DESIGN AND ANALYSIS OF SECURE SMART HOME FOR ELDERLY PEOPLE

Mayada Elsaid, Sara Altuwaijri, Nouf Aljammaz and Anees Ara

Computer Science Department, College of Computer & Information Sciences,
Prince Sultan University, Riyadh, Saudi Arabia

ABSTRACT

Internet of Things (IoT) technology is used to enhance the safety of the elderly living in smart home environments and to help their caregivers. The daily behaviour of the elderly people is collected using IoT sensors and then evaluated to detect any abnormal behaviour. This research paper analyzes the smart home based anomaly detection system from a security perspective, to answer the question whether it is reliable and secure enough to leave elderly people alone in their smart homes. In this direction comparative analysis of literature is done to identify the potential security breaches on all layers of an IoT device. Further, this paper proposes a secure smart home model, built using Cisco Packet Tracer to simulate a network of IoT devices in a smart home environment. Consequently, a list of security countermeasures is proposed to protect the IoT devices from the identified attacks. .

KEYWORDS

Cyber physical systems, anomaly detection system, intrusion detection system, secure smart home, IoT.

1. INTRODUCTION

Smart homes are those built with automation to control appliances and monitor activities. One of the primary goals for smart homes is to guarantee comfort, control, and safety for the home residents, so smart homes accustom to user behaviour. To improve the safety of the elderly their daily behaviour is collected using IoT sensors and then modelled to detect any abnormal behaviour [2].

Anomaly Detection System is a system that identifies both network and computer interruptions and abuse by observing the system's regular behaviour and deciding if other behaviour is ordinary or atypical[1]. Internet of Things (IoT) is the expansion of Internet network into physical regular devices. These devices are connected with each other over the Internet, and they can be controlled and monitored remotely. IoT is often also referred to as cyber-physical systems.

The basic architecture of IoT devices based anomaly detection system consists of four layers: Perception Layer, Network Layer, Processing Layer and Application Layer. Perception layer comprises of different sensors, for example, infrared, RFID, and QR code for collecting data about the environment such ad pressure, humidity, and temperature [11]. These sensors collect the data to send it to the next level, while actuators receive control commands to perform specific actions. Network layer comprises of network communication software which is in charge of

DOI:10.5121/ijdps.2019.10601

transmitting data procured from the sensors to different layers. Internet layer includes the data aggregation, measurement, and control. The processing layer, called middleware layer, breaks down, stores and processes a tremendous amount of data. Numerous advances like cloud computing and big data processing work in the processing layer. These are the edge of IT systems. All needed pre-processing and analytics before entering the data center is done here. It's the stage of analysis, management, and storage of data. Lastly, application layer gives the services to the user according to his necessity. However each of these layers is prone to a set of potential attacks.

1.1. Research Objective

The evaluation of real-life sensor data obtained from elderly people's households using movement, windows, doors and pressure sensors can then help detect irregularities in the sensor data. Such smart home tools that help identify and filter unexpected events do not simply use rules; they use statistical analysis and advanced machine learning methods to collect data from internet-connected home devices and store it on a cloud. Whether it is used in simple reminder systems or prompting systems that urge users to take a necessary action in response to an alarm, anomaly detection systems play a major role in smart homes where elderly people live.

For instance, one approach to monitor activities in order to find out the temporal, spatial, or behavioural anomalies is graph-based. A network graph shows the activities and their durations for a person and stores it for comparisons. If unusual trends occur, such as when a resident forgets the appropriate pattern of activities, doctors can guess whether a person is at the stage of forming cognitive disabilities[2].

Although advances in wireless sensor systems have empowered the observing of day by day activities of elderly people, many cyber-security attacks are expected as a result for these IoT systems being connected to the Internet [3]. From having the stored data disclosed to being hijacked and controlled remotely, these anomaly detection systems are not very reliable considering the multitude of possible security breaches they are exposed to.

Therefore, this research aims to find out if the anomaly detection devices and sensors are secure enough. The answer will determine whether it is safe to leave elderly people alone in a smart home with anomaly detection systems recognizing and reporting alarm situations.

The contributions of this paper are as follows:

1. We present a comprehensive literature review about the anomaly detection systems in elderly remote monitoring systems
2. We propose a secure smart home architecture model to simulate a network of IOT devices applicable in smart environment.
3. We highlight the recommendations for the counter measures to protect the IOT devices from some list of identified attacks.

The organisation of the paper is described as follows: section 3 comprises of the related work, section 4 discusses the proposed secure smart home architecture model, the section 5 highlights the recommended security countermeasures and open research issues and finally section 6 concludes the paper with some future directions.

2. RELATED WORK

In [1], the authors described how smart homes can promote elderly people with better health-care and social support services. They found that elderly people have a positive attitude towards the smart homes implementations[4]. Moreover, elderly people were interested in the health monitoring system which can lead them to live independently. However, at the same time, they were having some concerns about the privacy of their data and the security provided by the smart homes [5]. The researchers in [5] concentrated on answering the question whether the smart-homes really have an influence on the elderly quality of life. Smart homes have helped elderly people to reduce the feeling of loneliness, helped them remembering their medicines and daily tasks, such as brushing their teeth and drinking water. On the other hand, Lê and Barnett in [6] said that elderly people shouldn't live in smart homes because of financial accessibility, acceptance and technical accessibility. Moreover, smart homes require a lot of technologies which are costly. Also, elderly people have a limited experience in dealing with advanced technologies. Boyanov & Minchev [7] supported Lê and Barnett [6], they stated that although smart homes have many advantages, reliability of sensors, surveillance systems and misuse of personal or confidential information should be taken into account. Moreover, data could be modified in communication media by the attacker and sent to the cloud. Also, sensors are vulnerable to have attacks which can phase out the entire system. Finally, the attacker could read the data which is against the privacy.

In [8] the authors explained how they will use a graph-based approach using the GBAD tool to detect anomalies of elderly patients living in smart homes without interfering with residents' daily activity, and to reduce the cost of healthcare associated with such situations [8]. The authors defined the anomalous behaviours to be the temporal, spatial, and behavioural anomalies. They proposed two hypotheses which claim that a graph-based approach can be reliable enough to detect anomalies of elderly patients in smart homes and discovered anomalies are possible syndrome of impairment in their cognitive abilities [8]. However, the aim of these anomaly detection systems is to help the patients' caregivers and clinicians monitor elderly people and raise the patient's' independence to be able to perform the daily tasks and routine safely. These systems are set up by installing sensors all over the home to gather data about the patients' activities without interfering with their routines. The authors' methodology was to collect data, convert it into graphs with nodes and edges to display temporal and spatial information about the patients, and finally use these graphs or patterns to clearly analyse their situations and discover anomalies. They concluded to the result of detecting anomalies from three participants who mostly had a temporal anomaly. Temporal anomaly is when someone takes longer or shorter time to carry out a specific task than the usual duration. Moreover, these may be potential indicators for having a decline in cognitive health [8].

According to Rao & Haq in [9], IoT is widely functional to public activity appliances like smart homes. User security ought to be guaranteed by preventing illegal access since when an IoT layer is compromised, attackers can without a lot of effort get access to the whole system through that compromised node[9]. In addition, viruses, malicious software, and attackers can interfere with data and information integrity leading to risk for the whole IoT environment. In practical applications such as emergency, rapid response and traffic control, information collection must be fast and accurate. The research identifies the potential threats that may occur in all IoT layers. Perception layer attacks include Forged node insertion, malevolent code insertion, and Hardware Jamming. Some security Challenges in the Network Layer are Denial-of-Service (DoS) attack, Sinkhole attack, and Man-in-Middle attack. Attacks on the processing layer include Primary infrastructure security, Data security in cloud computing, Threat to shared resources, and Attack on Virtual Machines. Engineers attempt to build up an application safe however its security stays under threat because of lower layers of IoT which is likewise the responsibility of the provider of the service[9]. In Application layer, attacks are malevolent code assaults, Software defenselessness, and Phishing attacks.

Arwa et al in [9] discussed how fog computing is a promising technology for distributed computing providing many services to the edge network, yet faces lots of security and privacy problems in devices. Since IoT devices have limited resources regarding storage, battery, and processing capabilities, fog computing is new service that will provide a new solution for handling these real-time requirements which are not completely achieved by cloud computing [15]. The authors in [9] explained how fog computing could also address many security and privacy issues as in the cloud computing. Because of the fog's service of filling the gap between the resource-constrained devices and the clouds or remote data centers, and due to its characteristics like supporting mobility, decreasing latency, location awareness, heterogeneity, and large scalability, many security issues could be introduced. The researchers summarized the major challenges of security and privacy in IoT environments such as encryption, trust, red node detection, confidentiality, access control, intrusion detection, data protection, and others[9]. Authentication is affected in IoT devices because of the lack of processing and storage capabilities in end devices. Such expensive computations and cryptographic operations are hard to be accomplished in IoT devices. However, trust is a critical challenge in the IoT devices due to the integration of sensors and actuators. Furthermore, some malicious nodes in the IoT environment could pretend to be a legitimate one and may misuse collected data or send wrong data for malicious purposes. Also, privacy is an inevitable challenge on remotely accessed devices. Regarding the IoT devices' inability to perform cryptographic operations on data before transmission, users' location and usage information is all vulnerable to attackers.

Another privacy issue is when attackers are able to expose and extract data that are meaningful when analyzed. Pattern-of-usage analysis violates the users' privacy when information generated by IoT devices is accessible by adversaries[10]. Furthermore, access control is an important technique to ensure no malicious access can perform or generate malicious commands to any of the interconnected and resource-constrained devices. Intrusion detection on the other hand, is another challenge in widely interconnected mobile environments. IoT environment makes it hard to discover the misbehaviour or misuse of data. Moreover, data protection is a challenge in limited resource devices since data cannot be analyzed or processed in such a level. Data in IoT devices is sent to the cloud level for further analysis and hence, should be protected before and after the processing in the cloud. In order to improve their security, a new certificate revocation scheme is proposed in IoT built on fog computing [9].

The authors in [9] compared the most common methods for transmitting revocation data that is the Certificate Revocation List (CRL) with the OCSP (Online Certificate Status Protocol). CRL contains the black-listed certificates' serial numbers[9]. So, a client must download the list to know whether an intended certificate is in the list to be trusted or not. Similarly, the OCSP is a protocol that is used to get information about any digital certificate status. A client needs to submit the certificate's serial number to get a confirmation about the certificate if it has no issues. However, the authors proposed a solution to an efficient distribution of the certificate revocation information. The proposed scheme consists of the Certificate Authority (CA), back-end cloud, fog nodes, and IoT devices. The scheme uses a bloom filter in the fog nodes that stores the authorized certificates' serial numbers confirmed by a CA. After receiving a signed and updated CRL from the CA, the clouds forward them to the specific fog nodes. Then, a bloom filter that maps revocation information is created by the fog nodes, and then distributed to the intended IoT devices to verify the signature and store the information. To use it, an IoT device checks the bloom filter before any communication happens. If the certificate of the indented node to communicate with is not in the filter, the communication may begin. Security enhancement is provided by keeping the filter up-to-date, to avoid the risk of malicious use[9].

In the recent years, smart homes have seen a tremendous rise due to the technology addiction. Smart homes have invented to improve the quality of life for all people, especially ordinary nondisabled people. The idea of smart homes is to save energy, control the lights, control heating and air condition, door locks and coffee makers while people are comfortable. However, people with disabilities will not be able to enjoy the benefits of smart homes devices. Controlling devices while you are setting using smart technology is a good benefit for people who are physically disabled and older persons. To solve the problem of disabled people, the researchers in [12] discussed a control system based on smart home appliance for physically disabled people. In this paper [12], researchers presented a system that uses smart plugs, smart cameras and digital assistant, such as Google Assistant, Google Home, Amazon Alexa, or Apple Siri to take the orders by capturing the physical disabilities person's voice. Many manufactures have invented products that can interact with digital assistant, the proposed system in [12] will program those devices to let them act based on the voice commands.

Additionally, in [13] the researchers studied threats, security requirements and open research challenges of smart home-smartphone systems. Smart homes become so popular in many people' life. Controlling the home with a click on a smartphone becomes an aim to a lot of people. However, data confidentiality, privacy and financial loss are the main concern. Existing smart homes have much vulnerability and many attacks have occurred on these systems. Therefore, these systems' security is a major problem that needs to be analysed and solved. The researchers in [13] have addressed threats that the systems have. Threats have categorized into two categories, the first category is internal system threats, such as failure of home devices, power and internet malfunction, software failure and confidential data leakage. External system threats is the second category, it has denial of service, malicious injection, eavesdropping and man in the middle as threats. With the existing of all these threats, some security requirements have been suggested to increase the security level and minimize the threats exposure. Data encryption, network monitoring, user authentication could reduce the exposure of external threats while devices availability, physical protecting and devices authentication will play a major factor in decreasing internal threats.

3. PROPOSED SECURE SMART HOME MODEL FOR ELDERLY PEOPLE

3.1. Proposed Approach

The proposed research is designed from a qualitative point of view where a case study is evaluated to identify how safe and secure can the anomaly detection systems be for the elderly people.

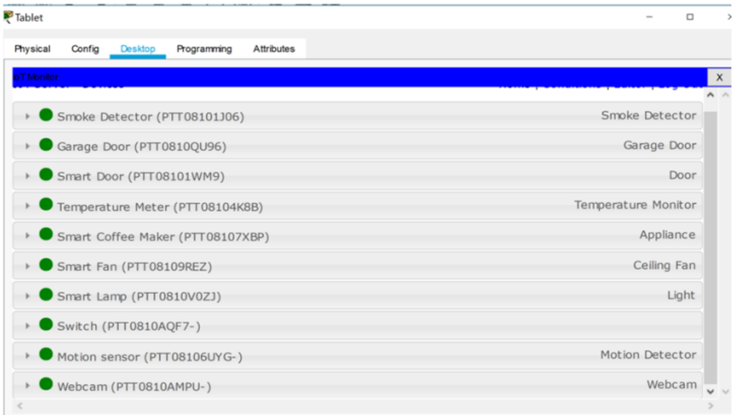
3.2. Adversary Model

Many hospitals use anomaly detection systems in smart homes to monitor elderly patients and track their health. These smart homes use the concept of the internet of things (IoT). Data collected from the smart home are sent to the cloud for detection of abnormal behaviour that is reported to the hospital. Since these systems are Internet connected, they are accompanied by multiple risks and threats that make smart homes not safe enough to leave elderly people alone.

Due to smart homes vulnerability to these Internet-based attacks, an elderly person could die when an adversary stops sensors, prevents data from reaching the hospital, or sends false information. A patient could need a treatment, but the hospital is not aware, or the hospital could give the patient an unneeded treatment in response to fake data it received about the patient. In the smart home environment there could be a possible list of attack on sensors network such as denial-of-service (DoS), sinkhole, man-in-middle, radio frequency identification (RFID) authorized access, gateway, and RFID Spoofing and also they can be extended to the cloud security risks with exposure of data by unauthorized users.

3.3. Smart Home System Description

The system of a smart home system is made of smart devices that have sensors to record activities of the elderly home residents. For instance, activities such as opening a smart door can indicate time spent in the bathroom or kitchen, or turning on a smart light switch can indicate waking up and sleeping hours (Figure 1). After sensing, smart devices send the real time data collected by sensors to the cloud to be compared against models of normal user behaviour. Whenever an abnormal behaviour is detected, the caregiver and hospital of the elderly person are notified.



● Smoke Detector (PTT08101J06)	Smoke Detector
● Garage Door (PTT0810QU96)	Garage Door
● Smart Door (PTT08101WM9)	Door
● Temperature Meter (PTT08104K8B)	Temperature Monitor
● Smart Coffee Maker (PTT08107XBP)	Appliance
● Smart Fan (PTT08109REZ)	Ceiling Fan
● Smart Lamp (PTT0810V0ZJ)	Light
● Switch (PTT0810AQF7-)	
● Motion sensor (PTT08106UYG-)	Motion Detector
● Webcam (PTT0810AMPU-)	Webcam

Figure 1.The smart devices that are controlled by the tablet

3.4. List of Anomalies in Smart Home

- Unusual action (movement in abnormal time) - A circumstance of an unordinary action is the point at which the resident is sitting in the kitchen or the lounge around evening time for certain hours, yet is expected to be at sleep.
- Wakeful evenings are frequently an indication of some issue.
- Unusually long action - Unusually long term of an action may happen when the resident falls or loses awareness.
- Unusually short action - Unusually brief length of an activity may happen for example around evening time, when the resident gets up significantly earlier than expected, for example he is normally resting till 7:30am however one day awakens at 2:40am. This may demonstrate medical issues.

3.5. Configuring the Simulation of the case study in Cisco Packet Tracer

The smart devices connected in the smart home environment are:

- Smoke detector to detect an increased level of smoke.
- Garage door to detect entry to and exit from the house.
- Smart door to calculate duration spent in a room.
- Temperature meter to measure temperature.
- Smart coffee to check when is coffee made.
- Smart fan to check when a person is active in a room or to cool a room when necessary.
- Smart Lamp to show sleeping and waking hours.
- Switch to show sleeping and waking hours.
- Motion sensor to indicate movement in a particular room.
- Webcam that records videos to be viewed when necessary.

All devices are using the IoT home gateway as the media path that connects the smart devices. The home gateway also provides automatic addressing to its wirelessly connected devices. Moreover, a tablet is connected to the home gateway as means for remote access, control, and monitoring to the other connected smart devices. Some sensors and actuators are connected to MCU-PT. The home gateway depends on the remote-control API that is programmed on the MCU-PT to get the sensor's status (Figure 2). On the other side of the home gateway is the connection to the cloud cluster, which is consisted of the switch and cloud server. Last, ISP router connects the hospital PC to the cloud so that the hospital is alarmed upon any detected anomaly (Figure 3).

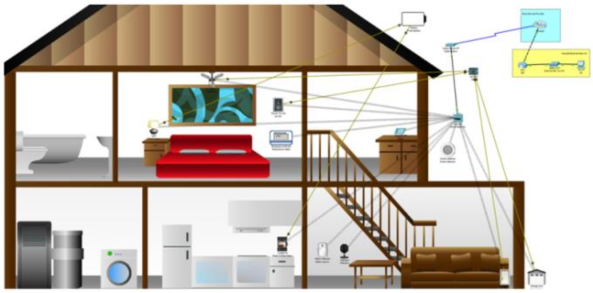


Figure 2. Smart home model using Cisco Packet Tracer

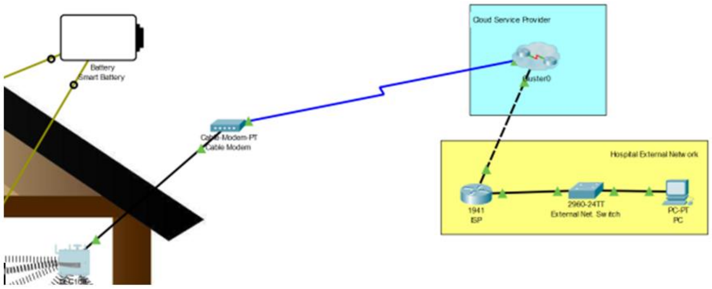


Figure 3. The home gateway is connected to a cloud service provider that connects the home gateway to the hospital's server

3.6. Security Concerns

Based on literature reviews where several threats are identified, the network layer and processing layer of devices are at high risk, therefore, they will be the main concerns of this research.

Network communication software transmits the collected data from the sensors to be stored on the cloud and to the hospital’s end devices to alarm the hospital. Confidentiality, integrity, availability of the data being transmitted are at risk [11]. While the data is transmitting, it is vulnerable to countless attacks, such as denial-of-service (DoS), sinkhole, man-in-middle, radio frequency identification (RFID) authorized access, gateway, and RFID Spoofing.

1. Denial-of-Service (DoS) attack, which prevents legitimate users from using the services of the system. DoS will block the data from being transmitted while sinkhole will drop the packets which supposed to go to the final destination.
2. Man-in-the-Middle attack that allows the attacker to monitor, control, and capture the communication between two devices. Man-in-middle will appear between the nodes to extract the desired information.
3. In RFID authorized access, tags are reachable to anyone since the security is low in tags. Therefore, tags can be affected easily.
4. RFID Spoofing attack, attacker concentrates on collecting the desired information from RFID tags in RFID signals. Using the actual ID, the hacker will be capable of transmitting his own data and taking full sensor control.

Processing layer or middleware layer is responsible for analyzing, processing and storing the collected data. Cloud computing is a technique used in the processing layer. Application security, primary infrastructure security, data security in cloud computing, threat to shared resources, attack on virtual machines and third-party relationship are considered attacks to the processing layer. In general, the attacks exist because of insecure network services, insecure data transfer and storage, insufficient privacy protection and access control on cloud, and lack of encryption.

1. Application Security: Is application security the sole obligation of the cloud provider or the obligation of the application proprietors – and accordingly, applications ought not to be deployed in the cloud because of security dangers or except if security is legitimately ensured.
2. Infrastructure Security: In primary infrastructure security, developers try to build secure applications. However, the security will be always week because of the lower layers of

IoT. Data is stored as plain text with means it is not encrypted. Therefore, it is the service provider responsibility to limit the access and ensure the privacy.

3. Virtual Environment Security: Virtual machines is targeted, since it will shut down the whole environment when an attack happen.
4. Threat to shared resources: Because of the cloud's nature as a shared resource, it is prone to breaches in protecting identity, maintaining privacy, and controlling access.
5. Cloud deployed web service security: A third party web service component is provided by platform as a service (PaaS), and because more than one service is binded, the security risk is increased.

3.7. Recommended Security Countermeasures

Based on the security concerns list in section 4.6 we list out the some of the recommended security countermeasures for the secure data collection and transmission at network and processing layers.

3.7.1. Network Layer

Data privacy: unauthorized access to any of the IoT devices can be avoided by using cryptographic techniques, authentication mechanisms, security standards or protocol, and encryption tools.

Routing Security: A basic concept to understand how Internet works, is by understanding the routing. Transmitted packets from end-to-end need enough information to be on routers to be forwarded to the next destination. So, it’s vital to secure the routing between any two nodes in the IoT environment. Any attack on routing security may access the routing tables and modify data stored on them to write deceptive information and misleading paths. Such an attack can introduce other major security attacks on the network layer, such as man-in-the-middle, traffic redirection, and router DoS.

Secure Shell Cryptography (SSH): SSH is a cryptographic protocol in network layer that ensures secure operations over the network. It provides a lot of options for establishing a strong authentication. This enhances the integrity of communication between to devices. However, data integrity is considered major concern in IoT environments, and more specifically, in anomaly detection systems.

Secure Real-time Transmission Protocol (SRTP): According the high level of sensitivity that anomaly detection systems have, instant communication and transmission of data is a key factor to the accuracy of the system. SRTP is an extension protocol of Real-time Transmission Protocol, which uses AES as the default cipher. It provides the same functionality of RTP while enhancing its security of unicast and multicast messaging. It’s critical to have both instant and secure communication between the levels in smart homes of elderly patients to ensure their health safety and privacy.

P2P Encryption: Point-to-point encryption security standards ensure securing the data stream between nodes, and aims to minimize the exposure of sensitive data in critical environments. For example, in healthcare fields, it’s very risky to lose or have wrong data collected. Such environments are connected with many alarms and actuators that may either act wrongly, or be out-of-service when needed.

Access Control Lists (ACLs): Setting up strategies and authorizations of who can access and control the IoT framework guarantees the privacy of the information. ACLs can block or permit traffic and give or block access to requests from diverse users inside or outside of the system.

3.7.2. Processing Layer

Encryption to Secure Classified Information: encryption, encryption is applied to secure classified information. By doing this technique, the data will be encrypted while it is transmitting and stored. We have many encryption techniques that defeats side channel attack and secure the IoT environment.

Fragmentation Redundancy Scattering: Data fragmentation redundancy scattering is basically separating the data into many fragments and stored them in various serves. The data now becomes meaningless since each single fragment does not represent anything, so the risk is minimized.

Web Firewall Applications: Web firewall is able to identify the threats and block them, so the threats will be blocked from coming into the IoT environment.

Virtual Identity (VID) Framework: The user sends a request of VID to service provider, who requests client's data, for example, name, age, sex, phone, capability. The VID is then given to the user. The supplier can issue a client more than one VID, which isn't connected to another. It stores the data of a user along a VID. The user can only access the system to utilize applications with his VID. This ensures privacy by preventing unauthorized access.

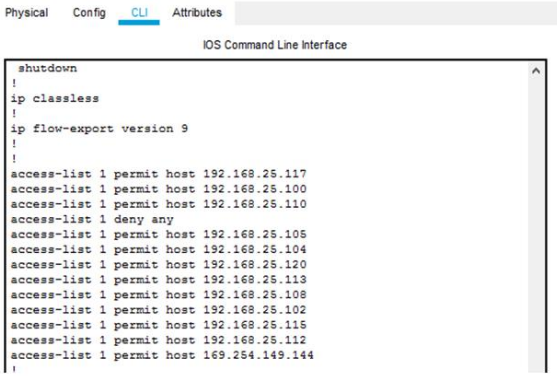
Software Defined Networking (SDN): SDN-based cloud conveys new opportunities to overcome DDoS attacks in cloud computing environments. Instead of every node in the system making its very own sending choices, a centralized software-based controller is in charge of ordering subordinate nodes on the way traffic is forwarded.

3.8. Implementation of ACL in Proposed Smart Home Environment using CISCO Packet Tracer

In this section, based on the above recommended list of security countermeasures, we implement Access Control Lists in a simulated smart home environment using CISCO packet tracer. The ACL is used to address the authentication and authorization issues in an IoT based smart home environment. The details of the implementations are as follows:

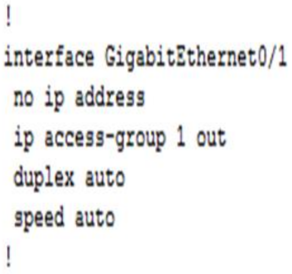
ACLs implementation: Access control list “ACL” is a list of permissions that specifies that the device is allowed to send data or not. ACL is implemented in the router to specify which data to be passed. In addition, ACL is used to make sure that only authorized sensors as discussed in Figure 1 can send data to the cloud to avoid data integrity. ACL consists of a list of Internet protocol “IP” address and specify whether the IP is granted to send or not. Moreover, all the sensors IPs are allowed, and any other IP address is denied (Figure 4).

The list is assigned to the interface GigabitEthernet0/1 which is the interface that is connected to the cloud service provider. The list is applied as an outbound access list (Figure 4) which means that packets will be routed to the interface and then processed through the access list before being queued (Figure 5).



```
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit host 192.168.25.117
access-list 1 permit host 192.168.25.100
access-list 1 permit host 192.168.25.110
access-list 1 deny any
access-list 1 permit host 192.168.25.105
access-list 1 permit host 192.168.25.104
access-list 1 permit host 192.168.25.120
access-list 1 permit host 192.168.25.113
access-list 1 permit host 192.168.25.108
access-list 1 permit host 192.168.25.102
access-list 1 permit host 192.168.25.115
access-list 1 permit host 192.168.25.112
access-list 1 permit host 169.254.149.144
!
```

Figure 4. List of Access Control



```
!
interface GigabitEthernet0/1
 no ip address
 ip access-group 1 out
 duplex auto
 speed auto
!
```

Figure 5. Applying the list to the interface

The above implementation of the ACL is an extract from the recommended security countermeasures. Due to the limitations of the simulation environment on packet tracer, we were able to perform few experiments. But in future we plan to extend our work in an real time arduino based smart home environment, were the flexibility of secure smart home architecture and design is expected to be high.

4. OPEN RESEARCH ISSUES

There are several open research issues related to the IOT based smart home environment for elderly monitoring systems. With the continuous growth and demand of the IoT devices and its applicability in various healthcare environments, the need for concrete privacy and security design and architecture, protocols and schemes is paramount important. As discussed in literature review, several researchers are publishing context related security protocols. However, there are very few research which address an holistic approach that addresses the issues problem related to identity management of the IoT devices; risk assessment methodologies in remote health monitoring systems; information control flow approaches in cloud enabled environments; and security management approaches, like patching, updates on IoT devices is not included. There is a need for the integration of security in design and of secure software design process model in the development of smart connected homes. Moreover, there is a shortage of privacy by design measures in the smart home environment.

5. CONCLUSION

A smart home anomaly detection system is prone to several attacks that may cause it to malfunction and disrupt its purpose. However, by adding sufficient and suitable security defenses, attacks are not likely to occur. Therefore, in this paper we propose a comprehensive study related to various security concerns and provide recommendations for security countermeasures. We propose a sample case study and implementation of smart home environment on cisco packet tracer. Hence we conclude that if a smart home is well equipped with proper security defenses, it is safe to leave elderly people alone in the smart home with anomaly detection systems recognizing and reporting alarm situations. We highlight some open research issues for IoT based smart home environment. In future research we plan to explore the artificial intelligence-based algorithms/techniques applicable in detecting an anomaly in elderly patience monitoring systems.

REFERENCES

[1] Aran, O., Sanchez-Cortes, D., Do, M. T., & Gatica-Perez, D. (2016, October). "Anomaly detection in elderly daily behavior in ambient sensing environments". In International Workshop on Human Behavior Understanding (pp. 51-67). Springer, Cham.

[2] Paudel, R., Dunn, K., Eberle, W., & Chaung, D. (2018, May). "Cognitive Health Prediction on the Elderly Using Sensor Data in Smart Homes". In The Thirty-First International Flairs Conference.

[3] Hoque, E., Dickerson, R. F., Preum, S. M., Hanson, M., Barth, A., & Stankovic, J. A. (2015, June). "Holmes: A comprehensive anomaly detection system for daily in-home activities". In 2015 International Conference on Distributed Computing in Sensor Systems (pp. 40-51). IEEE.

[4] Hsu, Y. L., Chou, P. H., Chang, H. C., Lin, S. L., Yang, S. C., Su, H. Y., ... & Kuo, Y. C. (2017). "Design and implementation of a smart home system using multisensor data fusion technology". Sensors, 17(7), 1631.

[5] Pal, D., Triyason, T., & Funikul, S. (2017, December). Smart homes and quality of life for the elderly: A systematic review. In 2017 IEEE International Symposium on Multimedia (ISM) (pp. 413-419). IEEE.

[6] Lê, Q., Nguyen, H. B., & Barnett, T. (2012). "Smart homes for older people: Positive aging in a digital world". Future internet, 4(2), 607-617.

[7] Boyanov, L., & Minchev, Z. (2014). "Cyber Security Challenges in Smart Homes". Volume 38: Cyber Security and Resiliency Policy Framework,IOS Press Ebooks

[8] Paudel, R., Eberle, W., & Holder, L. B (2018). "Anomaly Detection of Elderly Patient Activities in Smart Homes using a Graph-Based Approach". In: Proceedings of the 2018 International Conference on Data Science, pp. 163–169. CSREA .

[9] Rao, T. A. "Security Challenges Facing IoT Layers and its Protective Measures". International Journal of Computer Applications, 975, 8887.

[10] Lin, H., & Bergmann, N. (2016). "IoT privacy and security challenges for smart home environments". Information, 7(3), 44.

[11] Ara, A., Al-Rodhaan, M., Tian, Y., & Al-Dhelaan, A. (2015). "A secure service provisioning framework for cyber physical cloud computing systems". arXiv preprint arXiv:1611.00374.

[12] Mtshali, P., & Khubisa, F. (2019, March). "A Smart Home Appliance Control System for Physically Disabled People". In 2019 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-5). IEEE.

[13] Karimi, K., & Krit, S. (2019, July). "Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges". In 2019 International Conference of Computer Science and Renewable Energies (ICCSRE) (pp. 1-5). IEEE.

[14] Adiono, T., Tandiawan, B., & Fuada, S. (2018). "Device protocol design for security on internet of things based smart home". International Journal of Online Engineering (iJOE), 14(07), 161-170.

[15] Sultana, S. N., Ramu, G., & Reddy, B. E. (2014). "Cloud-based development of smart and connected data in healthcare application". International Journal of Distributed and Parallel Systems, 5(6), 1.

AUTHORS BIOGRAPHY

Mayada Elsaid is a senior Software Engineering (Cyber Security) student in Prince Sultan University. She is an IEEE member and chair in IEEE-Student Chapter. Her areas of interest and research are cyber physical systems security and IoT. She has presented security and business process management papers in local conferences and research forums.

Sara Altuwaijri is a bachelor student, majoring in Software Engineering (Cyber Security) at Prince Sultan University. She's currently leading two clubs in the university by arranging events and bootcamps that are related to many topics of computer science. She's the president of Edtech club and the Vice Chair if IEEE chapter at PSU. She received nano degrees in Artificial Intelligence and Self-driving cars. Her research interests include security & privacy in IoT and cyber physical systems.

Nouf Aljammaz is a senior Computer Science (Cyber Security) student focused on improving facility security through diligent approach and sense of personal responsibility. Resilient individual trained in security. Her research interest includes security domains related to risks management, optimization techniques relates to asset protection and threat minimizations.

Anees Ara received her BSc in Computer Science and MSc in Mathematics with Computer Science from Osmania University, India in 2005 and 2007 respectively. She has received her PhD degree from King Saud University and she is currently working as Assistant Professor at College of Computer and Information Sciences, Prince Sultan University, Kingdom of Saudi Arabia. She is an active member of Security Engineering Lab, Prince Sultan University, KSA and IEEE, computing society. In addition, she is an active reviewer of international journals. Her research interests are broadly divided into privacy and security, which are related to cloud computing, cryptograph, smart environment, cyber physical systems and big data.