Case Study Report for HalleyAssist, an Ambient Assisted Living System (AALS)

S M RAGIB REZWAN
School of Science, Computing and Engineering Technologies
Swinburne University of Technology
Melbourne, VIC, Australia
103172423@student.swin.edu.au

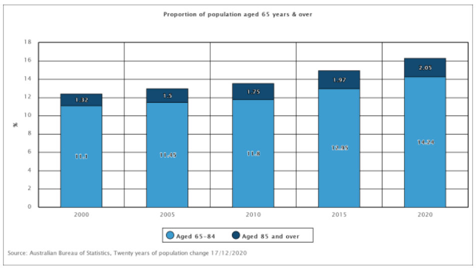
Executive Summary--- **This report provides a brief introduction about Ambient Assisted Learning System (AALS) and HalleyAssist before focusing on some of the security issues that it faces. This, in turn, links to an in-depth risk analysis on the 4 most critical risks faced by the system, found by using the Delphi method [1] (which ranks risks by identifying the asset at risk, its linked threat, likelihood and impact of threat, its possible counter measure and its effectiveness and relative cost).**

This information is then used to develop policy statements to identify the security goals that can overcome each risk (along with strict requirements that must be followed to avoid them). This, in turn, is used to perform a brief discussion of technologies and controls that can be implementing for them.

After this, the entire report is summarized in the conclusion with a list of recommendations that must be ensured in order to improve the security of the AALS HalleyAssist.

I. INTRODUCTION

Nowadays, people worldwide are living longer than their ancestors (the average life expectancy being that above 60 now according to WHO [2]), with the trend expecting to continue rising (See Fig. 1). Even so, the degradation of those people's mind and body due to age still continues, leading to an increase in number of people that require assistance. But unfortunately, due to restrictions such as distance, work hours, etc., their family members aren't able to provide them with the proper and timely care that they need.



Source: Australian Bureau of Statistics, Twenty years of population change 17/12/2020

Fig 1: Graph of proportion of people aged 65 years and over [3]

Even so, the elderly still prefer to stay in their own homes instead of moving to aged care facilities. So, in order to both ensure the elderly person's wishes and also maintain their health, Ambient Assisted Living System (AALS) has been developed.

AALS is basically an implementation of AAL whose aim is to provide the necessary technological support (through the use of Internet of Things (IoT), smart platform design, machine learning, etc.) to enable the aged population to stay at their homes [4, 5].This helps ensure that the elderly not only live independently at their own homes, but also remain healthy and thus removes the need for them to move to aged care facilities.

There are various types of AAL systems, ranging from simple IoT devices (like smart home appliance and wearable sensors) to complex sensor network (like combination of environmental sensors, smart devices, actuators, etc.) [6]. Among them, HalleyAsisst is one such system that uses the approach of monitoring and detecting abnormal changes in the elderly's behavioral patterns [5] in order to provide them with the support they need on time.

But even so, it still suffers with similar security issues that its AALS counterparts (of similar complexity) face in protection of its assets from threats. An asset is basically "anything that has value to the organization and therefore requires protection" [7], and can be in the form of information asset (like customer data, sensor event data, report data etc.), software asset (like system application data, model, etc.), physical assets (like wireless sensors and actuators such as motion sensors and speakers, devices used for central processing like Central Hub, etc.), etc. [5, 8] whilst a threats is basically a potential danger (like the compromise of information, loss of essential service, disturbance due to radiation, technical failures, unauthorized actions, compromise of function, etc. [7].

Note: Here, I am assuming that other AALS with similar complexity also have similar design framework as HalleyAssist.

Hence, in order to better understand the security issues faced by the HalleyAssist, an in-depth risk analysis is performed on 4 most critical risk factors in the Section II using the Delphi method [1]. This, in turn, is linked to section III where high level security goals are identified for those critical risks. These policies are later fed into section IV where details regarding implementation of the policies are identified. After this, the report concludes with a brief summary, alongside a list of recommendations to follow in the section V.

II. RISK ANALYSIS

In order to understand Risk analysis, one must first understand what risk is. According to ISO27005:2011 [7], risk is basically the potential that a threat will exploit the vulnerabilities present in an asset or group of assets and cause harm to an organization. Furthermore, it also states Risk Analysis as the process of comprehending the nature of risk and determining its level [7].

This analysis is generally performed by defining the asset, identifying the threat, determining the probability of occurrence, determining the impact (i.e. severity) of threat, setting up control (i.e. countermeasures) and documenting them [9]. These factors (merged with risk identification and evaluation aspects) form the risk assessment [7] for any system. Depending on the way they are combined, the risk assessment can be of two types, Quantitative or Qualitative.

In this report, the Qualitative risk assessment technique of Delphi [1] method is used. That’s because it’s far quicker and less expensive to perform qualitative assessment when compared to quantitative ones. Furthermore, it uses the opinions of domain and security experts which helps make the results more accurate and reliable [1].

But even so, it led to the creation of an enormous list of risks and countermeasures (as each asset has multiple threats and each threat has multiple countermeasures), like elderly data being breached through Caregiver portal (i.e. the control panel) due to lack of proper user authentication (which can be resolved with setting up proper user controls), lack of details regarding training of model and thus not being able to ensure lack of existence of system flaws (which can be resolved with proper auditing and testing of system), etc.

Hence, the information provided by Delphi [1] method (alongside authors from various papers and articles [10-21]) regarding the software and hardware utilized by the systems is summarized in the sections A-D for the 4 most critical risks.

Note: In the case study, very little details have been provided regarding security aspects of the system and its features, Hence it is being assumed that the system proposed is utilizing only the basics security aspects (i.e. only those that are common with typical AAL systems [11] and have not been specialized to deal with threats that are designed to target specific critical aspects.

Note: Relative cost value noted for each risk follows inverse order where higher numbers lower cost and vise-versa. This has been done to ensure that when the counter measures are ranked in terms of relative cost, the one at the top will be the cheapest one. Furthermore, it also ensures that proper ranking calculation can be performed using the formula mentioned in (1) to rank the risks

A) Risk to data stored in Raspberry Pi:

One of the most critical assets in the HalleyAssist system is the Elderly Personnel data that is stored in the database in the Central Hub inside the Raspberry Pi. Although various threats can impact it (like malicious actors brute forcing into the raspberry by connecting their laptop to it [16], device being damaged via short circuit due to improper power and ground pin connections [22], etc.), the most severe threat among them is having a malicious actors physically tamper with the device while the elderly or their caregiver are away. That’s because this threat would result in the malicious actor gaining full access to the stored data and allowing them to modify it at will.

But, this threat is quite unlikely to occur as there isn’t sufficient benefit for the actor to break into the person’s home (and risk getting caught) just to manipulate the raspberry pi and instead they can just burglarize the house. So, in terms of severity, it’s rank is 4 out of 5 while in terms of likelihood, it’s rank is 2 out of 5 (See Table no. I).

Note: Since Raspberry Pi itself is quite cheap (only around 55 dollars [23]), there actually isn’t much incentive for the malicious actors to steal it.

Furthermore, in this case, the simplest counter measure would be to keep the raspberry pi secured in a centralized location by bolting it to the wall or keeping it in a meshed enclosure or cabinet. This would be relatively inexpensive and would also be effective by acting as a deterrent for those who would wish to tamper with it. So, in terms of effectiveness, it’s 5 out of 5 and in terms of relative cost, it’s 4 out of 5 (See Table no. I).

B) Risk of unauthorized access through Caregiver Control Panel:

Through the Caregiver Control panel, caregivers or system supervisors can send threshold data to the model. Although these are various threats related to it (like loss of device used to access the control panel) , the most severe one is having unauthorized individuals (especially malicious actors) gain access to the Control panel, due to lack of adequate user authentication method either on the device or in the communication channel between device to model. That’s because this threat would result in the modification of the model and its thresholds, which can easily hamper the living condition of the elderly personnel.

This threat is also highly likely to occur as without proper user authentication, malicious actors can easily access and modify the model at any time (either directly through the caregiver’s device or by performing Man-in-the-middle type attacks between the device and the Central Hub). So, in terms of severity, it’s rank is 4 out of 5 while in terms of likelihood, it’s rank is also 4 out of 5 (See Table no. I).

In this case, the simplest counter measure would be to ensure that the client and their care-givers are aware of who has access to the Control Panel and not share that access with anyone else. Furthermore, this can be coupled with Multi-factor authentication (MFA) which stops basically 99.9% of automated attacks [24]. So, in terms of effectiveness, it’s 5 out of 5 and in terms of relative cost, it’s 4 out of 5 (See Table no. I).

C) Risk of adding new sensor to the system:

The HalleyAssist system also allows the flexibility of easily adding new IoT sensors. Although this a good advantage for the system, it does open the system to various threats. Among those threats the most prominent one is attacking the system through malicious IoT devices installed by malicious actors with the help of social engineering. That’s because the actors can utilize those devices to send false information to the system, causing it to behave in erratic manner (like playing high volume notifications through speaker, locking of door via latch, etc.).

Furthermore, it’s highly likely to occur as elderly people are more susceptible to such attacks due to their cognition decline due to age, lack of technical sophistication, etc.[25] So, in terms of severity, it’s rank is 4 out of 5 while in terms of likelihood, it’s rank is also 4 out of 5 (See Table 1).

In this case, the simplest counter measure would be making both the caregiver and the elderly personnel aware about various forms social engineering attacks and the ways to detect and avoid them. This is quite effective as even if the elderly personnel forget the various forms of social engineering attacks, their caregivers would still remember them and thus be will be able to keep the elderly safe. Furthermore, this method is quite cheap overall (but compared to the countermeasures mentioned in A and B, it’s slightly more expensive as the awareness must be provided and updated on a monthly basis). So, in terms of effectiveness, it’s 4 out of 5 and in terms of relative cost, it’s 3 out of 5 (See Table no. I).

D) Risk of data transfer over wireless network:

The system sends data in between the sensors, actuators and Raspberry Pi using wireless connection. While this provides an advantage in terms of flexibility, it does expose the system to various risks (like Man-in-the-middle type attacks, Denial of service type attacks, etc.) among which the most likely to occur is interference of data transfer due to devices such as microwave, radio, etc.

At a glance, this may not have much severity when compared to attacks such as MITM, DDOS, etc. But it shouldn’t be taken lightly as due to the sensitivity of wireless communication, this interference can even result in a network jamming [26-28]) which can have disastrous consequence (like house may catch fire while elderly is cooking using microwave but door isn’t opening as system isn’t being able to send the data to release the latch). So, in terms of severity, it’s rank is 3 out of 5 while in terms of likelihood, it’s rank is 5 out of 5 (See Table no. I).

In this case the best counter measure would be to use a network mesh of Zigbee devices where each device acts as a Zigbee signal repeater and ensure that the devices used have up to date hardware with their antennas pointing in the right direction. While this would have a high effectiveness, it will also be quite expensive. That’s because although each individual Zigbee signal amplifier is cheap (only 35.99 dollars [29]), a huge number of such devices are needed in order to minimize the impact of interference. So, in terms of effectiveness, it’s 4 out of 5 but in terms of relative cost, it’s 1 out of 5 (See Table no. I).

Since the relative values of severity and likelihood of each risk (along with their countermeasure’s relative, effectiveness and cost) have been found, these have been noted in Table no. I for ease of view.

Table no. I: Listing the severity and likelihood of the risks A-D, along with the effectiveness and cost of their respective countermeasures, (relative to one another)

Risk No.	***Severity***	***Likelihood***	***Effectiveness***	***Cost***
A	4	2	5	4
B	4	4	5	4
C	4	4	4	3
D	3	5	4	1

These values are then used in the following formula to calculate and rank the risks:

$$R = (L * S) - (E * C) \qquad (1)$$

where R = Risk Score, L = Likelihood, S = Severity, E= effectiveness of counter measure, and C = relative cost of countermeasure

This results in the following values for the risk score:

- For A- Risk to data stored in Raspberry Pi, the risk score is:-12
- For B- Risk of unauthorized access through Caregiver Control Panel, the risk score is: -4
- For C - Risk of adding new sensor to the system, the risk score is: 4
- For D - Risk of data transfer over wireless network, the risk score is: 11

Hence, the overall order or rank for the risks from most to least critical:

Risk D, Risk C, Risk B and Risk A

III. POLICY FORMULATION

Now that the 4 most critical risks impacting the system has been ranked and organized, it's time to determine the policies that can be used to address them. According to [5] and [30], Policies are high level statements of security goals. Hence, in order to formulate policies, one must consider what the ideal outcome will be and also ensure that it fully addresses the risk. Thus, following policies have been created with the help of SANS [31] and NIST [32].

A) Wireless communication policy between IoT devices:

It will mainly be utilized in order to overcome risk D and ensure that data can transfer between IOT device (i.e. sensors) and the Hub smoothly and securely, without being disrupted. This will be accomplished by fulfilling the following requirements:

1) All the IoT devices will be part of a dedicated wireless network channel whose frequency doesn't overlap with other networks (i.e. choosing between Zigbee channels from 11 to 26 [33]). This would ensure to protect it from disruption from other sources such as microwave, radio, etc. and ensure that data packets don't get dropped,

2) The network utilized by the IoT devices to communicate must utilize factors such as simple encryption protocols, authentication protocols, etc. to ensure that that data is transferred in a secure manner (avoiding Man in middle type attacks) and also ensure that there isn't too much overhead in data being transferred (and hence avoid data loss),

3) The IoT devices should utilize protocols (such as AMQP (advanced message queuing protocol), MQTT (Message Queue Telemetry Transport), etc. [34] to ensure proper queue of data when communicating with one another. This not only ensure that data is queued properly and but also ensures that the IoT devices can handle issues like poor network conditions, security, etc.,

4) The IoT devices should also utilize compression protocols (such as CoAP (Constrained Application Protocol)), which reduces size of network package [34]. This would reduce the network bandwidth overhead and thus ensure that no data is lost in transmission.

B) Social Engineering awareness policy:

It will mainly be utilized in order to overcome risk C and ensure that clients and their caregivers are not fooled by malicious actors pretending to be from the HalleyAssist organization. This will be accomplished by fulfilling the following requirements:

1) Ensure that the clients and their caregivers are made aware of all forms of social engineering attacks and ways to respond to them. That way they will be able to detect whenever social engineering attacks occur,

2) Ensure that the clients and their caregivers know who to contact in such situations. That way they will be able to inform the organization that such an attack had taken place,

3) Run various simulated test runs periodically (i.e. every 6 months or so) with the client and their caregivers of such scenarios so that they are more used to the proper steps to take whenever social engineering attacks are performed on them,

4) Ensure the client and their caregivers know which information should be kept fully confidential and why (i.e. password and login credentials for the system, version of software being used, etc.). That way they will be able to ensure the security of the system stays intact and thus not be harmed.

C) Remote access policy:

Here it has been assumed that the caregiver will be accessing the control panel remotely and not on site. Thus this policy will be utilized in order to overcome risk B and ensure that the caregivers can access the system securely. This will be accomplished by fulfilling these requirements:

1) Ensure that remote access is maintained by the use VPN (virtual private networks) with strong encryption and pass-phrases. This would ensure that the caregiver can access the control panel securely, even over insecure channels like the internet,

2) Ensure that caregiver protects that login and password properly and change it on a monthly basis. Furthermore, the caregivers should ensure that that good practice is maintained when choosing the password,

3) Ensure that the caregiver is accessing the panel on a secure device with up to date antivirus software in place. This ensures that the access to portal doesn't get breached due to insecure device,

4) Ensure that caregiver is not connected to any dubious networks simultaneously whilst accessing the panel. This ensures that malicious actors do not gain access to the panel by piggybacking their way through the dubious network.

D) Raspberry pi Security policy:

This policy will be utilized in order to overcome the risk A and ensure that the Raspberry pi device (that is holding the database) is not breached in any way, which in turn ensures the security of the clients' data. This will be accomplished by fulfilling the following requirements:

1) Ensure that the OS (operating system) in the raspberry pi remains up to date [16, 35]. This will be done by periodically connecting the device securely and temporarily to the internet and running the commands to update it. This ensure that the system has the latest security patches installed and thus reduce the chances of it being hacked,

2) Ensure that the default username and password has been changed and ensure that auto-login and empty passwords have been disabled [15, 16, 35]. This ensures that malicious actors can't use the commonly known username and passwords to access the system,

3) Ensure that a proper firewall has been installed on the device to ensure that only traffic from specified IoT devices (along with care giver's phone) has access to it and no other device. Furthermore, ensure to change the default port for SSH connection to the device. This prevents unauthorized access from unknown devices to the Raspberry pi which in turn reduces the chances of it being hacked [16, 35],

4) Ensure that brute force detection tools or plugins (such as Fail2ban [16]) are installed on the device. This prevent malicious actors from brute forcing the access to the system,

5) Ensure that the access between the device and the client and their caregivers is only done through encrypted, private channel like VPN. This ensures that malicious actors are not able to perform attacks such as MITM (man in the middle) and hence ensure the security of the device,

6) Ensure that the physical access to the device is protected. This can be done by keeping the device at a secure location (i.e. bolting it down to prevent it from being stolen). This will prevent malicious actors from tampering with the device and compromising its security.

IV. IMPLEMENTATION ONLINE

In the previous section, various policies and their base level requirement have been mentioned. Hence, in order to ensure that these requirements are met, the following technology and controls (i.e. the safeguards to protect confidentiality, integrity and availability of information, fulfilling security requirements [36] will be implemented:

A) *For wireless communication policy between IoT Devices:*

This can be fulfilled by finding the Zigbee protocol channel that has the least interference (amongst its 16 channels in 2.4 GHz range [33]) and restricting the IOT devices to only use that specific channel to pass data between the sensor and the central hub. This would ensure that the data transfer will face little interference, consume lesser amount of power whilst providing better coverage and security. Furthermore, these devices should also utilize Advanced Message Queuing Protocol (AMQP), and Message Queue Telemetry Transport (MQTT) for queuing the data [37] and Constrained Application Protocol (CoAP) for light-weight and efficient data transmission as part of the Data protocols [38]. Thus they will be able to overcome the issue of loss of data and data not reaching the hub (from sensor) in time (See Table no. II(a) and II(b) for comparison between the methods).

Table no. II(a): Comparison between solution methods' benefits and drawbacks for wireless communication policy between IoT Devices

Method	***Benefits***	***Drawbacks***
Using Specific Zigbee channel for all IOT devices	Ensures all IOT devices are following a single channel and thus makes it easy to find channel of least interference [39], HalleyAssist already utilizes Zigbee protocols and thus only needs to fix the channel which is relatively inexpensive (as no need to buy any new devices or install any new software).	Interference may still occur as even though Zigbee channels are narrow, that is not the case for Wi-Fi, microwave, etc. [39, 28].So, positioning of device and its surrounds will also need to be considered which can lead to extra planning, workarounds and expense (like changing setup and location of raspberry pi, sensor, actuators, etc.).
Using AMQP for data queuing	This messaging system has more options including reliable queuing, flexible routing security, message types, transactions, etc. [37].	It is not as lightweight and scalable as MQTT [37], It is not as easy to implement as MQTT [37].

Table no. II(b): Continuation of comparison between solution methods' benefits and drawbacks for wireless communication policy between IoT Devices

Method	***Benefits***	***Drawbacks***
Using MQTT for data queuing	It is extremely light weight and resource efficient (especially compared to AMQP) and thus has a fast response time and smooth data transfer [37], It is well suited to be used in embedded monitoring devices due to its scalability and in sending infrequent message on networks that have low bandwidth [37], It is easier to implement that AMQP [37].	It can only send basic messages and doesn't have in-depth security, meta data support or data transaction support as AQMP [37].
Using CoAP for lightweight and efficient data transmission	It is a simple protocol with little overhead and uses IPSEC and DTLS for secure communication [40], It has lower latency and consumes less power compared to HTTP [40].	It is unreliable as it uses UDP (so messages may be unordered or get lost) [40], It has communication issues for devices that use NAT [40].

B) *For Social Engineering Awareness Policy:*

This can be fulfilled by showing the clients and their caregivers' video demonstration of social engineering attacks, giving them list of social engineering scenarios and responses in a paper document and by providing them with periodic simulated social engineering attacks. These would not only ensure that the clients and their caregivers can detect whenever such attack occurs and would also know how to behave from the start and who to contact in such situations. Furthermore, it also ensures that they are aware of which information must be kept private and why (See Table no. III for comparison between the methods).

Note: Since both the elderly personnel and their caregivers are informed about these matters, even if the elder forgets about the matter, the caregiver can still ensure their protection from social engineering attacks.

Table no. III: Brief comparison between solution methods' benefits and drawbacks for Social Engineering awareness policy

Method	***Benefits***	***Drawbacks***
Using Video help clients and their caregivers be aware of social engineering type attacks	It conveys a lot of information in short time [41], It incorporates audio and visual effects which appeals to multiple senses and ensures better retention of information [41].	It takes time to set up video presentation [42].
Using Physical documents to help clients and their caregivers be aware of social engineering type attacks	There is ease of navigating between pages [43], It doesn't rely on access to electronic devices [43], It ensures that reader gets time to think about the information [43].	It is difficult to create copies and update the information presented in the paper document in a cheap manner [44], It is difficult to prevent it from being degraded over time, especially when not stored properly [44].
Using Simulated test runs with the client and their caregivers on different social engineering attack scenarios	This ensures that all senses of the person are utilized which ensure better retention on information, especially in older adults[45], It provides them with firsthand experience of the attack and thus makes them more alert and ready [46], It can be updated as needed and thus can account for changing attack scenarios.	It takes time, resources and personnel to set up a simulated attack scenario.

C) Remote Access Policy:

This can be fulfilled by setting up VPNs and by ensuring caregiver accesses portal on secure device and uses good practice when creating and securing their credentials. These will prevent MITM, eavesdropping, brute force type attacks, etc. which in turn would help ensure unauthorized access do not occur (See Table no. IV for comparison between the methods).

Table no. IV: Brief comparison between solution methods' benefits and drawbacks for Remote Access policy

Method	***Benefits***	***Drawbacks***
Setting up a VPN (like peer to peer) that the caregiver can use to pass data between the control panel and the system	It passes information between the panel and hub in an encrypted manner, securing the data [47].	It causes in overhead in data transfer which slows down data transmission rate [48].
Caregiver using secure device when accessing the control panel	It ensures that only the caregivers are accessing the panel and not any unauthorized individual [49].	Caregiver can only access the panel through specific devices (whose security fits the standards required by the company) which reduces flexibility.
Caregiver following Good practice in choosing and securing their credentials	It ensures password is of proper length (at least 16 characters), uses alphanumeric and symbols, and is something that is easy to remember but hard to guess. Furthermore, it should be regularly changed [50,51], It ensures password can't be found by malicious actors snooping around the client or their care giver online or offline (i.e. not sharing them with anyone, not passing it around in emails, not passing or storing them in clear text, etc.) [52].	It takes time and effort to create and update such a password on regular basis and the caregiver may instead use a common one for ease of access [53, 54].

D) Raspberry pi Security Policy:

This can be fulfilled by ensuring that the Operating System (OS) in the device is up to date, ensuring to change the default user credentials on device, setting up firewalls on system, setting up VPNS transfer data to and from the device and sensors and actuators, setting up plugins to detect brute force attacks, protecting physical access, etc. (See Table no. V for comparison between the methods).

Table no. V: Brief comparison between solution methods' benefits and drawbacks for Raspberry pi Security policy

Method	*Benefits*	*Drawbacks*
Updating OS of the raspberry pi holding the database	It ensures that security patches are up to date [16, 55].	Can have incompatibility issue with existing application [56], Can lead to chance of loss of data during update [56], Can lead to introduction of bugs into the system [56], Can lead to higher consumption of power or storage space [56].
Not using default credentials on the raspberry pi holding the database	It ensures malicious actors can't easily gain access to device [15, 16, 55].	It takes time and effort to create and update strong passwords on a regular basis and the technician setting up the credentials might be lazy [53, 54].
Setting up firewalls on the raspberry pi holding the database	It ensures malicious actors can't easily gain access to device [16, 55].	It needs to ensure only certain devices can gain access through the firewall which requires knowledge regarding firewall setup on raspberry pi [57].
Setting up VPN channels for raspberry pi to use when communicating with its sensors (like peer to peer)	It ensures malicious actors can't access or modify data being passed between the device and its sensors and actuators due to encryption [16].	It causes in overhead in data transfer which slows down data transmission rate [48].
Setting up plugins (like Fail2ban [16]) on the raspberry pi holding the database to detect brute force attacks	It ensures brute force attack on device can be prevented [16, 55].	Plugins needs to be set up properly to ensure legitimate device's IP is not blocked.
Protecting physical access to the raspberry pi device by keeping it in a secure location (like bolting it down)	It ensures that malicious actors don't tamper with the device or its SD card [16].	It may require additional expense (like cost for buying cage to keep it, ensuring SD card can't be removed, etc.[16, 58]) It may require placing it in certain locations, impacting the rate of data transmission.

V. CONCLUSION

Overall, in this report, a brief introduction is provided which explains the reason behind the creation of AALS type system like HalleyAssist and yet still suffers from security issues (both common and uncommon with AALS of similar complexity).

After this, a risk analysis is performed on the 4 most critical risks faced by the system, where Delphi method [1] is used to identify the asset at risk, its linked threat, likelihood and impact of threat, alongside its possible counter measure (and their effectiveness and relative costs). This is later utilized to accurately rank the risks.

This, in turn, is used to develop policy statements to identify the security goals that can overcome each risk (along with strict requirements to ensure all aspects of the risk have been addressed). These are later utilized in the implementation section where possible technologies and controls to implement the policies are discussed, along with their benefits and drawbacks.

Thus, using all of this information the following list of recommendations is created:

- Ensure proper authentication and encryption channels have been set for access into the system via the caregiver control panel (by setting up VPNs),

- Ensure adequate time and resources is provided for training the model (along with appropriate and in-depth testing to ensure avoidance of all system bugs),

- Ensure that the IoT devices are restricted to use only the specific Zigbee channel (in the 2.4Ghz range) that has least interference, alongside having simple encryption, using the best practices for data protocols (like AMQP, MQTT, CoAP), etc.,

- Ensure that adequate measures (like video, paper documentation and simulated test runs of various, social engineering attack type, etc.) have been taken to enable the elderly and their caregivers to not only detect instances of social engineering attack, but also know who to contact and the ways to defend against it,

- Ensure that the Caregiver control panel is properly protected (i.e. by setting up VPNs, by ensuring caregivers use strong credentials and updating them on regular basis, by ensuring that panel is accessed by properly secured device, etc.),

- Ensure that the device that contains the database (that is used to store the elderly's data) is secured (i.e. by ensuring it's up to date, by ensuring it doesn't use default credentials, by ensuring proper firewall setup, by ensuring setup of plugins to detect and prevent brute force attacks, by ensuring access is only permitted through VPNS, by ensuring physical device and its SD card is protected, etc.).

REFERENCES

[1] P.Branch (2023). TNE30009/TNE80009 - Formulating and implementing the security policy - Lecture 8 [Portable document format (pdf)]. Available: https://swinburne.instructure.com/courses/49751/pages/lectures-week-3?module_item_id=3185476 (Accessed May 19, 2023).

[2] World Health Organization (WHO). "Ageing and Health." *World Health Organization*, World Health Organization: WHO, 1 Oct. 2022, www.who.int/news-room/fact-sheets/detail/ageing-and-health (Accessed May 19, 2023).

[3] Australian Bureau of Statistics. "Twenty Years of Population Change | Australian Bureau of Statistics." *Www.abs.gov.au*, 17 Dec. 2020, www.abs.gov.au/articles/twenty-years-population-change#ageing-population (Accessed May 19, 2023).

[4] Fuchsberger, Verena. "Ambient Assisted Living: Elderly People's Needs and How to Face Them." *Proceedings of the 1st ACM International Workshop on Semantic Ambient Media Experiences*, Association for Computing Machinery, 2008, pp. 21–24, https://dl.acm.org/doi/abs/10.1145/1461912.1461917 (Accessed May 19, 2023).

[5] P.Branch (2023). TNE30009/TNE80009 - Case Study [Portable document format (pdf)]. Available: https://swinburne.instructure.com/courses/49751/assignments/508059 (Accessed May 19, 2023).

[6] G. Cicirelli, R. Marani, A. Petitti, A. Milella and T. D'Orazio "Ambient Assisted Living: A Review of Technologies, Methodologies and Future Perspectives for Healthy Aging of Population." *Sensors*, vol. 21, no. 10, 19 May 2021, p. 3549, https://doi.org/10.3390/s21103549 (Accessed May 19, 2023).

[7] *Information Technology—Security Techniques—Information Security Risk Management (ISO/IEC 27005:2011)*. Online, Australian/New Zealand Standard, 2012, https://subscriptions.techstreet.com/products/814099 (Accessed May 19, 2023).

[8] P.Branch (2023). TNE30009/TNE80009 – Security Management - Lecture 7 [Portable document format (pdf)]. Available: https://swinburne.instructure.com/courses/49751/pages/lectures-week-3?module_item_id=3185476 (Accessed May 19, 2023).

[9] Peltier, Thomas R. "Risk Analysis and Risk Management." *Information Systems Security*, vol. 13, no. 4, Sept. 2004, pp. 44–56, https://doi.org/10.1201/1086/44640.13.4.20040901/83732.7 (Accessed May 19, 2023).

[10] C. Ge, C. Yin, Z. Liu, L. Fang, J. Zhu, and H. Ling, "A privacy preserve big data analysis system for wearable wireless sensor network," *Computers & Security*, vol. 96, p. 101887, Sep. 2020, doi: https://doi.org/10.1016/j.cose.2020.101887 (Accessed May 19, 2023).

[11] M. Schmidt and R. Obermaisser, "Adaptive and technology-independent architecture for fault-tolerant distributed AAL solutions," *Computers in Biology and Medicine*, vol. 95, pp. 236–247, Apr. 2018, doi: https://doi.org/10.1016/j.compbiomed.2017.11.002 (Accessed May 19, 2023).

[12] A. Koren and D. Šimunić, "Requirements and challenges in wireless network's performance evaluation in ambient assisted living environments," *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2016, pp. 624-627, doi: https://doi.org/10.1109/MIPRO.2016.7522216 (Accessed May 19, 2023).

[13] J. Sainz-Raso, S. Martin, G. Diaz and M. Castro, "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses," in *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 47-52, 1 Nov. 2019, doi: https://doi.org/10.1109/MCE.2019.2941347 (Accessed May 19, 2023).

[14] J. Carson, O. Nichols, C. Bonham, P. Bond, W. Simpson, and M. Crow, "Exploring the Vulnerabilities and Prevention of Raspberry Pi System," *emerging-researchers.org*, 2023. https://emerging-researchers.org/projects/12496/ (accessed May 19, 2023).

[15] CVEdetails, "CVE-2021-38759: Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain a," *www.cvedetails.com*, 2021. https://www.cvedetails.com/cve/CVE-2021-38759/ (accessed May 19, 2023).

[16] P. Fromaget, "17 security tips for your Raspberry Pi," *Raspberry tips*, 2020. https://raspberrytips.com/security-tips-raspberry-pi/ (accessed May 19, 2023).

[17] M. Sharma, "Safe by Design – An Overview of UX Security," *Toptal Design Blog*, 2023. https://www.toptal.com/designers/product-design/ux-security (accessed May 19, 2023).

[18] Jeppe, "Importance of user Interface protection from cyber attacks," *Codesealer*, Oct. 30, 2019. https://codesealer.com/what-is-user-interface-protection/ (accessed May 19, 2023).

[19] A. Hewko, "Application Security in UX Design | 4 Common Concerns and Risks," *Software Secured*, Sep. 09, 2021. https://www.softwaresecured.com/security-in-ux-design/ (accessed May 19, 2023).

[20] U. O. Nwokedi, B. A. Onyimbo, and B. B. Rad, "Usability and Security in User Interface Design: A Systematic Literature Review," *International Journal of Information Technology and Computer Science*, vol. 8, no. 5, pp. 72–80, May 2016, doi: https://doi.org/10.5815/ijitcs.2016.05.08 (accessed May 19, 2023).

[21] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," *Wireless Networks*, vol. 27, no. 8, May 2020, doi: https://doi.org/10.1007/s11276-020-02340-0 (accessed May 19, 2023).

[22] Robotics Backend, "Raspberry Pi 4 Pins - Complete Practical Guide," *The Robotics Back-End*, May 06, 2019. https://roboticsbackend.com/raspberry-pi-3-pins/ (accessed May 19, 2023).

[23] Pi Australia, "Raspberry Pi 3 Model A+ — Raspberry Pi Australia," *Pi Australia*, Feb. 09, 2020. https://raspberry.piaustralia.com.au/products/raspberry-pi-3-model-a-plus (accessed May 19, 2023).

[24] M. Maynes, "One simple action you can take to prevent 99.9 percent of attacks on your accounts," *Microsoft Security Blog*, Aug. 20, 2019. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/ (accessed May 19, 2023).

[25] M. Saltzman, "Elder fraud is real. Tell your parents, grandparents and friends about these scams," *USA TODAY*, Sep. 18, 2022. https://www.usatoday.com/story/tech/2022/09/18/cybercrime-cost-american-seniors-3-billion-last-year-62-jump/10420029002/ (accessed May 19, 2023)

[26] Quora, "My microwave is interfering with WiFi, how can this be fixed?," Jun. 18, 2016. https://www.quora.com/My-microwave-is-interfering-with-WiFi-how-can-this-be-fixed (accessed May 19, 2023).

[27] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, Secondquarter 2022, doi: https://doi.org/10.1109/COMST.2022.3159185.

[28] A. Tiwari, "Wifi Microwave: Why Do Microwave Interferes With Wifi?," *Science ABC*, Jan. 17, 2018. https://www.scienceabc.com/innovation/do-microwaves-interfere-with-wifi-signals.html (accessed May 19, 2023).

[29] Amazon, "Amazon.com : zigbee repeater," *www.amazon.com*. https://www.amazon.com/zigbee-repeater/s?k=zigbee+repeater (accessed May 19, 2023).

[30] P.Branch, private communication, Apr. 2023.

[31] SANS, "Information Security Policy Templates | SANS Institute," *www.sans.org*, 2020. https://www.sans.org/information-security-policy/ (accessed May 19, 2023).

[32] NIST, "Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE," Sep. 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf (accessed May 19, 2023).

[33] RF Wireless World, "zigbee channels-2.4GHz,868MHz,915MHz zigbee channels," *www.rfwireless-world.com*, 2012. https://www.rfwireless-world.com/Terminology/zigbee-channels.html

[34] Particle, "A 2022 Guide to IoT Protocols and Standards," *Particle*, 2023. https://www.particle.io/iot-guides-and-resources/iot-protocols-and-standards/ (accessed May 19, 2023).

[35] J. Jolles, "Increasing security," *The Raspberry Pi Guide*, 2021. https://raspberrypi-guide.github.io/other/Improve-raspberry-pi-security (accessed May 19, 2023).

[36] CSRC - NIST, "security control - Glossary | CSRC," *csrc.nist.gov*. https://csrc.nist.gov/glossary/term/security_control (accessed May 19, 2023).

[37] Inbound Square, "AMQP vs. MQTT: A deep dive comparison," *Macrometa*, 2023. https://www.macrometa.com/iot-infrastructure/amqp-vs-mqtt (accessed May 19, 2023).

[38] J. Gomez, "IoT Protocols: All You Need to Know," *Koombea*, Aug. 11, 2021. https://www.koombea.com/blog/iot-protocols/ (accessed May 19, 2023).

[39] Meta Geek, "ZigBee and Wi-Fi Coexistence," *MetaGeek*, 2023. https://www.metageek.com/training/resources/zigbee-wifi-coexistence/ (accessed May 19, 2023).

[40] RF Wireless World, "Advantages of CoAP protocol | disadvantages of CoAP protocol," *www.rfwireless-world.com*, 2012. https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-CoAP.html (accessed May 19, 2023).

[41] Crowd Wisdom, "5 benefits of video-based learning." *CrowdWisdom by Community Brands*, Mar. 15, 2017. https://www.crowdwisdomlms.com/blog/5-benefits-of-video-based-learning/ (accessed May 19, 2023).

[42] Student Brands, "The Key Pros and Cons of Video Learning - Student Brands," *studentbrands.co.za*, 2019. https://studentbrands.co.za/student-news/the-key-pros-and-cons-of-video-learning/ (accessed May 19, 2023).

[43] D. Oppenheimer, "The relative advantages and disadvantages of paper and digital media in education," *My College*, Jan. 16, 2019. https://my.chartered.college/impact_article/the-relative-advantages-and-disadvantages-of-paper-and-digital-media-in-education/ (accessed May 19, 2023).

[44] K. Takahashi, "Paper based learning`s disadvantages and the implementation of our learningBOX,lms. (Paper based learning`s disadvantages and why we should implement learningBOX)," *learningBOX / E-learning and learning management system that anyone can use easily*, Jul. 12, 2019. https://learningbox.online/en/2019/07/12/advantagesofelearning/ (accessed May 19, 2023).

[45] J. Mora, I. Quito, and L. Sarmiento, "A case study of learning styles of older adults attending an English course," *MASKANA*, vol. 8, no. 2, pp. 1–15, Dec. 2017, doi: https://doi.org/10.18537/mskn.08.02.01 (accessed May 19,2023).

[46] N. A. Ahmad, M. F. Abd Rauf, N. N. Mohd Zaid, A. Zainal, T. S. Tengku Shahdan, and F. H. Abdul Razak, "Effectiveness of Instructional Strategies Designed for Older Adults in Learning Digital Technologies: A Systematic Literature Review," *SN Computer Science*, vol. 3, no. 2, Jan. 2022, doi: https://doi.org/10.1007/s42979-022-01016-0 (accessed May 19,2023).

[47] Fortinet, "Benefits of VPNS: What are the pros and cons of a VPN?," *Fortinet*, 2023. https://www.fortinet.com/resources/cyberglossary/benefits-of-vpn (accessed May 19, 2023).

[48] L. Loic, "7 Disadvantages of Using a VPN," *MUO*, Dec. 29, 2022. https://www.makeuseof.com/disadvantages-of-using-vpn/ (accessed May 19, 2023).

[49] Kensington, "Why It's Important to Secure my Device?," *Kensington*, Apr. 08, 2022. https://www.kensington.com/en-au/news-index---blogs--press-center/security-blog/why-its-important-to-secure-my-device/ (accessed May 19, 2023).

[50] SANS, "CONSENSUS POLICY RESOURCE COMMUNITY Password Construction Guidelines," Oct. 2022. [Online]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt12766e4f951b7c37/636f1a30cfdbc24307bfdf58/Password_Construction_Guidelines.pdf (accessed May 19, 2023).

[51] Technology Solutions, "How to Make a Strong Password," *Technology Solutions*, Mar. 23, 2018. https://www.techs.co.nz/how-to-make-a-strong-password (accessed May 19, 2023).

[52] SANS, "CONSENSUS POLICY RESOURCE COMMUNITY Password Protection Policy," Oct. 2022. [Online]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf5d5757503e36442/636f1a316bafb12e165da155/Password_Protection_Policy.pdf (accessed May 19, 2023).

[53] Cyber Security Connect, "Lazy passwords putting two-thirds of Aussie organisations at risk," *www.cybersecurityconnect.com.au*, May 05, 2022. https://www.cybersecurityconnect.com.au/commercial/7798-password-laziness-linked-to-hacking (accessed May 19, 2023).

[54] A. Truly, "Passwords are hard and people are lazy, new report shows," *Digital Trends*, Oct. 21, 2022. https://www.digitaltrends.com/computing/passwords-are-hard-and-people-are-lazy/ (accessed May 19, 2023).

[55] Emmet, "Improve the Security of your Raspberry Pi," *Pi My Life Up*, Sep. 01, 2020. https://pimylifeup.com/raspberry-pi-security (accessed May 19, 2023).

[56] LinkedIn, "What are the benefits and risks of updating to the latest OS version?," *www.linkedin.com*, 2023. https://www.linkedin.com/advice/1/what-benefits-risks-updating-latest-os-version (accessed May 19, 2023).

[57] Sunny Valley Networks, "What is the Most Common Cause of Firewall Failure? - sunnyvalley.io," *www.sunnyvalley.io*, 2023. https://www.sunnyvalley.io/docs/network-security-tutorials/most-common-cause-of-firewall-failure (accessed May 19, 2023).

[58] Raspberry Pi, "Disabling password reset - Raspberry Pi Forums," *forums.raspberrypi.com*, Dec. 09, 2014. https://forums.raspberrypi.com/viewtopic.php?t=93628 (accessed May 19, 2023).