The following rubric will be used:

	Pass	Credit	Distinction	High Distinction
Format (10%)	• The submitted report is formatted using the IEEE Conference template • All figures/tables are appropriately labelled • The submitted report is in PDF format	All Pass requirements plus: • PDF fonts compiled into document • Images/figures in vector format	All Credit requirements plus: • Formatting is clean with no words/tables wrapping beyond the edge of a column/page	All Distinction requirements
Structure (25%)	• The submitted report is properly structured with Executive Summary, Introduction, Risk Analysis, Policy Formulation, Implementation Outline and Conclusion • The report is complete but some sections are lacking detail • A reference list is provided	All Pass requirements plus: • Clear use of sub-sections as required to clearly delineate different aspects of the findings • The reference list is professionally structured and complete	All Credit requirements plus: • Suitable references have been located and used for all claims made by the student	All Distinction requirements

TNE30009/TNE80009

Case Study

Analysis (50%)	• Four risks have been identified based on assets of the system or assets related to the system. • The risks have been ranked. • Policies to address the risks have been formulated. • Technologies suitable for implementing the policies have been identified.	All Pass requirements plus: • The ranking of the risks has been justified. • An outline of how the policies address the risks is included. • How the technologies implement the policies has been explained.	All Credit requirements plus: • A discussion of the risk environment with a justification of the choice of risks and risk rankings is included. • Clear evidence is presented that all risks are addressed by the policies and an explanation of how they do so is included. • An evaluation of different technologies that can implement the policies is included.	All Distinction requirements plus: • An in-depth evaluation of the risk environment with citing of relevant literature justifying the choice of risks and risk rankings is included. • A thorough explanation of how the policies address the risks is included. • A detailed discussion of the relative strengths and weaknesses of different technologies that can be used to implement the policies with citing of relevant literature and a recommendation of an appropriate technology is included.
Language (15%)	Basic language and grammatical skills	All Pass requirements plus: • Good grammatical structure and flow of argument	All Credit requirements plus: • A document suitable for reading by a professional audience	All Distinction requirements plus: • An excellent report suitable for reading by an academic audience

HalleyAssist: A Personalised Internet of Things Technology to Assist the Elderly in Daily Living

Abdur Rahim Mohammad Forkan[*,a], Philip Branch[*,a], Prem Prakash Jayaraman[a], Andre Ferretto[b]
[a]School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC, Australia
[b]SP Tech Solutions, Melbourne, VIC, Australia
{ fforkan, pbranch, pjayaraman}@swin.edu.au, andre@ferretto.com.au

Abstract

Ambient Assisted Living (AAL) research has received extensive attention in recent years. AAL applications combine aspects of Internet of Things (IoT), smart platform design and machine learning to produce an intelligent system. In this paper we describe a personalised IoT-based AAL system that enables an independent and safe life for elderly people within their own home via real-time monitoring and intervention. The system, HalleyAssist underpinned by smart home automation functions includes a novel approach for monitoring the wellbeing and detecting abnormal changes in behavioral patterns of an elderly person. The significance of the approach is in the use of machine learning models to automatically learn normal behavioral pattern for the person from IoT sensor data and using the models derived to detect significant changes in behavioral pattern should they occur. The architecture and developed proof of concept of the proposed system is presented along with discussion of how privacy and security concerns are addressed. We also report on outcomes of real-world in-home trials of an early version of the system where it was installed in four older people's home for a period of six weeks. The response from the older people to the deployed system was very positive. Finally, the paper presents a discussion and an analysis of the results using the data collected during the in-home trials.

1. Introduction

As they age, most older people would prefer to live in their original home for as long as possible rather than move to an Aged Care Facility. However when children live far away from their aged parents, frailty, living alone after the death of a partner, the risk of falls, and perhaps the early stages of dementia [1] usually make a move from the family home to an Aged Care Facility very likely. Nevertheless, many older people could remain in their home longer than might otherwise be possible if they had some modest form of support and monitoring.

The potential of technology to fulfil both these roles has been recognised for some time. Some adult children have taken to asking their aged parents to wear fitness monitors [2] in order to ensure their older parent is well. Regrettably, it is also the case that older people generally dislike wearing technology solely for the purpose of being monitored and, particularly if suffering early stages of dementia, may forget to wear such items. Consequently, attention has turned to ambient systems for both support, monitoring and intervention. Ambient Assisted Living (AAL) is smart home technology to support elderly and disabled people at home. The goal of AAL is to secure the health of its users so they can live independently. It simplifies the activities of daily living with home automation using IoT sensors and monitors and cares for the user with intelligent solutions.

Smart home automation, achieved via advances in IoT such as lighting triggered by motion sensors [3], medication and fluid intake reminders, and security systems such as door and window closing sensors and latches can all make living alone without supervision quite feasible [4]. IoT can not only assist with home automation [4] but can also provide unobtrusive monitoring [5] of person's behavioral patterns. For example, motion sensors can indicate if the older person has moved about their home during the day, bed sensors can indicate if the person has been obtaining enough sleep, door sensors on a refrigerator can indicate if the person is feeding themselves and tap sensors can indicate if they are drinking sufficient water.

Moreover, the data stemming from such IoT devices/sensors can also be used to provide an indication as to whether behavior has changed in a manner that might be indicative of a more serious problem. For example, an increase in the number of visits to the bathroom might indicate a urinary tract infection. An increase in the amount of water intake might indicate issues related with diabetes. With prior knowledge about the elderly person coupled with aforementioned intelligence using IoT sensor data, a smart system can

URI: https://hdl.handle.net/10125/59857
ISBN: 978-0-9981331-2-6

identify when a carer (health professionals, caregivers, family members and emergency services) should be contacted automatically.

In this paper, we propose, develop and implement HalleyAssist, a smart IoT-based solution for monitoring the wellbeing and detecting abnormal changes in the behavioral pattern of an elderly person, enabling an independent and safe lifestyle as long as possible. HalleyAssist also includes a combination of smart home automation and monitoring services including security, motion detection-based lighting, medication and hydration reminders. In particular, this paper makes the following contributions:

- A novel anomaly detection approach that is highly flexible and configurable and can be based on a single IoT sensor events or group of IoT sensors events (aggregated, pairwise and/or sequence). The proposed anomaly detection approach uses machine learning models to automatically learn normal behavioral patterns for the person unobtrusively and, using this model to detect significant changes in behavioral pattern should they occur.
- A proof-of-concept (PoC) implementation of the proposed system that addresses the issue of privacy and security by doing all processing locally i.e. individualised analysis of all collected data are performed within a central hub located on the premises. HalleyAssist is built completely from off-the-shelf hardware and software.
- Outcomes of real-world in-home trials of the PoC system in four older people's home for a period of six weeks.

The rest of the paper is organised as follows. Section 2 reviews the background of IoT-base smart AAL systems and describes state-of-art approaches for behavioral monitoring and anomaly detection. Section 3 presents the architecture of the system. Section 4 demonstrates the techniques we have used for learning patterns and detection of anomalies. Section 5 describes the Proof-of-concept (PoC) implementation of HalleyAssist. Section 6 describes the results and findings of the in-home trials. Finally, Section 7 concludes the paper and describes potential future work.

2. Background and Related Work

Smart home technologies to unobtrusively monitor older adults has been described in literature [6, 7]. The integration of multiple technology domains such as wireless sensor networks, IoT, data mining and machine learning techniques have made assisted living systems [8, 7] a feasible solution for remote monitoring of elderly people.

In traditional systems daily behaviour of older adults is assessed through using self-report and questionnaire in an app or a web portal [9]. However, such self-assessment can contain biased answers and not capture real-time behavioural changes. Another approach is to use fitness trackers such as a Fitbit or wearable sensors to monitor basic vital signs [2]. Such fitness trackers usually push data to the cloud to be accessed anywhere by suitably authorised people and allows children or carer of an adult person to monitor his/her activities. However, elderly people generally dislike being obliged to wear monitoring devices or if they are suffering from mild dementia may not remember to wear them [10].

Therefore, a better approach is to observe the daily behaviour of each individual using a smart IoT-based technology that allows monitoring in a less intrusive manner. An AAL system based on IoT devices/sensors provide the effective infrastructure to continuously monitor daily behaviour of older adults in an unobtrusive way [11]. It gathers real-time data continuously and therefore can rapidly detect any changes in pattern by analysing historical data. A proper data analytics over the captured data from sensors can provide a better view of daily behaviour in real-world scenario than self reports.

Statistical analysis and machine learning are widely-used to model behavioural pattern and activities of the elderly user in smart-home or AAL environment using various IoT sensors [3, 11, 4, 12, 13]. In addition, some research focus has been on detecting anomalies in daily activities [1, 14, 11, 15, 16] for such a setup. The statistical analysis described in [17] suggests that for a Gaussian distribution, a threshold of three standard deviations from a normal pattern can be considered an anomaly. Data mining techniques such as Hidden Markov model [16], Support Vector Machine (SVM) [18] are also used to detect anomalies in sensor events in home settings. Other approaches such as Recurrence Quantification Analysis (RQA) [19] have been used for anomaly detection in different application domains. We have used all these techniques in our implementation. Most of these approaches use limited amount of real-world data for modelling pattern and do not have any flexible support tool for adapting behaviour based on observed changes. In HalleyAssist we have long-term real-world data collected from our testbeds and we provide a mechanism to configure key parameters for anomaly detection as well as configuring suitable number of observation periods.

3. HalleyAssist: System Architecture

The architecture of HalleyAssist is illustrated in Figure 1. The system consists of five main components: the Ambient Assisted Living (AAL) subsystem, Learning module, Anomaly detection module, Caregiver module and Reporting module.

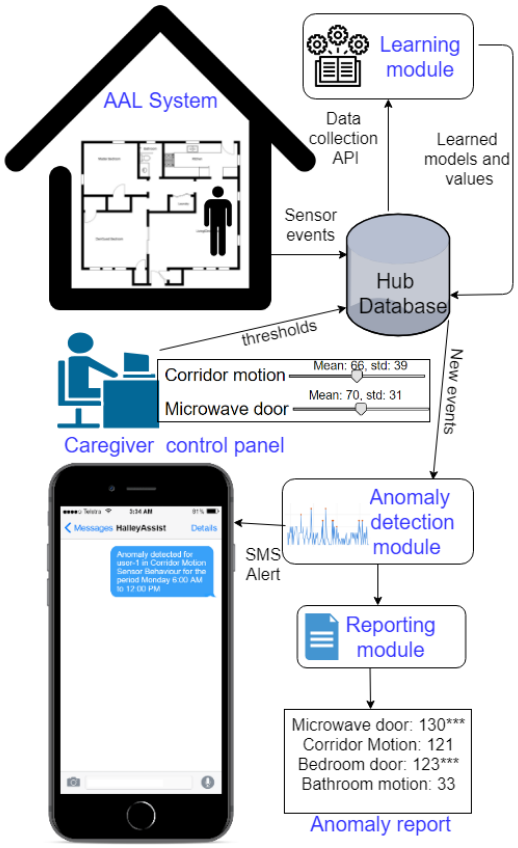

Figure 1. The architecture of HalleyAssist System

The system is flexible, open, customisable and extensible. Any new IoT sensor can be installed in the system very easily. For example, in one of the trials we have successfully installed a bed sensor which is capable of detecting sleep and wake up times, sleep duration, pulse rate and respiratory rate of the user. This data can be used for health monitoring purposes.

A detailed description of the main components of the system is provided below.

3.1. AAL Subsystem

HalleyAssist AAL subsystem consists of multiple IoT sensors and actuators connected wirelessly to a central hub located within the home. The system is designed for a single-resident home. The setup of the AAL system is fully customised and personalised according to the requirements of the elderly person, the layout of the home, and the number of sensors that they want to deploy. The hub monitors and stores events triggered by all connected sensors along with time-stamp values inside an internal database. To use this stored data for analysis by the other components we developed RESTful APIs (Data collection APIs). An external module can use a GET request to collect historical sensor events with filtered queries. The hub also carries out home automation tasks (e.g. control light sensor to turn light on/off, assist people through speaker).

3.2. Learning module

This module collects historical sensor events from the AAL system using REST APIs and performs required filtering to clean the data (e.g. eliminate noise, remove duplicate events, extract active states of sensor events). A configurable time window (e.g. two weeks, a month) is used as the observation period to understand the usual patterns of different sensors in various time periods (e.g. Monday afternoon, Tuesday night, weekend, week) for a specific user. The statistical behaviour of each sensor or a group of sensors is computed and also stored in the hub's database. The learning module is adaptive and continuously updates upon collecting new data. We have developed and implemented three learning models inside the learning module of HalleyAssist to capture the normal pattern from observation window and later used in anomaly detection. They are as follows.

- A Statistical model based on statistics such as mean, standard deviation of individual sensor events or group of sensor events in various time periods [17].
- A Markov model [20] based on the probabilities of transitions between a pair of sensors or sensor groups.
- A recurrence model [21] using the sequence of sensor activations to understand recurrence patterns in a particular time window.

3.3. Anomaly detection module

Once the system is trained with various learning models by the learning module, the role of the anomaly detection module is to collect new daily data from AAL system and analyse it to identify deviations from normal behavior. Decisions as to what is anomalous behaviour is based on statistics of the learned parameters. When

behaviour, as reflected by sensor activation, changes significantly from the learned pattern by the learning models then it indicates anomalies that may correspond to a change in the health of the person. In the simplest case these unusual patterns of behaviour are reflected as unusually low or high numbers of sensor activations. For example, if the usual number of visits to the kitchen is 10 per day and 2 are recorded, it may be an indication that the elderly person is not drinking enough water or eating meals. The other models detect anomalies in similar ways.

3.4. Caregiver control panel

The control panel provides a user interface (UI) to make the training periods for learning and statistical threshold values of anomaly detection (e.g. number of standard deviation from the mean) configurable and adjustable. An option for creating groups from a list of sensors is also available. This control panel can be used by a supervisor of the system or a carer. The carer can also set the frequency of report generation of anomalies using the interface. The generated statistics about the normal patterns by the learning model make recommendations for suitable configuration. This flexibility in design provides a carer with greater control to configure various parameters and enables more accurate identification of unusual sensor event which corresponds to unusual behaviour of the elderly person.

3.5. Reporting module

The reporting module generates regular reports at a preferred frequency (e.g. every 12 hours). If any anomalous pattern is observed by the anomaly detection module according to the configured parameters in the control panel then the reporting module flags those values in the generated report. The report displays what value is observed and what value was expected. HalleyAssist is connected to an SMS gateway. If activated in the control panel, the reporting module sends an alert to the caregiver regarding the observed anomaly. These notifications are only sent in the event of the system detecting unusual behaviour that might indicate an illness of the elderly person or a condition that the carer should be made aware of.

4. Anomaly Detection Approach

The *Anomaly detection module* of HalleyAssist determines whether a pattern of behaviour is or is not usual is by comparing with historical data that was captured during a training period by the *Learning module*. During this training period the system records the usual number and patterns of activations expected from a sensor or group of sensors. After the training period, significantly large deviations from the historically observed mean computed during the training period are flagged as anomalies. We have implemented and evaluated three different techniques for detecting and reporting anomalies in sensor events generated by the HalleyAssist system. These techniques along with our defined notations are described formally as follows.

4.1. Sensors and Groups

Let, n be the number of sensors, $S_1, S_2, ..., S_n$ are deployed in HalleyAssist system. In HalleyAssist there is a flexibility to create m number of groups from n sensors, $G_1, G_2, ..., G_m$ where each group $G_i = \{S_{a1}, S_{a2}, ...\}$ can consists one or more sensors. This flexibility allows observational aggregated behaviour from a list of sensors. For example, a particular room or group of rooms can be aggregated. A carer may like to group all motion and door sensors installed in a bedroom to observe anomaly based on number of activations obtained from that group. Here $m = n$ if each group has only one sensor.

4.2. Sensor Events

A door or motion sensor event is represented by three parameters $e = (t, s, a)$ where t is the time of occurrence of the event, s is sensor id in the system and a is a boolean value which represents active state of sensor. $a = 1$ when s is triggered at time t, otherwise 0. Here we are only interested in events when a is 1. Let, $E(\theta)\{e_1, e_2, ...e_p\}$ represents the sequence of events that occurred within a particular time period, θ where each $e_i = (t_i, s_i, 1)$. We only use the active state of sensors for analysis.

4.3. Observation and Training Window

A carer may be interested in seeing anomalies for a specific observation period within a day (e.g. 6 AM to 6 PM on Monday). $O(t_s, t_e)$ is an observation window that starts at time t_s and ends at time t_e. The maximum value of $O(t_s, t_e)$ can be 24 hours which means a complete day and minimum can be 1 hour. Let, k be the number of observation windows $O_1, O_2, ...O_k$ configured in the system. $T(d_s, d_e)$ is training window from date d_s to d_e. T can be up to a month based on availability of data but should be at least one week. T is used to extract statistics describing the usual behaviour of number of activations each sensor group G_i under each observation window O_j. We use the

notation $E(T)\{(G_i, O_j)\}$ to describe all active sensor events $\{e_i = (t_i, s_i, 1)\}$ of sensors in group G_i under observation window O_j for training window T. Let, $R(G_i, O_j)$ is the reporting window for group G_i that matches for observation window O_j.

4.4. Statistical Values

If $D_k = \{d_1, d_2, ...d_q\}$ is the number of days in training window T that match for observation window O_j then we can measure the Gaussian distribution, $\mu_{ij}(T), \sigma_{ij}(T)$ [17] of events in each group G_i (or each sensor S_i) for each observation window O_j for training window T using data in $E(T)\{(G_i, O_j)\}$ where $\mu_{ij}(T)$ and $\sigma_{ij}(T)$ is the mean and standard deviation of the distribution respectively.

4.5. Anomalies based on Mean Occurrence

This type of anomaly is based on statistical analysis involving a single or a group of sensors. The statistics calculated on reporting window R and compared with the statistics generated during the learning period T. If $\Omega_{ij}(R)$ is the total value computed by taking the sum of active events of group G_i where R matches with observation window O_j, the anomaly for sensor S_i or group G_i occurs in R if $\Omega_{ij}(R) \geq \mu_{ij}(T) + \sigma_{ij}(T) \times \delta_{ij}(T)$ or $\Omega_{ij}(R) \leq \mu_{ij}(T) + \sigma_{ij}(T) \times \delta_{ij}(T)$ where $\delta_{ij}(T)$ is a configured threshold value in the control panel of *number of standard deviation* for the pair (S_i, O_j) or (G_i, O_j) in training window T.

4.6. Anomalies based on Mean Transitions

Such anomalies are computed by generating a Markov model [20] between a pair of groups (G_x, G_y) or Sensors (S_x, S_y). If m is the number of groups then a square matrix $M(O_j) = \{m_{xy}\}$ of dimension $m \times m$ is constructed for observation window O_j. Where m_{xy} is the total number of transitions of active states from sensors in group G_x to sensors in group G_y during observation O_j. Transitions between sensors within the same group are considered one activate state and so $m_{xy} = 0$ when $x = y$. Then for the training window T the mean $\{\mu_{xy}(O_j, T)\}$ and standard deviation $\{\sigma_{xy}(O_j, T)\}$ matrix is computed for O_j. The anomaly between a pair of groups (G_x, G_y) for reporting window R is then computed in the same way using a configurable threshold value $\delta_{xy}(O_j)$ of *number of standard deviation*, σ in the control panel.

4.7. Anomalies based on Recurrence Pattern

Let, $g_1, g_2, ..., g_q$ be a sequence of active states from k groups/sensors. If a recurrence pattern is observed for observation O_j within training period T then a deviation from this pattern is considered as anomaly. The deviation is measured by applying Recurrence Quantification Analysis (RQA) [21] on the group sequence $R\{g1, g2, ..., g_q\}$ of reporting window R and observing RQA measures such as recurrence rate (RR), determinism (DET), average line length (L) and entropy(ENTR) [21].

5. HalleyAssist: Proof-of-concept Implementation

As described in Section 3 the AAL subsystem of HalleyAssist contains multiple IoT sensors connected to a central hub. In this section, we describe a proof-of-concept (PoC) implementation of HalleyAssist including sensors and development technologies.

An example of sensor deployment along with the IoT sensors/devices used in our PoC implementation is shown in Figure 2. We have only used IoT sensors that embed into the home in our system design. The system can be completely customised and layout can be different to suit each individual user/home. It is configured according to the preference of the user and layout of the home. The IoT sensors/devices deployed in HalleyAssist are off-the-shelf and low cost. They are described as follows:

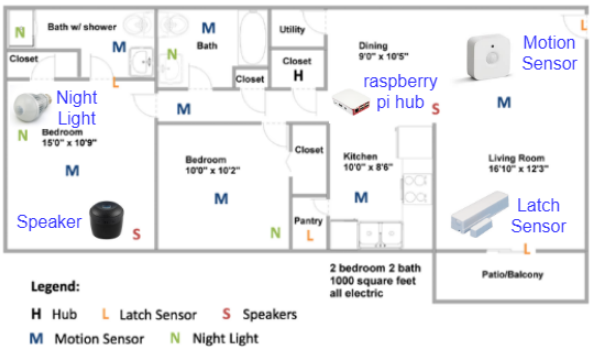

Figure 2. An example of a typical deployment of sensors in a HalleyAssist System

- Motion sensors (M) for sensing movements by detecting close proximity of the user near the sensor. Motion sensors are placed in the most commonly used locations of the house (e.g. Corridor To Bedroom Motion, Kitchen To Front Motion, Bedside Motion). The active value in a

motion sensor indicates the presence of user in that particular area.

- Latch sensors (L) are normally placed on doors and are used to detect in-house mobility of the user from one location to another (e.g. Entry And Bedroom Door, Bedroom And Bathroom Door). Such sensors are also used to detect appliances usage and behaviour for medication intake (e.g. Microwave door, Laundry door, Medicine cabinet door). The open value in latch sensors indicate a transition of user from one room to another room or use of appliances.
- Night Light sensors (N) are used for energy saving. Lights are turned on/off based on the presence of the user.
- A speaker (S) to provide reminders for taking medication and fluid intake.
- A powerful central hub (H) which is a raspberry pi3 running linux operating system. The central hub maintains the repository of sensors placed in the house, communicates with those sensors using zigbee protocol and is responsible for collecting and storing all sensor events in the database installed in the hub. The hub is also responsible for continuous monitoring and detection of anomalies.

The battery level of these sensors can be monitored using the *Control panel*. The collected data from users is highly secure as it remains within the hub's database and is not stored in any external server or cloud. For *Control panel* we developed a flexible web-based front-end interface that can be accessed using computer or hand-held devices where a carer can view and easily interpret the collected data and configure parameters of anomaly detection. A screen-shot of control panel UI for creating groups and configuring threshold values of anomaly detection is shown in Figure 3.

HalleyAssist has been implemented using multiple software development technologies. The tools and technologies used to develop various modules of the PoC implementation are listed in Table 1.

6. Trials and Results

We deployed an early version of our system in four homes in Geelong, Australia to test and validate the efficacy of our solution. All participants in the study granted consent as part of human ethics approval. More than 20 sensors (latch and motion) were installed in each home along with a separate hub. The system was

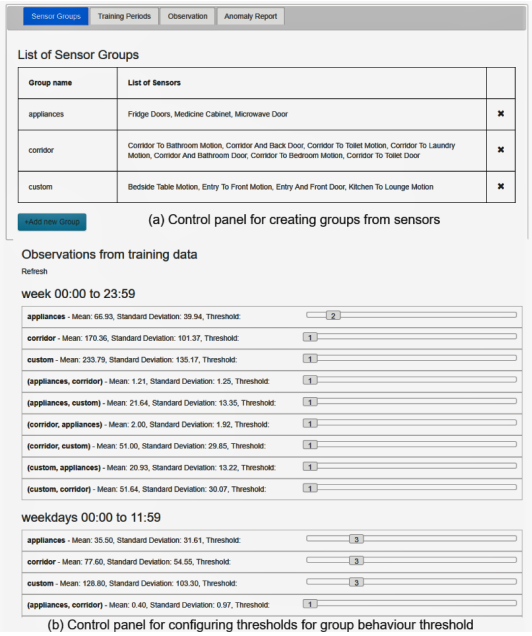

Figure 3. A screen-shot of control panel UI

Table 1. Technologies used to implement the PoC of HalleyAssist

Component	technology
Hub SDK	NodeJS
Hub Database	PostgreSQL
REST APIs of hub	Ruby
Communication protocol	NodeJS
Learning models, Anomaly detection and Reporting	Python2
Storing learned models	SQLite
Control Panel UI	HTML, JavaScript

left unattended and the duration of data collection was four to six weeks. In this section, we analyse the data collected during the trial and how we utilised this data to validate the proposed novel anomaly detection approach incorporated in HalleyAssist.

6.1. Trial description

All trials were setup in single-resident home. We named them trial-1 to 4. The occupants were elderly people aged over 65. A sample setup was shown in Figure 2. A sensor in the system is represented by <device id, name>(e.g. <8,Corridor To Bedroom Motion>) and the information is stored in the hub's database.

6.2. Data Collection

A dataset containing activations of sensors were recorded and stored in the hub's database. Software running in the hub communicates with all installed sensors in the system and stores event information along with time-stamp values in the database. A snapshot of collected data is shown below.

time	device id	action
2016-03-03 00:06:05	5	1
2016-03-03 00:08:43	2	1
2016-03-03 00:07:24	5	0
2016-03-03 00:12:51	12	1
2016-03-03 00:13:07	15	0

For example, for latch sensors attached to door the action value is stored as *1* when the door is opened and *0* when it is closed.

6.3. Behaviour modelling

To understand the behavioural pattern of each sensor, we conducted statistical analysis of the collected data. Our first step is to find the distribution of the number of activations of a particular sensor per day. After taking the clean data from the collected dataset we summarized them by summing up number of active states (value 1) of each sensor in a day. Then for each sensor we obtain a daily time-series data. Thus, our summarized data is similar to the following example.

Date	Device Id	activations
2016-03-03	12	110
2016-03-04	12	96
2016-03-04	13	337
2016-03-05	12	79
2016-03-05	13	355

Then, for each trial, we observe the distribution of activations for each sensor using a qq-plot .The qq-plot is a quantile-quantile plot of the quantiles of the sensor activations data y versus the theoretical quantiles values from a normal distribution. The plot appears linear when the data distribution is normal. Figure 4 shows the distribution of 20 different motion and latch sensors of trial-3 in qq-plot. We can observe from these plots that most devices tend to be linear, typical of a Normal distribution.

We can also see from histogram plot in Figure 5 that the sensor activations appear to have Normal distribution. This histogram is for bathroom door sensor installed in trial-4. In the histogram, the x-axis is the number of activations per day which is binned in six intervals of size 10. The y-axis is the number of days that fall into each bin. This plot also supports the occurrence of Normal distribution in sensor data.

We have observed such Normal distribution in more than 90% of the IoT sensors across four trials. A Normal distribution is also observed for pairwise sensor activations (occurrence of one after another) . Figure 6 shows such distribution for <seat motion, lounge to entry motion>sensor pair of trial-3.

To identify specific patterns in sequences of sensor activations we first converted the daily data to a sequence of numbers that represents device id (e.g. 3, 4, 20, 3, 20, 3, 15). If we combine all events for a particular observation period (e.g. 6 AM to 12 PM) in a day, we obtain a time-series of random sequence. A recurrence plot (RP) of 31 days (sequence length 10691) for the observation period 6:00-12:00 in trial-1 is shown in Figure 7. The visual appearance of an RP gives hints about the dynamics of the system.

We obtained RP to perform recurrence quantification analysis (RQA) [19]. RQA indicates the deterministic dynamics of a sequence of sensor events to determine whether their distributions are significantly different over the time. Here the state space of our system for RQA is all devices (motion and latch sensors) installed in the system. The RP is a graph of a square matrix in which the matrix elements correspond to those times at which a state of a dynamical system recurs. The RP reveals all the times when the phase space trajectory of the dynamical system visits roughly the same area in the phase space. A homogeneous pattern is observed in RP of Figure 7 which indicates the process is stationary as it is generated from a random time-series. Here the distribution of sequence is a stochastic process whose unconditional joint probability distribution does not change when shifted in time. Consequently, parameters such as mean and standard deviation also do not change over time. Therefore we can conclude that, a common pattern exists in each day observation. Anomalies in such processes can be observed using RQA which is discussed in the next section.

6.4. Anomaly detection

We have tested our implementation of anomaly detection on collected data of four trials for four cases - using single sensor, group of sensors, pairwise sensors and sequence of sensors activations. For each trial first we created different observation periods in the system. Example of such observation periods is presented in 2.

We have tested our approach with various time periods. We separated the first 2 weeks (14 days) data as a training set (T). Then we computed the mean μ_{ij} and standard deviation σ_{ij} of each observation period O_j for each sensors S_i.

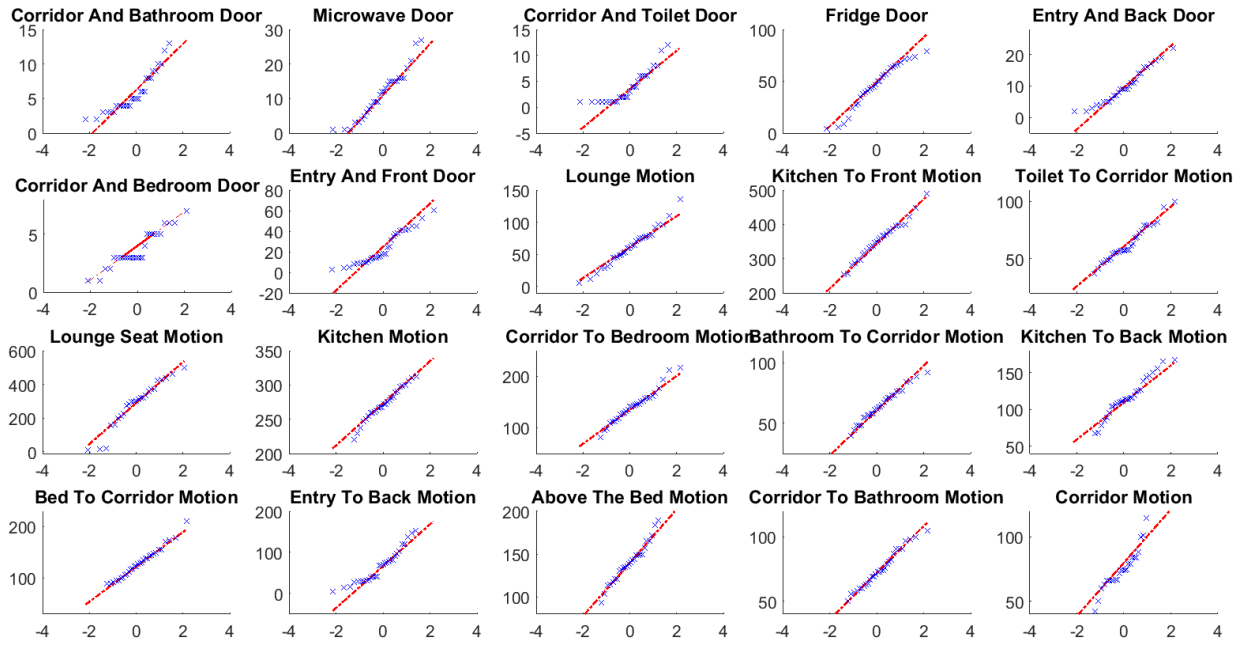

Figure 4. Identification of normal distribution using qq-plot of 20 different sensors installed in trial-3

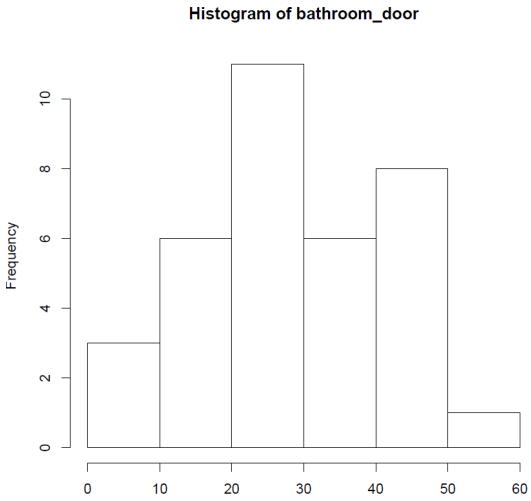

Figure 5. Distribution in histogram plot

Table 2. Observation periods

Monday 6:00 to 18:00 (6 hours)
Monday 6:00 to Tuesday 12:00 (18 hours)
Week 00:00 to 23:59 (24 hours)
Week 06:00 to 18:00 (12 hours)
Weekdays 12:00 to 23:59 (12 hours)
Friday 00:00 to 23:59 (24 hours)

An example observation of two sensors (kitchen and bedside motion sensor) of trial-1 is shown in Figure 8. Here the observation period is 6 AM to 6 PM (12 hours) of each day (O_j = Week 06:00 to 18:00) and training period T is 14 days. The sensor behaviours are examined for remaining 17 days data.

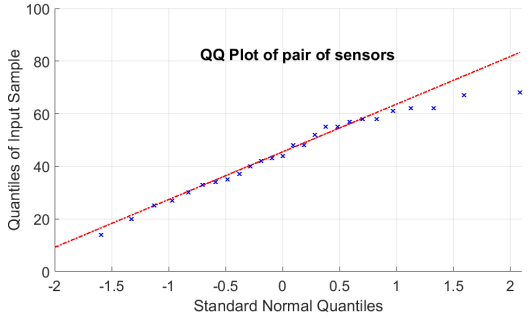

Figure 6. Normal distribution in pair of sensors

Here the threshold δ_{ij} is set as 1σ. Based on this δ the maximum (τ_{max}) and minimum (τ_{min}) tolerance values for anomaly detection is shown in red and purple reference line for both sensors. We observed four anomalies in *kitchen motion* at day 7,10,14 and 17 which are higher than τ_{max}. Four anomalies are found also in *Bedside motion sensor* (day 1,10,15 and 17). In day 1 it is lower than τ_{min} and in day 10,15 and 17 it is higher than the τ_{max}.

Anomaly has been also observed for group of sensors. A snapshot of sample generated report for anomaly detection based on aggregated sensor behaviour is shown in Figure 9.

Here, we computed statistics of a whole day

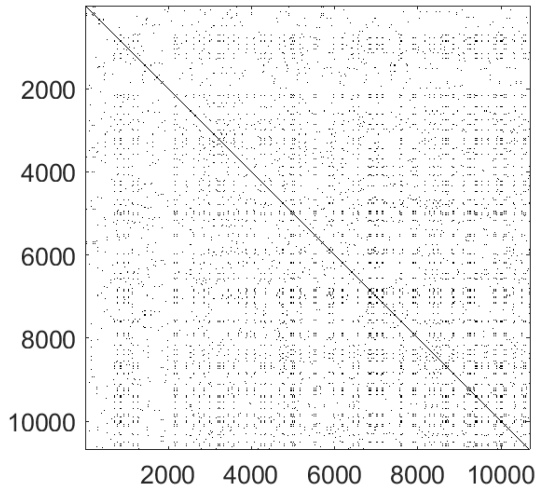

Figure 7. Recurrence plot of trial-1 data over 31 days for observation period 6:00-12:00

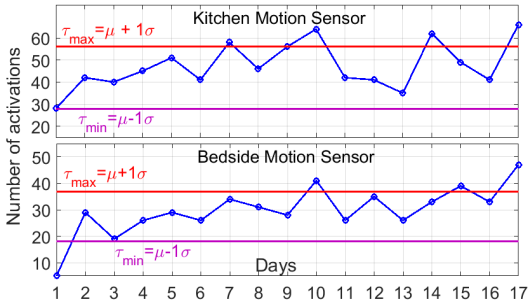

Figure 8. Anomaly in single sensor behaviour for period of 17 days using 14 days training

(24-hour) observation period for three groups. with threshold value set as 3σ for first 2 groups and 1σ for the last one. As we can see in Figure 9, for a new day our system detected anomaly in the behaviour of sensors in *Corridor* group and flagged that value with a marker (observed 490 where τ_{max} is 475) in the report.

Figure 10 shows a pairwise observation pattern that represents the number of occurrence in lounge room motion sensor above usual entry chair followed by lounge to entry motion sensor in trial-3. This case is also using 6 AM to 6 PM (12 hours) observation period of each day and 14 days training data. The sensor behaviours are observed for 17 days.

τ_{max} and τ_{min} using threshold value of 1σ and 2σ

```
Training Period #00:00:00-23:59:59 on week
==========================================
+----------+--------+---------+-----------+--------------+--------------+----------+
|  Group   |  Mean  | Std Dev | Threshold | Expected max | Expected min | Observed |
+----------+--------+---------+-----------+--------------+--------------+----------+
|Appliances| 66.93  |  39.94  |    3.0    |    186.75    |     0.00     |   117    |
| Corridor | 170.36 |  101.37 |    3.0    |    474.37    |     0.00     |   490*** |
| Bedroom  | 233.79 |  135.17 |    1.0    |    368.96    |    98.62     |   317    |
+----------+--------+---------+-----------+--------------+--------------+----------+
```

Figure 9. A sample report of anomaly detection

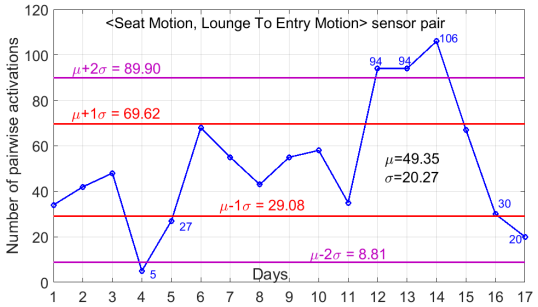

Figure 10. Anomalies in pairwise sensors behaviour for a period of 17 days using 14 days training

is shown in red and purple line in Figure 10. Here we observed six anomalies using threshold 1σ (on day 4,5,12,13,14,17). However, the number of anomalies is reduced to four when the threshold is 2σ.

We further applied this data to RQA and computed four RQA measures namely recurrence rate (RR), Determinism (DET), averaged diagonal line length (L), and entropy (ENTR). RR is a probability which indicates that a specific state will recur. DET is the percentage of recurrence points which form diagonal lines in the recurrence plot. Entropy normally reflects the amount of disorder in a data distribution. The result of RQA for the same data (used in Figure 7) is shown in Figure 11.

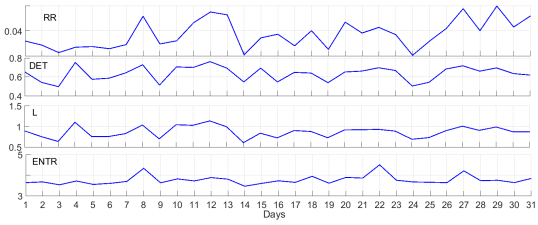

Figure 11. RQA measures of trial-1 data over 31 days for observation period 6:00-12:00

A high value of these four measures is a good indication that the system evolves very similar state as during another time. A very low value indicates significant difference which is an anomaly. Using this approach with Figure 11 anomalies are observed in day 3,9,14,19 and 24.

From our analysis we conclude that, our proposed approaches for anomaly detection is feasible and effective for detecting significant deviations in behaviour patterns of elderly. This is based on the evidence as proven by experimental outcomes presented earlier that 90% of IoT sensor activations fit a normal distribution which is an underlying aspect for detecting anomalies using the proposed approach.

7. Conclusion and Future Work

In the context of increasing demand for remote patient-care and early detection of abnormal situations for wellness monitoring, we proposed HalleyAssist, a personalised and secure IoT-based smart home system for AAL. Our system incorporates a novel anomaly detection approach that self-learns the user's normal behaviour patters from a combination of IoT sensor event patterns. A self-learned model is used for automated detection of anomalies which are indications of changes in behaviour of an elderly person. The approaches were validated for efficacy via large-scale real-world in-home deployment trial. The response from the older people to the deployed system was very positive. An analysis of the data collected from the trials demonstrate the existence of normal distribution in sensor behaviours and the proposed anomaly detection approach was able to effectively identify significant deviations in behaviour patters of the user.

As part of our future work, we plan to integrate additional IoT sensors such as a microphone which provide the cpability to detect emergencies as well as improve the accuracy of the anomaly detection solution. An alternative use of the system could be in detecting fall for elderlies in smart homes. We also plan in conducting a trial to evaluate the usability of the system.

References

[1] A. Lotfi, C. Langensiepen, S. M. Mahmoud, and M. J. Akhlaghinia, "Smart homes for the elderly dementia sufferers: identification and prediction of abnormal behaviour," *Journal of ambient intelligence and humanized computing*, vol. 3, no. 3, pp. 205–218, 2012.

[2] K. R. Evenson, M. M. Goto, and R. D. Furberg, "Systematic review of the validity and reliability of consumer-wearable activity trackers," *International Journal of Behavioral Nutrition and Physical Activity*, vol. 12, no. 1, p. 159, 2015.

[3] G. Yin and D. Bruckner, "Daily activity learning from motion detector data for ambient assisted living," in *Human System Interactions (HSI), 2010 3rd Conference on*, pp. 89–94, IEEE, 2010.

[4] M. A. Zamora-Izquierdo, J. Santa, and A. F. Gómez-Skarmeta, "An integral and networked home automation solution for indoor ambient intelligence," *IEEE Pervasive Computing*, vol. 9, no. 4, pp. 66–77, 2010.

[5] J. Austin, H. H. Dodge, T. Riley, P. G. Jacobs, S. Thielke, and J. Kaye, "A smart-home system to unobtrusively and continuously assess loneliness in older adults," *IEEE journal of translational engineering in health and medicine*, vol. 4, pp. 1–11, 2016.

[6] G. Demiris, B. K. Hensel, *et al.*, "Technologies for an aging society: a systematic review of smart home applications," *Yearb Med Inform*, vol. 3, pp. 33–40, 2008.

[7] M. Chan, D. Estève, C. Escriba, and E. Campo, "A review of smart homespresent state and future challenges," *Computer methods and programs in biomedicine*, vol. 91, no. 1, pp. 55–81, 2008.

[8] A. Forkan, I. Khalil, and Z. Tari, "Cocamaal: A cloud-oriented context-aware middleware in ambient assisted living," *Future Generation Computer Systems*, vol. 35, pp. 114–127, 2014.

[9] P. N. Dawadi, D. J. Cook, and M. Schmitter-Edgecombe, "Automated cognitive health assessment using smart home monitoring of complex tasks," *IEEE transactions on systems, man, and cybernetics: systems*, vol. 43, no. 6, pp. 1302–1313, 2013.

[10] R. Steele, A. Lo, C. Secombe, and Y. K. Wong, "Elderly persons perception and acceptance of using wireless sensor networks to assist healthcare," *International journal of medical informatics*, vol. 78, no. 12, pp. 788–801, 2009.

[11] N. K. Suryadevara, S. C. Mukhopadhyay, R. Wang, and R. Rayudu, "Forecasting the behavior of an elderly using wireless sensors data in a smart home," *Engineering Applications of Artificial Intelligence*, vol. 26, no. 10, pp. 2641–2652, 2013.

[12] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman, and T.-Y. Lin, "The role of prediction algorithms in the mavhome smart home architecture," *IEEE Wireless Communications*, vol. 9, no. 6, pp. 77–84, 2002.

[13] E. M. Tapia, S. S. Intille, and K. Larson, "Activity recognition in the home using simple and ubiquitous sensors," in *International conference on pervasive computing*, pp. 158–175, Springer, 2004.

[14] V. Jakkula, D. J. Cook, *et al.*, "Anomaly detection using temporal data mining in a smart home environment," *Methods of information in medicine*, vol. 47, no. 1, pp. 70–75, 2008.

[15] M. Novák, M. Biňas, and F. Jakab, "Unobtrusive anomaly detection in presence of elderly in a smart-home environment," in *ELEKTRO, 2012*, pp. 341–344, IEEE, 2012.

[16] A. R. M. Forkan, I. Khalil, Z. Tari, S. Foufou, and A. Bouras, "A context-aware approach for long-term behavioural change detection and abnormality prediction in ambient assisted living," *Pattern Recognition*, vol. 48, no. 3, pp. 628–641, 2015.

[17] C. C. Aggarwal, "Outlier analysis," in *Data mining*, pp. 237–263, Springer, 2015.

[18] J. H. Shin, B. Lee, and K. S. Park, "Detection of abnormal living patterns for elderly living alone using support vector data description," *IEEE Transactions on Information Technology in Biomedicine*, vol. 15, no. 3, pp. 438–448, 2011.

[19] B. Al-Musawi, P. Branch, and G. Armitage, "Detecting bgp instability using recurrence quantification analysis (rqa)," in *Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance*, pp. 1–8, IEEE, 2015.

[20] B. Schuster-Böckler and A. Bateman, "An introduction to hidden markov models," *Current protocols in bioinformatics*, vol. 18, no. 1, pp. A–3A, 2007.

[21] C. L. Webber Jr and N. Marwan, "Recurrence quantification analysis," *Theory and Best Practices*, 2015.