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

Contents

Executive summary:

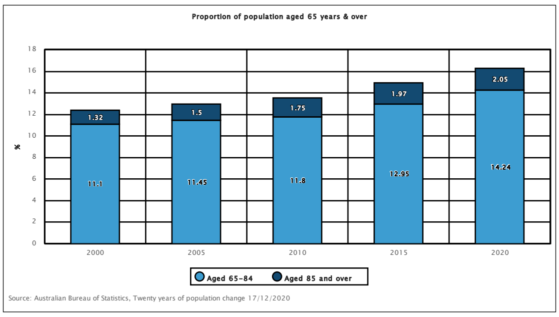
This report provides a brief introduction focusing on the reason behind the creation of AALS (ambient assisted living system), how HalleyAssist stands out (among the other AALS of similar complexity), along with the security issues that it suffers. This, in turn, links to an in-depth risk analysis on the 4 most critical risks faced by the system performed using 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 was later 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, was used to create a brief discussion of technologies and controls that can be implement them.

After this, the report was 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 being seen to be living longer than their ancestors and having higher life expectancy (more than 60 **[2]**).Not only does this not show any signs of slowing down, but instead is even expected to continue increasing, with the World Health Organization, WHO), expecting 1/6 of the population to be 60 years old or above by 2030 **[2]**. This increase in lifespan leads to greater number of memories which in turn leads to stronger family bonding. Thus, it results in elderly population being keener on living with their family.



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]**

But usually their family members have to live far away or have to work long hours and so are unable to properly provide the care the elderly need. Thus it results in poor living condition for the elderly.

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, AALS (ambient assisted living system) has been developed.

AALS is basically 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 ensures that the elderly can not only live independently at their own homes, but also remain healthy and thus removes the need to 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]**. Amongst them, HalleyAsisst System stands out with its novel approach in monitoring and detecting abnormal changes in the elderly's behavioral patterns **[5]**.

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**: Assuming other AALS with similar complexity also have similar design framework.]

Hence, in order to better understand the security issues faced by the HalleyAssist, an in-depth risk analysis have been performed on 4 most critical risk factors in the **"II. Risk Analysis"** section using the Delphi method [1]. This in turn has been linked to **"III. Policy Formulation"** section where high level security goals have been identified for those critical risks. These policies have been later fed into **"IV. Implementation Outline"** section where details regarding implementation of the policies have been identified. After this, the report has been concluded with a brief summary of the report, alongside a list of recommendations to follow in the **"V. Conclusion"** section.

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 asset 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 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 has been utilized. That's because it far quicker and less expensive to perform qualitative assessment when compared to quantitative ones. Furthermore, it utilizes the opinions of domain and security experts which make the results more accurate and reliable **[1]**.

But even so, it has 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 Career 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 can't ensure no system flaws exists (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] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21]** regarding the software and hardware utilized by the systems have been summarized in the following two tables:

No	Asset	Threat	Severity /Impact	Likelihood
A	Elderly person's current data stored in database in Central Hub	Raspberry pi getting hacked and thus allowing malicious actors to modify the stored data	8	5
B	Threshold data sent to model from Caregiver Control Panel	Malicious actors gaining access to the Control Panel due to lack of adequate user authentication method	8	8
C	New sensors added to the system	Malicious actors using social engineering to convince the elderly or caregivers to add custom made malicious IOT device	8	8
D	Data transfer over wireless	Data not being able to reach from sensor to hub in time, due to interference from devices like microwaves, radios, etc.	5	10

Table 1: Analyzing risk environment by segmenting into asset, threat, severity/impact and likelihood

[**Note**: Here, the first table notes the asset, its linked threat, severity of threat, likelihood of threat occurrence, whilst the second one notes the easiest way to counter it, alongside the effectiveness of the counter measure and its relative cost (for the previously mentioned asset and threat pairs).]

[**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 base 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 noted 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 ensures that proper ranking calculation can be performed in for the formula utilized to rank the risks]

No	Counter--measure	Effectiveness	Relative cost
A	Periodically update the OS in the Raspberry pi	10	5
B	Ensure that the client and their care-givers are aware of who has access to the Control Panel and not share	10	8

	that access with anyone else		
C	Ensure that the client and their care-givers are aware of social engineering attack and ways to avoid them	8	8
D	Modifying devices to ensure they use 5Ghz band to transfer data instead of 2.4 (as microwaves utilize that frequency and thus can cause noise **[22]**	8	2

Table 2: Analyzing risk environment by noting down counter measure and their effectiveness and cost for the corresponding asset and threat pair

[**Note**: In order to fully understand the risk environment (that has been noted in the above 2 tables), the meaning behind the numbers stated in severity/Impact, Likelihood, effectiveness and relative cost have been noted in the tables below (created with help from information in NIST **[23]**)]

Severity/ Impact Score	Meaning
10	The threat event might cause multiple instances of: (i) severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) major damage to organizational assets; (iii) major financial loss; (iv) severe or catastrophic harm to individuals, including loss of life
8	The threat event might cause a single instance of: (i) severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) major damage to organizational assets; (iii) major financial loss; (iv) severe or catastrophic harm to individuals, including loss of life
5	The threat event might cause: (i) significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but not effectively; (ii) significant damage to organizational assets; (iii) significant financial loss; (iv) significant harm to individuals, without any loss of life

2	The threat event might cause: (i) degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but slightly less effectively; (ii) minor damage to organizational assets; (iii) minor financial loss; (iv) minor harm to individuals
0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, organization's individuals and other organizations, or the Nation.

Table 3: Linking up Severity/Impact numbers to their meaning to better understand the risk environment [modified from NIST **[23]**]

Likelihood Score	**Meaning**
10	i) Adversary is almost certain to attack, ii) Error, accident or act of nature is almost certain to occur, or occur more than 100 times a year
8	i) Adversary is highly likely to attack, ii) Error, accident or act of nature is highly likely to occur, or occur between 10-100 times a year
5	i) Adversary is somewhat likely to attack, ii) Error, accident or act of nature is somewhat likely to occur, or occur between 1-10 times a year
2	i) Adversary is unlikely to attack, ii) Error, accident or act of nature is unlikely to occur, or occur between less than a year or more than once every 10 years
0	i) Adversary is highly unlikely to attack, ii) Error, accident or act of nature is highly unlikely to occur, or occur between less once every 10 years

Table 4: Linking up likelihood numbers to their meaning to better understand the risk environment [modified from NIST **[23]**]

Effectiveness Score	**Meaning**
10	The Control measure will result in complete removal of the risk that has been noted with no chance of any re-emergence of risk
8	The Control measure will result in almost complete removal of the risk that has been noted, but there might be small chance of re-emergence of risk
5	The Control measure will result in partial removal of the risk that has been noted, with a moderate chance of re-emergence of risk

2	The Control measure will result in little impact in removal of the risk that has been noted, with a high chance of re-emergence of risk
0	The Control measure has no impact on removal of risk

Table 5: Linking up effectiveness numbers to their meaning to better understand the control noted for the risk environment

Relative Cost Score	**Meaning**
10	The chosen Control measure has little to no cost when compared to the rest and thus should definitely be used
8	The chosen Control measure has little cost and is quite cheap when compared to the rest and thus should definitely be used
5	The chosen Control measure is moderately expensive when compared to the rest
2	The chosen Control measure is quite expensive when compared to the rest and thus shouldn't be used unless no cheap alternatives
0	The chosen Control measure is extremely expensive when compared to the rest and thus shouldn't be used

Table 6: Linking up Relative Cost numbers to their meaning to better understand the control noted for the risk environment

Once this has been done, the risk score has been calculated using the following formula:

Risk Score = (Severity/Impact * likelihood) – (effectiveness*relative cost)

This resulted in the following values for the risk:

- For A (risk of raspberry Pi getting hacked and allowing actors to modify stored data in database), the risk score is:-10
- For B (risk of actors gaining access to Control Panel), the risk score is: -16
- For C (risk of actors adding malicious IOT device using social engineering), the risk score is: 0
- For D (risk of data not being able to reach from sensor to hub), the risk score is: 34

<u>Hence, the overall order or rank for the risks from most to least critical:</u>

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 P. Branch **[24]** (and the case study **[5]**), Policies are basically 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 **[25]** and NIST **[23]**.

1. <u>Wireless communication policy between IoT devices:</u>

   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:

a. All the IoT devices will be part of a dedicated wireless network band whose frequency doesn't overlap with other networks (i.e. utilizing 5G instead of 2.4G that is utilized by Zigbee **[26]**. 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

b. 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),

c. The IoT devices should utilize protocols (such as AMQP (advanced message queuing protocol), MQTT (Message Queue Telemetry Transport), etc. **[27]** 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.

d. The IoT devices should also utilize compression protocols (such as CoAP (Constrained Application Protocol)), which reduces size of network package **[27]**. This would reduce the network bandwidth overhead and thus ensure that no data is lost in transmission

2. <u>Social Engineering awareness policy:</u>

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:

a. 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

b. 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

c. 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.

d. 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

3. <u>Remote access policy:</u>

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:

a. 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

b. 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

c. 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

d. 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

4. <u>Raspberry pi Security policy:</u>
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 and which ensure security of the clients' data. This will be accomplished by fulfilling the following requirements:

a. Ensure that the OS (operating system) utilized in the raspberry pi remains up to date **[16] [28]** . 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

b. Ensure that the default username and password has been changed and ensure that auto-login and empty passwords have been disabled **[15] [16] [28]**. This ensures that malicious actors can't use the commonly known username and passwords to access the system

c. 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] [28].**

d. 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

e. 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

f. 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 Outline:

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 **[29]** will be implemented:

1. <u>For wireless communication policy between IoT Devices:</u>
   This can be fulfilled by utilizing the mMTC, NB-IoT, etc. instead of Zigbee protocols 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 also utilize AMQP (advanced message queuing protocol), and MQTT (Message Queue Telemetry Transport) for queuing the data **[30]** and CoAP (Constrained Application Protocol) for compression of data **[31]**, Thus they will be able to overcome the issue of loss of data and data not reaching the hub (from sensor) in time.

Method	Benefits	Drawbacks
Using mMTC protocols to pass data between sensors and central Hub	Uses 5G features to transfer small amount of data quickly **[32]** Ensures optimal battery usage of devices **[32]** It is scalable **[32]**	Needs to send a lot of control signals before transferring data **[32]** Uses existing infrastructure which isn't well adapted for small data transfers and shorter sessions **[32]**
Using NB-IOT protocols to pass data between sensors and central Hub	Optimized for low throughput **[32]** Provides deployment flexibility **[32]**	Makes use of old LTE technology **[32]**
Using Z-Wave protocols to pass data between sensors and central Hub	Uses low amount of power and is easy to install **[33]** It is cheaper and provides AES-128 for encryption **[33]**	Operated in ISM bands 868 and 908 MHZ which can have interference issue **[33]** It has lower data communication speeds, even compared to Zigbee **[33]**

Table 7: A brief comparison between mMTC, NB-IOT and Z-wave in terms of benefits and drawbacks

2. <u>For Social Engineering Awareness Policy:</u>
   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.

Method	Benefit	Drawback
Using Video help clients and their caregivers be aware of social engineering type attacks	Conveys a lot of information in short time **[34]** Incorporated audio and visual effects which appeals to multiple senses and ensure better retention of information **[34]**	It takes time to set up video presentation **[35]**
Using Physical documents to	Ease of navigating between pages	It is difficult to create

help clients and their caregivers be aware of social engineering type attacks	**[36]** Doesn't rely on access to electronic devices **[36]** Ensures that reader gets time to think about the information **[36]**	copies and update the information presented in the paper document in a cheap manner **[37]** It is difficult to prevent it from being degraded over time, especially when not stored properly **[37]**
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**[38]** It provides them with firsthand experience of the attack and thus makes more alert and ready **[39]** 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

Table 8: Brief comparison between solution methods benefits and drawbacks for Social Engineering awareness policy

3. 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, eaves dropping, brute force type attacks, etc. which in turn would help ensure unauthorized access do not occur.

Method	Benefit	Drawback
Setting up a VPN (like peer to peer) that the caregiver can use to pass data between the control panel and the system	Passes information between the panel and hub in an encrypted manner, securing the data **[40]**	Causes in overhead in data transfer which slows down data transmission rate **[41]**
Caregiver using secure device when accessing the control panel	Ensure that only the caregivers are accessing the panel and not any unauthorized individual **[42]**	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	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 **[43][44]**	It takes time and effort to create and update such a password on regular basis and the caregiver may

	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.) **[45]**	instead use a common one for ease of access **[46] [47]**

Table 9: Brief comparison between solution methods benefits and drawbacks for Remote Access policy

4. 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.

Method	**Benefit**	**Drawback**
Updating OS of the raspberry pi holding the database	Ensures that security patches are up to date **[16] [48]**	Can have incompatibility issue with existing application **[49]** Can lead to chance of loss of data during update **49]** Can lead to introduction of bugs into the system **[49]** Can lead to higher consumption of power or storage space **[49]**
Not using default credentials on the raspberry pi holding the database	Ensures malicious actors can’t easily gain access to device**[15][16] [48]**	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 **[46] [47]**
Setting up firewalls on the raspberry pi holding the database	Ensures malicious actors can’t easily gain access to device **[16] [48]**	Needs to ensure only certain devices can gain access through the firewall which requires knowledge regarding firewall setup on raspberry pi **[50]**
Setting up VPN channels for raspberry pi to use when communicating with its	Ensures malicious actors can’t access or modify data being passed between the device and its	Causes in overhead in data transfer which slows down data

sensors (like peer to peer)	sensors and actuators due to encryption **[16]**	transmission rate **[41]**
Setting up plugins (like Fail2ban [16] **) on the raspberry pi holding the database to detect brute force attacks**	Ensures brute force attack on device can be prevented **[16]** **[48]**	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)	Ensures that malicious actors don't tamper with the device or its SD card **[16]**,	May require additional expense (like cost for buying cage to keep it, ensuring SD card can't be removed, etc.**[16]** **[51]**) May require placing it in certain locations which may impact rate of data transmission and coverage

Table 10: Brief comparison between solution methods benefits and drawbacks for Raspberry pi Security policy

V. Conclusion:

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

After this, a risk analysis has been performed on the 4 most critical risks faced by the system, where Delphi method **[1]** had been 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 has been later utilized to accurately rank the risks.

[**Note**: These had been linked with tables to explain what each of the values assigned in likelihood, impact, effectiveness and relative costs meant for better understanding and appreciation of the values used to create the risk ranking.]

This, in turn, has been 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 were later utilized in the implementation section where possible technologies and controls to implement the policies had been discussed, along with their benefits and drawbacks.

Thus, using all of this information the following list of recommendations has been 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 use the latest communication technology (like mMTC, NB-IOT, etc.) alongside having simple encryption, using the best practices for data queuing and compression protocols (like AMQP, MQTT, CoAP), etc.,

- Ensure that adequate measures (like video, paper documentation and simulated test runs of various, common 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 who to contact and the ways to defend against the attack,

- Ensure that the Caregiver control panel is properly protected (i.e. by setting up VPNs, by ensuring caregivers use strong credentials and update 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.)

VI. References:

[1] A/Prof. 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] A/Prof. 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] Cicirelli, Grazia, et al. "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] A/Prof. 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] 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).

[23] 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).

[24] A/Prof. P.Branch, private communication, Apr. 2023

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

[26] Wikipedia, "Zigbee," *Wikipedia*, Mar. 31, 2023. https://en.wikipedia.org/wiki/Zigbee (accessed May 19, 2023).

[27] 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).

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

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

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

[31] R. Soua, M. R. Palattella, A. Stemper and T. Engel, "Enhancing CoAP Group Communication to Support mMTC Over Satellite Networks," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6, doi: https://doi.org/10.1109/ICC40277.2020.9148784 (accessed May 19, 2023).

[32] L. Dineshwori, “5G mMTC: Challenges and Solutions | Profit From IoT,” *Profit From IoT | IoT India*, Sep. 06, 2019. https://iot.electronicsforu.com/content/tech-trends/5g-mmtc-challenges-and-solutions/ (accessed May 19, 2023).

[33] RF Wireless World, “Advantages of Z-wave | Disadvantages of Z-wave,” *Rfwireless-world.com*, 2012. https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-z-wave.html (accessed May 19, 2023).

[34] 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).

[35] 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).

[36] 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).

[37] 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).

[38] 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).

[39] 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).

[40] 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).

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

[42] 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).

[43] 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).

[44] 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).

[45] 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).

[46] 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).

[47] 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).

[48] 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).

[49] 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).

[50] 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).

[51] 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).