IoT for smart homes

Chapter · September 2019

DOI: 10.1049/PBCE122E_ch7

5 authors, including:

Anindya Nag
TUD Dresden University of Technology
160 PUBLICATIONS **5,628** CITATIONS
SEE PROFILE

Md Eshrat E Alahi
Walailak University
84 PUBLICATIONS **3,017** CITATIONS
SEE PROFILE

Nasrin Afsarimanesh
Curtin University
61 PUBLICATIONS **1,331** CITATIONS
SEE PROFILE

Sumedha Prabhu
Chinese University of Hong Kong, Shenzhen
17 PUBLICATIONS **188** CITATIONS
SEE PROFILE

Chapter 7
IoT for smart homes

Anindya Nag[1], Md. Eshrat E. Alahi[1], Nasrin Afsarimanesh[1], Sumedha Prabhu[1], and Subhas Chandra Mukhopadhyay[1]

The usage of smart homes in real-time applications has been one of the state-of-the-art due to the quality of life they provide to the residing life. Internet of things (IoT)-based smart homes are booming in the market where a large number of IoT-connected daily used items are commercially available. These devices are used in the smart homes for ubiquitous monitoring of the different activities of the residing people. This chapter gives an overview of some of the smart devices available for IoT-based smart homes along with some of the research work done on IoT-based smart homes in the laboratory. This also showcases some of the sensors that have been used for biomedical applications and have the potential to be used in smart homes.

7.1. Introduction

With the advancement in science and technology, there have been many ways to improve the quality of life for human beings. The implementation of specific methodologies in terms of electronic assistance had been researched and worked upon to increase the longevity of human life. One of the most popular choices for this goal has been the implementation of smart homes [1], where people with ailment have been kept and taken special care. The importance of smart homes lies in the precise monitoring of the people regarding their day-to-day activities to figure out any abnormality in comparison to their normal life. Among the different types of specialized homes designed for monitoring people in commercial and research-based conditions, smart homes for elderly care has been a standout. In these specialized homes, sensors have been positioned at different locations to identify the activities and movements of the residential elderly people.

One of the biggest advantages of these homes is the automated monitoring system which makes it easier and efficient to keep a track of the minute changes happening in every individual's life. Figure 7.1 shows the schematic diagram of the operating phenomenon of a smart home [2]. It is seen that the sensors located in the

[1] School of Engineering, Macquarie University, Macquarie Park, NSW 2113, Australia

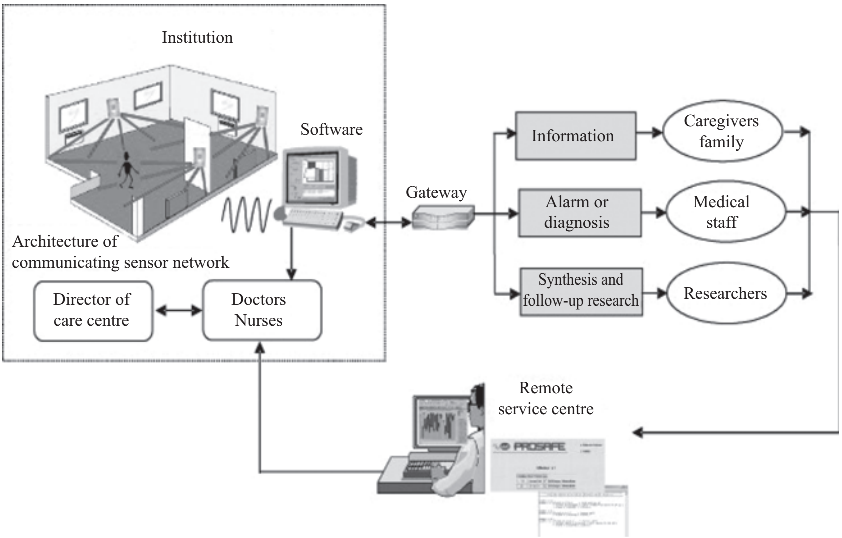


Figure 7.1 *Schematic diagram of the working phenomenon of a general smart home [2]*

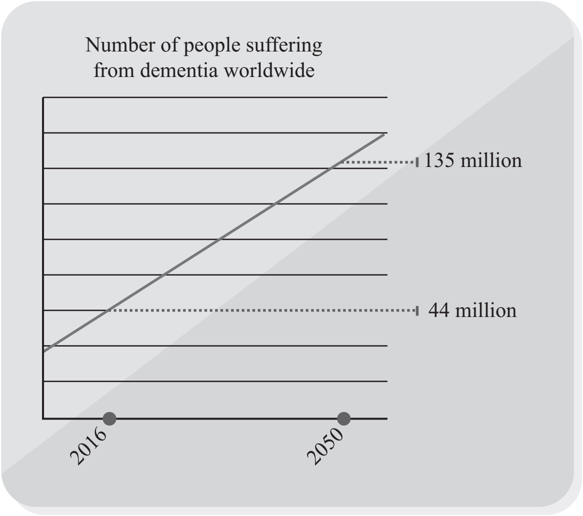


Figure 7.2 *Increase in the number of elderly people suffering from dementia between the years 2016 and 2050 [3]*

house form a sensor network in order to communicate among each other to send the signals to the monitoring unit via a gateway. The monitoring unit then immediately informs the medical staffs, family members or researchers depending upon the type of assistance required. This approach seems to be an effective way to significantly reduce the probability of casualties during an emergency. Figure 7.2 shows a fact of the increase in the number by a factor of 3 for the elderly people suffering from dementia between the years 2016 and 2050 [3]. As a result of these problems, researchers all around the world have been trying to come up with two solutions. First, smart devices are designed to monitor the specific activities of the elderly people. For example, smart beds, smart ovens and fall detectors are some of the devices that are installed in different locations of the house.

Second, these smart sensing devices employ Internet of things (IoT)-enabled technology to monitor and control the operations inside these homes in an easier and controlled manner. In this chapter, we will talk about some of the significant research work done on IoT-based smart homes. We will also talk about some of the IoT-embedded commercial smart sensing devices that are used in smart homes. Finally, we will also discuss some of the parameters that are being monitored along with their associated sensing systems in these specialized homes.

7.2 IoT-based smart homes

The usage of smart sensing devices in the specialized smart homes designed for elderly people have started since the last two decades [4,5], by the time sensors were available commercially to be used for ubiquitous applications. The sensing devices have been implemented in everyday items, forming a cognitive network for the individuals residing in the house to provide an environment for the people to have a happy and independent life. There are some established research works going on around the world that utilizes IoT-based smart sensing devices in these specialized care centres. Some of them are Gator Tech Smart House, University of Florida [6], Smart Community Alliance, Japan [7], KIDUKU, Japan and Ireland [8], Smart homes, UK [9], etc. The ultimate agenda of these projects is to monitor the normal and healthy lifestyle of elderly people residing in these houses. This section defines IoTs, their utilization in smart homes in integration with some of the commercial smart devices and finally some of the research work going on IoT-based smart homes in laboratory-based environment.

IoT is one of the most common concepts of things that are readable, controllable, addressable and locatable via internet in the twenty-first century. All the surroundings of our daily life can be associated with the Internet due to the growing faster computing and communication abilities. Figure 7.3 shows the schematic diagram of a smart home employed with different IoT connected utilities. IoT-based smart homes consist of several sensors, which are connected wirelessly to develop supporting distributed networks. Each IoT-enabled sensor node in the smart home includes three subsystems: (1) sensor subsystem for environment sensing, such as temperature, humidity and light intensity; (2) processing subsystem, consisting a microcontroller and integrated circuit to process the sensor data for computation and (3) a communication subsystem for exchanging the collected data between different sensors [10–15].

The traditional Wireless Sensor Networks (WSNs) offer specific applications which are mostly designed as a closed system; however, IoT-based applications are independent of specific applications [16] and are more focused to develop a

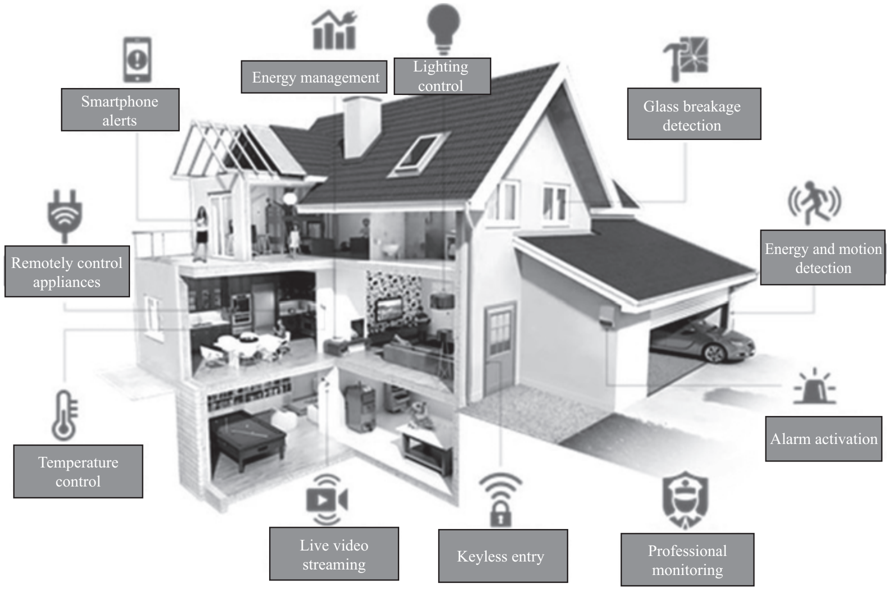


Figure 7.3 Schematic diagram of an IoT-enabled smart home depicting the employment of smart sensing devices in different utilities

large-scale WSNs infrastructure, which could support open standard. In most of the IoT-based smart home systems, the smart actuators and smart sensors are installed within the home environment to control and supervise its operations. It also incorporates smart devices to run the whole home smartly without the human direction. Some of the applications are home appliances, lighting, security cameras and alarm systems. These smart devices are connected to the local server via a wireless medium for data collection and analysis. One of the most significant issues is how securely the smart devices can send data to the appropriate destination. All the smart devices have constraints such as limited resources including power supply, memory, limited data processing capability and range of communication [17,18]. The following sensors are important to develop a smart home:

1. Fire/Smoke detector: Fire or smoke detector is one of the essential sensors to build a smart home and to protect the home from fire. The function of the smoke detector is to detect the first sign of fire or smoke almost as quickly as possible and keep the human lives safe. They always create alarm sounds to alert the inhabitants inside the home. Some of the detectors have notification system which can be sent to all the members of the home. The image of a commercial smoke detector that is used in smart homes is shown in Figure 7.4 [19].
2. Humidity detector: Leak sensor is used in a smart home to detect the water leakage in a supply unit. Moisture detection sensors can alert the people to leaks in home so they can fix the problem immediately avoiding any kind of damage. The sensor can be placed around water heaters, dishwashers, refrigerators,

Figure 7.4 Commercial smoke detectors used in smart homes [19]

Figure 7.5 Commercial humidity detector used in smart homes [20]

sinks, water pumps and anything at risk for water leakage. If the sensor detects unwanted water a notification is sent to the owner of the house, so they can check out the problem quickly and take the necessary actions. Figure 7.5 shows a commercial humidity detector that is used in smart homes [20].

3. Smart thermostat: The smart thermostat provides control over the heating and cooling in smart home – from any location. They are always useful to save money by monitoring the temperature and humidity inside and outside of the home. The temperature of a house changes due to the number of reasons and a smart thermostat can adjust the temperature based on behaviour and room usage. The ideal thermostats adjust the room temperature on a room-by-room basis to maintain the ideal temperature when any bodies are in the room and can change the temperature to an energy saving mode when no one is in the room. Figure 7.6 shows a commercial thermostat that is used in smart homes [21].
4. Motion sensors: A motion sensor detects motion and movement in an area. These sensors can alert immediately if there is any movement within the home, or if the doors or windows have been opened or closed. They can even turn the lights on and off as doors are opened and closed. These sensors work as an extra pair of eyes when nobody stays at home. These sensors are the first line of security for smart home break-ins; some sensors might be useful as they can detect when an intruder breaks a window. They always alert the owner by sending the notifications of potential intruders. They are also useful to save energy and can be connected to lighting or the thermostat to help control the energy usage in a room based on the occupancy of the room. Figure 7.7 shows the motion sensors that are used in smart homes [22].
5. Video cameras: The video cameras allow the owner to visually locate the positions of different people in the house with a smartphone.

Whether the owner is inside at home or at work and someone is at the house, the owner can always know and takes the immediate necessary actions. These devices are always useful to keep an eye on the potential intruders. Figure 7.8 shows a commercial video camera used in smart homes [23].

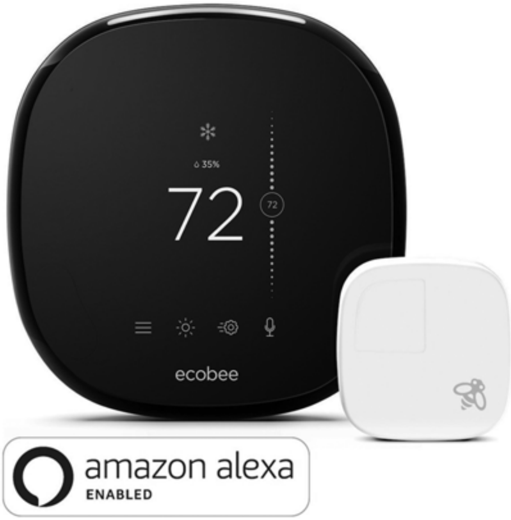


Figure 7.6 Commercial thermostat used in smart homes [21]

Figure 7.7 Motion sensors that are used in smart homes [22]

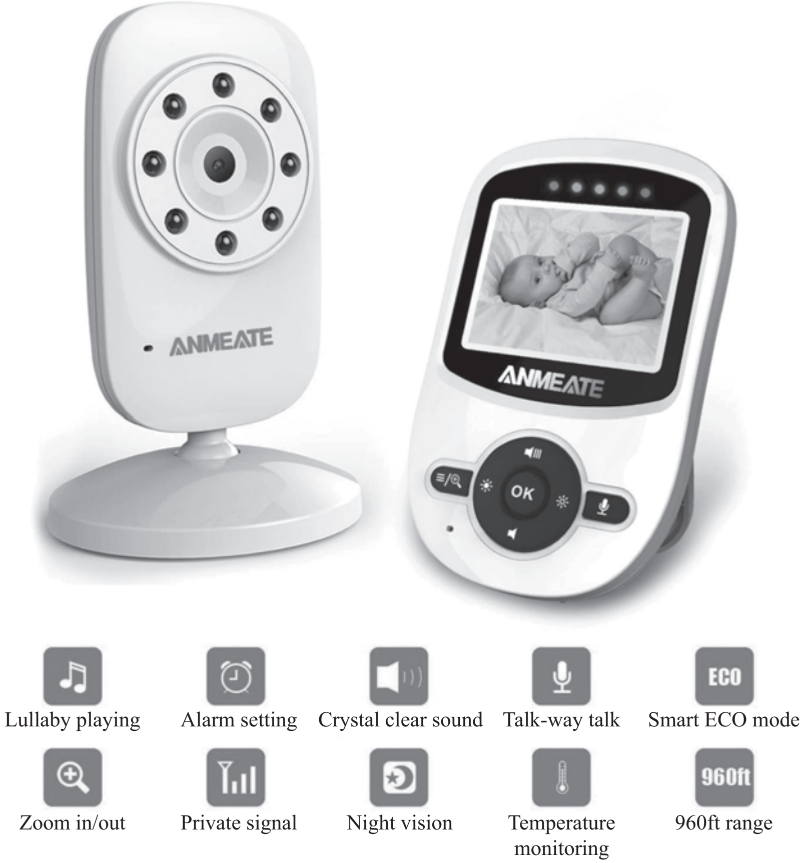


Figure 7.8 Commercial video cameras used in smart homes [23]

From the research point of view, different types of devices are used in the smart homes for monitoring the usage of the devices. Table 7.1 exhibits some of the devices based on the category and purposes they are being used [24]. Even though wireless medium of data transmission is the most favourable one, hybrid media are also used in smart homes with the significance of having a Zeno configuration. Some of the hybrid media are Ethernet, Infrared and Radio-Frequency.

7.2.1 Models for smart homes

Continuous research is being done on smart homes with a range of work done on the behaviour detection of the residing people. The wellness determination [25,26] is one such idea where two functions β_1 and β_2 were introduced to determine the duration of the use of different appliances at a defined time t. The time series modelling was applied to determine the updated time parameters and maximum durations in order to analyse the trend in the usage of household objects for past, current and future conditions. Smart homes over the years have conceptualized different models to understand, analyse and predict the behaviour of the residing people [27]. The prediction of data was also performed using support vector

Table 7.1 Category and purpose of smart home monitoring devices [24]

Category	Name	Purpose
Sensor	Light	Measurement intensity of light
	PIR	Identify user location
	Temperature	Measure room temperature and body temperature
	Pressure	Identify inhabitant location
	Switch sensor	Door open or close status detection
	RFID	Object and people identification
	Ultrasonic	Location tracking
	Current	Measure current usage
	Power	Calculate power usage
	Water	Measure volume of water usage
Physiological device	ECG	Pulse rate and variability
	PPG	Pulse rate and blood velocity
	Spirometer	Respiration rate, peak flow, inhale/exhale ratio
	Galvanic skin response	Sweating
	Colorimeter	Pallor, throat inflammation
	Pulse Oximeter	Measure oxygen saturation of blood
	Sphygmomanometer	Blood-pressure measurement
	Weight	Measure patient weight
	Pulse meter	Monitor heart weight
Multimedia device	Camera	Monitoring and tracking
	Microphone	Voice command
	Speaker or headset	Announce alert and information
	Display (LCD, Plasma panel)	Show visual information

machines (SVM) where the activities of daily living (ADL) were studied using different kinds of wearable devices like kinetic sensors [28]. These sensors determined activities like postural transitions and walk periods and then classify each of the temporal frames into one of the daily activities. A varied range of sensors including motion sensors, activity detection sensors, etc. are fixed at different locations of the house to obtain a large data set, which are then studied with different methods like neural networks [29], predictive algorithm [30], hidden Markov model [31], etc. to determine the anomalous behaviour in the future. One of the interesting approaches towards the IoT-based smart homes is related to the Web-based system which was used by formulating an application framework that supported the concurrent interaction of the residing people [32]. The system consisted of a 6LoWPAN-based WSN inside the smart home that implemented on HTTP caching and push messaging techniques. Different issues like device discovery and service description were addressed using this proposed algorithm. Representational state transfer (REST) algorithm had been employed for the connection of the web with household appliances. The architecture of the web-based system was principally based on three layers: device, control and presentation for the device control and management, processing of the data and representing the available devices dynamically, respectively. Web application description language (WADL) was adapted for the services to the HTTP-based application. The experiments were executed with commercial ZMOTION sensors which were used in the event-based scenarios using push technology. The results were based on the trials with one-hop topology which helped to identify the amount of time required for the motion detector to notify application framework.

Another interesting research work involves the use of vital-radio inside smart homes, which operated as an activity monitoring device via wirelessly sensing of the breathing and heart rate [33]. The operation was based on the change in the signals as a result of the change in position of the chest wall due to inhalation and exhalation. One of the attributes of this system is its wireless sensing capability of physiological parameters of the residing people. Another interesting work involves the evaluation of the elderly people necessities to adapt existing technologies as part of smart home projects [34]. This is a significant work as most of the times the elderly people living in the house wants to have an independent life without any interference and breach of privacy. The work on the management of the devices has also been worked up where a proactive architecture has been proposed [35] that deploys an event–condition–action (ECA) method for the management of the heterogeneous devices in the smart homes. This is a significant work from the point of view of time management as heterogeneous sensing devices are deployed inside a smart home, huge amount of data is generated as a result of which, it is difficult for the monitoring unit to classify the significant ones or the information from similar devices. In addition to the device API and device stub in the system, the modules consisted of SQL statements which communicate with the proactive architecture. The modules generate the SQL statements in accordance with the rules of the system. The IoT-based system consisted of a surveillance device, audio device and an alarm for the execution of the tasks.

7.2.2 Communication protocols in smart homes

The connectivity of the IoT-based smart homes has also been worked upon [36] regarding the different connectivity standards used in smart homes. Some of the common communication protocols used in smart homes to connect the sensors and the gateway are ZigBee, Z-Wave, Bluetooth, Wi-Fi and thread. The most prominent one among this is Wi-Fi, which works on start and mesh topologies and has the highest current consumption (116 mA), giving the highest covered range (150 metres). Some of the problems faced by these communication protocols in the home network are interoperability, self-management, maintainability, signalling, bandwidth and power consumption. For the interoperability challenge, other than Wi-Fi, all the other protocols, especially ZigBee products face this problem the most. This is why, a combined effort solution of ZigBee and thread was released in April 2015 to ensure high interoperability due to the similarity in their basic physical specifications. The inclusion of the Z-wave with ZigBee makes it easier for the sensor nodes operating with this protocol to adjust and adapt to the changes in the environment, while being able to collaborate with other devices efficiently. The maintainability of the network protocol refers to the reliability and dependability of the protocol with the change in environment, activities, nodes and gateways. All of the mentioned protocols have good maintainability to be used in smart homes. The signalling is an important parameter keeping in mind about the losses that happen with the protocols working on long distances. For example, even though Wi-Fi is reliable to be used for medium ranges, where it can have considerable amount of signal losses compared to ZigBee and Z-Wave protocols. One of the main reasons for this is the difference in the range of bandwidth between the protocols as the ZigBee and Z-wave have very low bandwidth. The problems of bandwidth keep on increasing with an increase in the number of IoT-based smart homes creating a huge amount of data in the network server. The lower bandwidth of ZigBee, thread and Z-wave compared to Bluetooth and Wi-Fi does make them a viable open for future applications. The challenge of power consumption in the protocols is somewhat related to the data transfer between the sensor nodes and gateway. Even though the Wi-Fi consumes more power compared to ZigBee, Z-wave and Bluetooth, it does transfer the data at a faster rate, which is sometimes useful in emergency situations. Thread, being a comparatively newer protocol, can be assumed to be in the middle with a moderate speed of data transfer and very low power consumption. But one of the problems that thread faces is the high consumption of power per bit, which makes it a non-viable option for low amount of data transfer.

The usage of IoT in smart homes has been optimized over the years by deploying different communication protocols in these homes. One of the works [37] involves the usage of ZigBee protocol where the XBee modules were connected to the objects as end devices in order to commute their usages via IoT gateway. With the use of ZigBee protocol [38] to send the data to the cloud services, researchers have also worked upon the received data in the cloud using JSON data format to improve the data exchange efficiency. ZigBee has also been used with other technologies like 3G and Ethernet [39] to transfer the data collected by the sensor modules. The work has been done on three layers namely sensing, network and application layer. The hardware consisted of five different parts: ZigBee module, Ethernet module, 3G module, video module and data sampling and control module. The presence of both 3G and Ethernet modules confirmed the transmission of data wirelessly if the latter one fails. Other than the 3G module, researchers have also used Arduino boards and applications to implement IoT-based applications [40]. They operated with two different prototypes namely Bluetooth and Ethernet in indoor and outdoor environments, respectively. The mobile app present in the smartphone was directly linked with the Bluetooth connectivity using serial communication protocol. MAC address of the Bluetooth module was used to pair up with the mobile app in the phone. But two of the biggest challenges they faced with the Arduino board system were the assessment of unique IP address to the heterogeneous devices connect to the Internet in smart homes and the absence of a commercial standard for the integration of the different sensors for the IoT-based devices.

Another concept used in smart homes is the mobile RFID-based IoT systems [41] which is based on the multistandard Near Field Communication (NFC) and Ultra High Frequency (UHF) technologies. The master and slave readers were used in a hierarchical architecture where the slave readers falling within the range of the master reader would respond passively and send the data of the RFID connected objects. The significance of this work lies in the mobile RFID reader, which behaves as an 'Energy Generator' device as it powers up while facing the master and slave readers. One of the research works [42] was done to emphasize on the different services required by the ISO layers to obtain high quality of data from different heterogeneous data sources in the smart homes. The first is the perceptive layer which deals with the controlling of the WSN used for data collection monitoring purposes. RFID, sensors, device control and energy management are some of the attributes at this layer that are analysed, dealt and worked upon. Second is the network layer which deals with the communication of the collected data. Some of the basic examples are Satellite communication, ZigBee, 3G, PLC network, Infrared Ray, Bluetooth and Wi-Fi. The third layer is the software infrastructure layer which is the most significant one as it bridges between the user layer and network layer. The SOA framework and Web Services platform are some of the examples of the type of services used for this layer. The last one is the application layer which is the service provided to the people residing in these homes. Security, medical, data and entertainment are some of the common services offered in these specialized automated homes.

7.2.3 Architecture of smart homes

In terms of architecture, researchers have tried [43] to improve the quality of service by developing a model that categorizes the monitoring system into three different levels. These levels are categorized as the monitoring, control and user-level services. The first category can be defined as the data acquisition level where different kinds of devices are used for ubiquitous monitoring of activities. This is the primary level where the sensor data are collected and calibrated for the second level. The second step is the information processing one where the sensor data are processed with the threshold values set according to user requirements. The last step is the context making where the model generates awareness to the monitoring unit for the required action depending on the information generated by the knowledge engine. Researchers have also worked [44] on the adaptation capability of the IoT-based systems for the activity recognition in the smart homes using a spatio-temporal feature technique which does a semisupervised learning. The model included five major processes: *Initial classification*, *temporal feature-based verification*, *spatial features-based clustering*, *spatio-temporal match evaluation* and *model update*. For the classification part, the data are divided into recognized and unrecognized ones. The recognized data then goes to the second step for verification while the unrecognized ones go for the third step to form clustered instances. The outputs of the second and third steps are then fed into the match evaluation step to join the candidate activities together to form multiple groups of new instances perform a comparative study between each activity of each group for evaluation. The difference of this proposed model from the conventional semi-supervised adaptation model lies in its spatio-temporal features, which gives a higher chance to discover more instances of different activities that are useful for training purposes in order to increase the performance efficiency of the model. The activity recognition was also done using a pattern cluttering technique to a temporal ANN algorithm [45]. The model is divided into two steps, where it starts off with a relevant and efficient unsupervised learning technique named the K-pattern clustering algorithm. The second step is related to the training of the environment for determining and predicting the activities of a person using an artificial neural network based on Allen's temporal relations. Initially, the large amount of data collected from the sensors in the IoT-based smart home goes through an unsupervised learning algorithm. The entire data are computed and grouped into clusters with similar user activity patterns. The algorithm is also able to detect the discontinuous and interleaved activity pattern of the users, resistance towards the noise in the overall data in the set and computing data efficiently by grouping similar activities. The processing of the perceived data was done to detect the temporal relations between them. The second part of the algorithm does the conversion of the perceived data, observation and mining of the most frequency pattern and again grouping of similar patterns. The detection, mining and grouping of the patterns was at a faster rate in comparison to that of the threshold set in the first part of the algorithm. The advantages provided by this approach lies in the decreased amount of time and space required to intercept the activities happening in the smart home environment.

The application layer can also be subdivided into three layers, namely, Kernel layer, Agent layer and Interface layer [46]. The first layer is responsible for the agent management and data transportation from the application layer to the other layers. This layer interacts with the network layer to transfer the collected data for analysis purposes. The interface layer is responsible for providing the different kinds of interfaces in terms of resources to the application layer. The modelling of the resources to the upper layers is done at this level. The agent level is responsible for defining the type of different smart devices used in the smart homes. The most significant level in this architecture is the Kernel level, which manages all the levels in the application layer. It is also responsible for the management, transportation, authentication and authorization of the data and monitoring of its transfer from the application layer to the upper layers. Even though the authorization and authentication are done on the application layer, it is specially controlled by the certification authority (CA), which is centrally located in the smart home for controlling purpose. The CA performs the double-checking process on the call of an agent during an operation. When the CA sends its certification to the agent to validate its decision, the agent sends back its own response to CA through certification. If the responses between the CA and the agent are positive, the CA informs its subordinate agents to work with the other controllers. Research work also includes the use of commercially available ARM microprocessors like SAMSUNG S3C2440A [47] to collect the data from the sensors and process it. These data are then communicated through ZigBee protocol to the monitoring unit. The WSN also prefers using CPLD, which is a complex programmable logic device, but mainly for industrial purposes [48]. Sensors can be controlled using a radio-frequency wireless sensor and actuator network (WSAN) at a frequency of 433 MHz to control, monitor and manage the appliances in the smart homes. The use of CPLD/FPGA is sometimes more preferable than the microprocessors in the smart homes due to their advantages of real-time performance and synchronicity.

Another common phenomenon used in smart homes is the speech recognition of the residing people with specific controllers to differentiate the significant voices from the surrounding noises. One of them [49] used the Griffiths-Jim method in a speech recognition engine where the reception of the speech was done within a specified boundary to immune from the noise and having a high signal-to-noise ratio. Machine learning was done with the engine with limited vocabulary specialized for devices working on Boolean logics like lighting, TV, radio, etc. Another project involved speech recognition using different novel ASR techniques in a multiroom smart home designed for a project named SWEET-HOME [50]. Twenty-one speakers were tested with microphones at different scenarios including activities of daily living. It was found out that the results obtained using techniques like DDA was better than the baseline or other available techniques. The work on the communication protocol has been further enhanced by researchers [51] to showcase the use of 5G for smart homes and smart cities. A four-layered model consisting of the integration of the technologies like 5G, IoT, cloud of things and distributed artificial intelligence was developed for the analysis of handling big data sets obtained from smart homes and smart cities. Another interesting research work employed Bluetooth as the communication protocol in smart homes [52] to transfer the data due to its advantage of reduced energy consumption. The proposed algorithm uses a fuzzy logic mechanism to analyse the sleeping time of each device by determining the ratio of the throughput to the workload. In this way, there is an increase in the lifetime of the devices by 30%. The fuzzy logic approach has been backed up simulation results, which showed there is a considerable reduction in the required power. Another important sector where research work had been done was the development of a protocol for face identification and emotion recognition through image processing techniques. The system comprises two elemental blocks, sensors and decision maker. The first block consisted of the sensors located in the environment and the second element consisted of a single machine which processed the information passed on by the first element. Other than the different kinds of sensors like gas, humidity, temperature, motion, etc. located inside the house, wearable sensors like smartwatches were also used to determine the different physiological parameters of an individual. The processed information was then passed onto the cloud for remote monitoring purposes. For facial recognition, Face tracker was used for mapping process to determine the facial representation using facial points.

In one of the interesting research works, an alternative approach towards the IoT for the replacement of the most commonly used host-centric Internet Protocol with an Information-Centric Networking (ICN) paradigm in a smart home domain [53]. The proposed algorithm does provide a more quick, flexible and efficient technique for data transmission and configuration management. ICN can be used both for providing naming content objects and identification of the functionalities of different IoT connected devices in a logical way, without the need of any of the addresses. The packing of the names with different components is done in a hierarchical manner using this protocol, where it moves the names between two consecutive layers. In some of the systems, the network domain uses a hybrid of ICN and IP protocol instead of singularity to have better communication between the sensors and the gateway for the sensing data. The framework comprised of a configuration manager and authorization manager through which the fixtures are assigned and the credibility to access the fixtures, respectively. The idea of ICN associated with smart home applications does provide a viable option due to the simplified configuration of its associated network and data retrieval capability and, most significantly, it provides security to the network layer to a great extent. The work on the use of ICN on smart homes does provide an interesting insight based on the scalability of the problem, traffic characteristics and handling mobility [54]. It also enhances the storage of the data by giving leverage to the application requirements as much as possible. The privacy and the security of the data are two other issues that get affected on their relation to any communication paradigm. One of the interesting research works depicts the usefulness of video cameras and sensors in terms of the increase in the monitoring capability of the smart homes [55]. The use of Building Control Services (BCS) was done in the smart home to manage the sensors and actuators, having *timewheel* as the central data structure to manage the chain of events. They have employed the Markov Chain Monte Carlo and Hungarian models to analyse the problem faced with the non-overlapping tracking of the residing people in smart homes with a network of cameras.

7.2.4 Security in smart homes

Since, all the IoT-based smart homes involve the uploading of data on the cloud, security is an important factor to ensure the privacy of the personal information of the residing people. Regarding the analysis of the security problems and challenges, another significant work [56] has been done to bridge the gap through a detailed study of the attack surfaces, security issues, forensics and threat models. One of the surveys conducted by Hewlett-Packard in 2014 showed [57] that 80% of IoT-enabled daily used devices in smart homes breaches privacy related to the personal information, while almost an equal amount of communications were not encrypted and had security vulnerabilities. A few of the devices that can be altered are the smart TV, magnetic sensors and the alarm system via different antennas and RF signals. The security issues related to the communication of the data can be addressed by the IoT devices with proper authentication and access control of peers with which the nodes communicate. The surface attacks take place in two networks, public and local with six different communication levels: device-device, device-coordinator, coordinator-gateway and device-controller for the local network and controller-IoT service provider and service-service for the public network. Another work [58] involves the approach towards strong security system by implementing an AllJoyn framework that used an asymmetric Elliptic Curve Cryptography to provide authentication during the system operation. The system ran on a Wi-Fi network where a gateway was used as the central node of the system. Android-based mobile phones were used as end devices which provide a mean for set up, access and control the system. The authentication was done in two rounds to ensure extra stability of the proposed system. In the first round, the user had to load the identity and preshared key of the IoT connected device on the mobile device while in the second round, the identity was uploaded on the home gateway. In the review article by [59] on the IoT applications on smart homes, the problems related to the security was addressed in terms of filtering false network traffic and avoiding unreliable home gateways. One of the ways to circumvent the initial problem is to use a cooperative authentication scheme to prevent insignificant or false data to be distributed in the network [60]. The second problem could be addressed by using a side channel monitoring (SCM) technique [61] to handle the problem at a minimal cost. The technique is the optimized selection of subnet of neighbours for each node along the patch of the router to determine its performance in message transmission in the forward direction. But the source has the reverse direction of message transmission as its primary communication channel.

One of the networking challenges addressed by this group is in terms of the interference of the unreliable nodes during the data communication and filtering of the false data traffic in the community network. Another group has worked [62] on the network-level security of the IoT-enabled devices in smart homes to restrict the illegitimate intruding into residing people's activities. The work was done to augment the device level with the network-level security solutions in order to use the software-defined networking (SDN) technology to dynamically block devices with suspicious behaviour. A three-party architecture was proposed via an open-source SDN platform to determine the efficacy to provide security to the IoT-enable devices. The solutions were based on SDN implementing dynamic security rules that were based on contexts depending on the time or occupancy of people in the house. The protocol was developed on the assumptions that the ISP has the visibility of the devices present in the house and its access was SDN enabled. Floodlight (v0.9) OpenFlow controller was used for operating the ISP network. One of the major ideas proposed for the security and privacy of the smart homes was in terms of a blockchain by eliminating the Proof of Work (POW) and concept of chains [63]. The proposed algorithm was executed by using an online, high-resource device named 'miner', which was responsible for the communication taking place inside and outside the smart home. The concept of POW and bitcoins was eliminated as it faced several challenges like high-resource demand and long latency for the confirmation of transaction, which would result in low scalability and blockage of the whole network due to the broadcasting transactions. The algorithm relied on the hierarchical structure and distributed trust in order to maintain the blockchain and specifying it to the IoT to ensure the security of the home. In order to evaluate the performance of the proposed algorithm, a further simulation was done using three remote sensors and IPv6 communication protocol. The simulation contained handled situations with encryption, hashing and blockchain that was proposed in the algorithm. Although the overlay delay and processing conditions were not considered during the simulation, the transfer of the bytes between the devices, miner and the cloud is three to seven times for the proposed algorithm compared to that of the results obtained from simulation.

The security of the smart homes also dealt with the amount of protection the residing people get from cyber-attacks [64]. This is very helpful from the network point of view as the resource-constraint nature of some of the devices does not permit to provide solutions for any security problems, thus increasing the vulnerability of the information of the users to be hacked or intruded by the third party. Most of the devices were operated in around the GHz range with the use of ZigBee, Wi-Fi (IEEE 802.11), Bluetooth and NFC as the communication protocols. Some of the security problems addressed in this work are the resource and energy constraints, heterogeneous communication protocols resulting in unreliable communication leading to decrease in the computing performance and storage capabilities, execution of the security solutions between the end-devices located inside the smart homes and Internet applications, low reliability of the delivery of the packets, limited availability of energy for communication between different devices and tampering attacks, respectively. Different potential security threats in an IoT-based smart home system in the five different layers in an ISO model showcased the maximum probability of threats and attack framework in the network layer. One of the most significant attacks on the network layer is the Black hole attack on RPL where the attack is initiated with a node and progresses through all the nodes in that pathway, dropping the packets that are transmitted through that pathway. This causes disruption in the flow, thus causing data trafficking in the network. The attack on the application is initiated by the *XMPPloit* command-line exploit tool which enforces the IoT-based smart home devices to remove the encryption on the transmitted data to make it easier for the attacker to modulate them during their transmission. A few of the requirements that can be done to minimize the attacks on the different layers are to possess an intrusion detection system in order to detect unauthorized intrusions and anomalies, employing tamper-resistant devices for the physical layer, employing a device authentication system to classify the authorized devices from the unauthorized ones, have a security-key management system for protecting the sensing devices inside the smart homes that are employed with pre-installed network keys.

The attacks on the security are also based on the location, property, access level and strategy and information damage level [56]. The attack on the location depends on the internal or external position of the attacker in terms of IoT network. When the attacker is external, he gets unauthorized remote access of the network domain from any public network. The attack on device property is based on the low-end and high-end devices used to get access to the IoT network and its associated devices. The low-end devices include the wearable devices used by the people residing inside the homes for ubiquitous monitoring purposes, whereas the end–end devices include the computer, laptop and virtual machines. The access-level attacks are based on active and passive attacks. Active attacks attempt to affect the functionality of the IoT system by disrupting the normal transmission of data. Passive attacks are involved in the unauthorized access to the network domain of a system and perform illegitimate activities to obtain personal information of the residing people. The strategical attacks are defined as the physical and logical attacks which involve the damage and tampering to the IoT devices and affecting the devices in the communication channel, respectively. The vulnerability of IoT-based smart homes for security in terms of privacy was also studied [65] by the researchers in relation to the IoT network traffic created during the data transmission. One of the major concerns remains in revealing the personal information of the residing people happening through metadata and trafficking of the encrypted data. Certain possibilities to deal with the trafficking problem are to separate the traffic into packet streams, labelling the streams by the definite type of device and examining the traffic rates.

7.3 Potential sensors for smart homes

Different kinds of sensors have been used to sense the environment and determine the activities of the people. The fabrication and usage of some of the sensor prototypes have been described in this section. These sensor prototypes have the potential to be used in smart homes for monitoring purposes. A flexible sensor prototype was developed from Multi-Walled Carbon Nanotube (MWCNT) and Polydimethylsiloxane (PDMS) via casting method and used for monitoring physiological parameters of an individual [66]. Figure 7.9 shows the schematic diagram of the fabrication process of the sensor prototypes. Initially, the PDMS layer was cast, desiccated and cured on the PMMA template to form the substrate of the sensor prototype. A nanocomposite layer which formed by the mixing of 4 wt% of MWCNTs into PDMS was then cast on the cured PDMS layer. This layer was then desiccated, cured and laser cut to form the electrodes of the sensor prototypes. The sensor patches were then employed to monitor the movements of the limbs and respiration. The connection of the sensor patches on the individual for limb

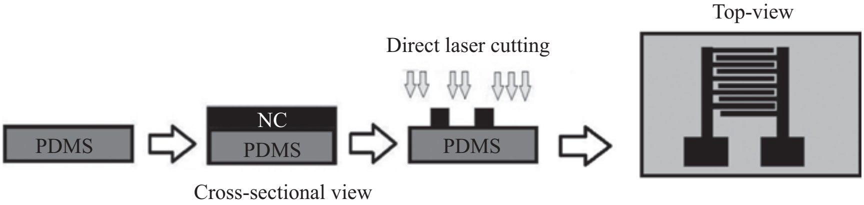


Figure 7.9 Schematic diagram of the fabrication process of CNT-PDMS-based sensor prototypes for physiological parameter monitoring [66]

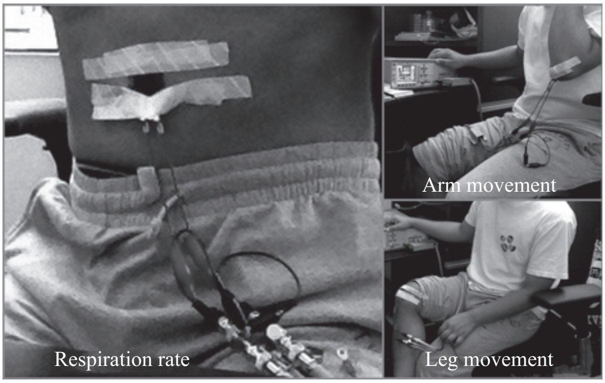


Figure 7.10 Connection of the CNT-PDMS sensor patches to different parts of the body for monitoring purposes [66]

movements and respiration is shown in Figure 7.10. The sensor patches were used as wearable devices where they were attached to the individual with biocompatible tapes. Figure 7.11 shows the respiratory response of the CNT-PDMS sensor patches for two different individuals. It is seen from the response that the fabricated sensor patches are capable of distinguishing the response of the separate individuals. This sensor can turn out to be very useful for smart homes as they can be used in systems for monitoring multiple activities. This would not only help to be used as wearable sensors that can be attached to the clothing of the individuals residing in smart homes but will also help to reduce the overall cost of the sensing system.

Another flexible sensor patch that has the potential to be used in smart homes as a wearable sensor was fabricated by from Graphite and PDMS based on casting on 3D printed moulds. The schematic diagram for the steps of fabrication is shown in Figure 7.12. The 3D moulds were used as templates on which graphite, followed by PDMS was cast to develop the electrodes and substrate, respectively.

The sample was cured to form the prototype which was attached to different parts of the body like neck, elbow, knee and finger to determine their movements based on the stress induced on the sensing area of these patches [67]. Figure 7.13 shows one of the responses where the sensor patch was connected to the neck of an

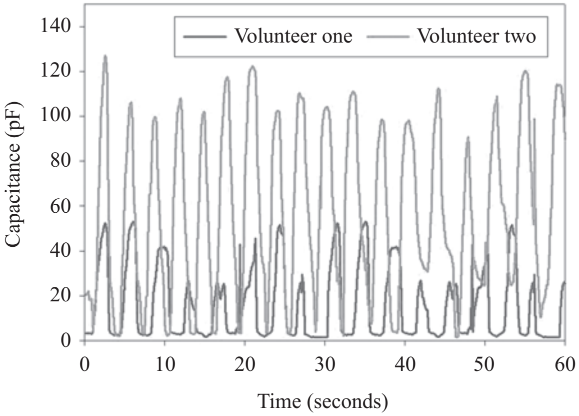


Figure 7.11 Comparative response of the CNT-PDMS-based sensor patches for the respiration of two individuals [66]

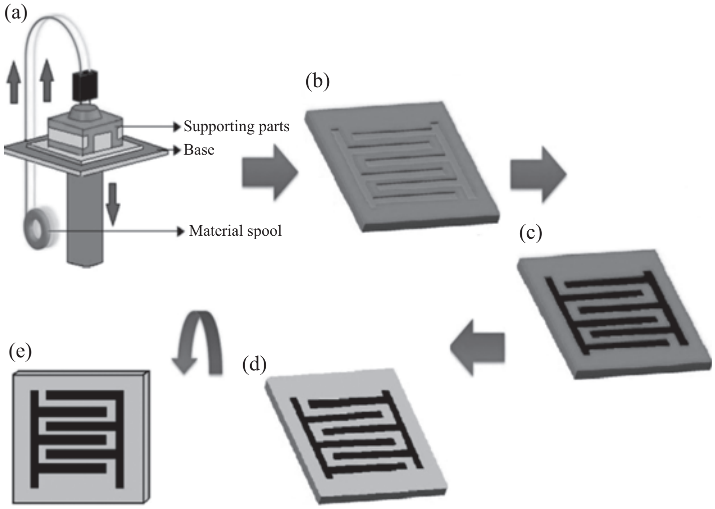


Figure 7.12 Schematic diagram of the fabrication process of the graphite-PDMS sensor patches

individual. Two different situations, namely 'flexed' and 'extended' were considered, which refers the bent and normal/straight positions respectively for the neck. It is seen the sensor patch was capable of monitoring the oscillatory movement of the neck with proper distinction. The oscillatory movements with these sensor patches were done to check the repeatability in their responses.

The graphite-PDMS sensor patches also hold a high potential to be considered commercially for the usage in smart homes due to two factors. First, in the current

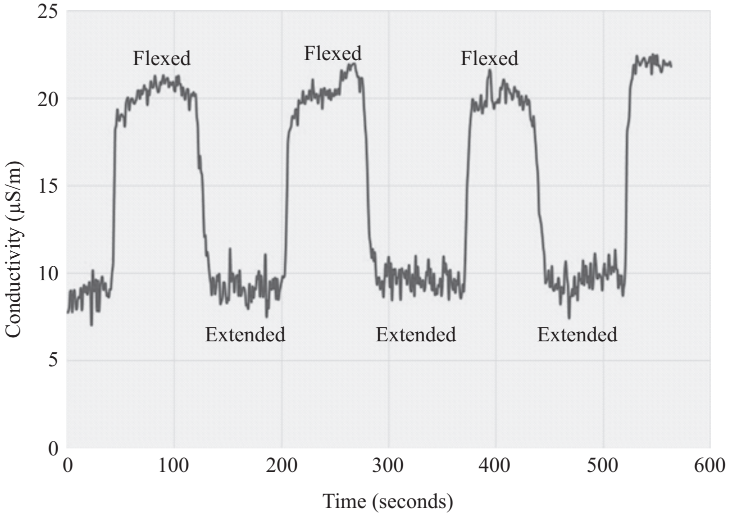
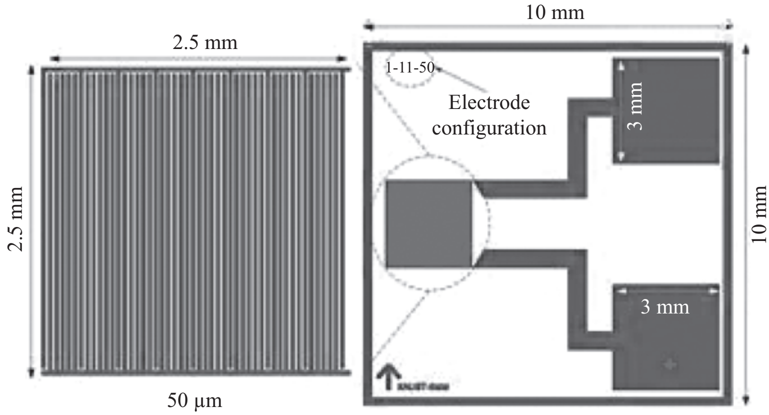


Figure 7.13 Response of the graphite-PDMS sensor patches for monitoring neck movements [67]

era of 3D printing, where most of the electronic devices are being fabricated using this quick and low-cost technique, development of the flexible sensor prototypes for monitoring physiological parameters holds high regard. Second, due to the strain induced nature of this sensor prototype, it can be considered for monitoring patients going through rehabilitation or elderly people in smart homes who are suffering from stroke. Another potential sensing system that can be introduced in smart homes involves the usage of silicon sensors for early detection of osteoporosis. The significance of this work is related to the elderly people who face problems with osteoporosis. In simple words, osteoporosis is a disease that causes bones to become weak and fragile. Worldwide, osteoporosis is a serious problem and it is growing with the ageing population. Early detection of bone loss is necessary to restrict the occurrence of this disease to a large extent. Monitoring the bone turnover markers can be helpful in early detection and monitoring bone problems and to decide the type of therapy. Bone loss can be detected by regular monitoring of serum or urine C-terminal telopeptide of type 1 collagen (CTx-1) [68]. Therefore, fast, portable and low-cost point-of-care (PoC) devices could be helpful for a regular measurement. A highly selective and sensitive portable PoC device was proposed for early detection of bone loss by regular measurement of CTx-I in serum. A MEMS-based interdigital sensor was employed to perform the experiments. The configuration of the sensor was 1-11-50 as shown in Figure 7.14, which means each eleven sensing electrodes is located between two working electrodes and the gap between the consecutive electrodes is 50 μ. Interdigital sensors are designed in a digit-like pattern following the same principle of parallel



Chip configuration 1-11-50
Electrode width: 25 µm
Spacing between electrodes: 50 µm

Figure 7.14 Configuration of the interdigital sensor

plate capacitors. There are some advantages in using these sensors such as the uniformity of the electric field, non-destructive, in situ and single-sided access to the material under test (MUT). When a time-dependent AC signal is applied to the sensor, the electric field lines generated which bulge from the positive electrodes to the negative ones and carry some information about the properties of the MUT.

Molecular Imprinted Polymer (MIP) technique was used to prepare the artificial antibodies for CTx-I molecules. The MIP-based artificial antibodies have certain advantages over the natural biological antibodies; they are highly stable in harsh environmental and mechanical conditions and they can be prepared with a very low cost which reduces the total cost of the sensing system. Moreover, no sample preparation is required that is suitable for the development of a rapid system. The artificial antibodies were immobilized on the sensing area of the interdigital sensor using to introduce the selectivity of CTx-I molecules into the sensor. In order to design a portable PoC system for CTx-I monitoring, a microcontroller-based system was designed to quantify the concentration of the target molecule in serum and transfer data to an IoT-based cloud server. The results can be supplied to the medical centre and further analysis and investigation can be done for bone loss detection and treatment. An AD5933 [69] impedance analyser was utilized to measure the impedance, which was produced by varying the concentration of CTx-1. I^2C protocol [70] was employed to collect the impedance information from the MIP-coated sensor. Finally, the measured level of CTx-1 was transferred to an IoT-based cloud server in order to supply the information to a medical person for further analysis. An ADG849 switch was used to calibrate the PoC sensing device before every measurement. The microcontroller generates the impedance information from the impedance analyser and using the standard calibration graph calculates the level of CTx-1. Figure 7.15 shows the first prototype developed as the PoC device for CTx-I detection and quantification. The microcontroller board includes an integrated Wi-Fi that is useful to connect the PoC system to a gateway to transfer data to a remote cloud server. Thingspeak [71] which is a free IoT-based cloud server was utilized to store the data. Thingspeak could be accessible from any location, which helps the medical practitioner to have access to the real-time data for early detection of bone loss. The Arduino Ciao [72] library was used to transfer the CTx-I concentrations to the designated private channel in Thingspeak.

The calibration curve was developed by measuring the CTx-I concentration of five samples, which were prepared by mixing the CTx-I peptide with distilled water. The calibration curve equation was provided to the microcontroller to measure the concentration of CTx-I in unknown samples. Four unknown serum samples collected from sheep blood were tested using the proposed PoC device and the results were validated using a standard ELISA kit. Figure 7.16 shows the correlation analysis between the proposed PoC device and a standard ELISA kit for CTx-I measurement. The developed PoC device employs blood serum as the test sample. However, Blood sampling might not be acceptable and popular for PoC devices. Hence, design and development of a system which uses urine as the test sample can be desirable. A PoC urine testing system could be developed following the principle of the proposed serum PoC device. It can then be installed in for regular and automatic monitoring of bone condition without human interaction. The measured data would be transmitted wirelessly to the health care practitioner for further analysis and actions [73].

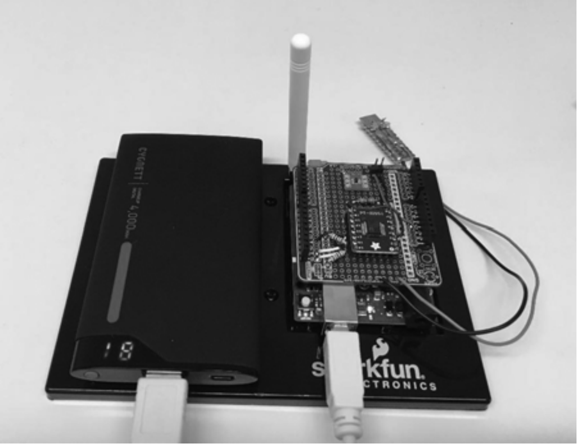


Figure 7.15 The first prototype of the proposed PoC device

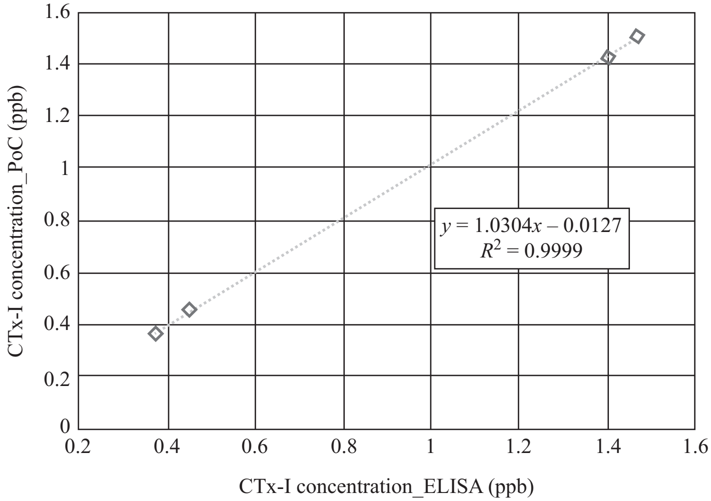


Figure 7.16 Correlation analysis between the proposed PoC device and a standard ELISA kit for CTx-I measurement

7.4 Challenges and future opportunities

Even though a lot of work has been done on the different sectors of IoT-based smart homes, there are still some possibilities to improve the existing approach and algorithms. Some of the possible solutions are discussed here. First, the smart homes operating commercially in today’s world are not reachable to the wider range of people but are only accessible to a group of people. One of the major reasons behind this is the cost of living in these homes, which might not be affordable for every person. Second, the information about the advantages of living in these homes should be circulated more among people. The second challenge is the huge amount of data generated in these homes. This requires a lot of memory space in the database, making it difficult to handle it. Algorithms should be developed in such a way that machine learning is done in the most efficient way to determine only the significant data. The third challenge would be the availability of the devices used in the smart homes. Even though some of the commercial devices that are mentioned in this chapter are available to people, they are not being able to comprehend the logic and circuitry of all of them. This makes it difficult for them to use it, in spite of the advantages they provide. The operating principle of the sensing systems should be simple, so that the residing people, especially the elderly ones, are able to comprehend. Another problem with the IoT-based smart homes is the lack of standardization in data collection and processing techniques. Even though so many researchers are working to develop optimized protocols, no standard techniques are yet available to follow. One possible solution for this could be setting a standard by an international organization so that any investor working on developing a smart home would follow those standards. Another problem with these smart homes lies in the high dependability on the Internet connection. If the rate of data transfer goes down, the normal functioning of the monitoring of the different activities goes down. This creates data traffic, thus leading to further problems. Also, the signals from the wireless connections can be interrupted among each other as a result of different heterogeneous sensing devices, leading to false sensed data. One of the possible solutions to this problem could be the division in the frequency bands of the sensing devices to minimize the data interference. If the researchers come up with significant solutions for the above problems, the quality of life can be greatly improved in these IoT-based smart homes.

References

[1] Aldrich FK. Smart homes: past, present and future. Inside the smart home. London: Springer; 2003. p. 17–39.

[2] Chan M, Estève D, Escriba C, Campo E. A review of smart homes: present state and future challenges. *Computer Methods and Programs in Biomedicine*. 2008;91(1):55–81.

[3] Elderly care-smart homes. Available from http://www.jamesdearsley.co.uk/smart-homes-elderly-care/. Last accessed on 1st June 2018.

[4] Chan M, Hariton C, Ringeard P, Campo E, Editors. Smart house automation system for the elderly and the disabled. IEEE International Conference on Systems, Man and Cybernetics, 1995 Intelligent Systems for the 21st Century, Vancouver, BC, Canada. IEEE, 1995.

[5] Tang P, Venables T. 'Smart' homes and telecare for independent living. *Journal of Telemedicine and Telecare*. 2000;6(1):8–14.

[6] University of Florida. Gator Tech Smart House. Available from http://www.icta.ufl.edu/gt.htm. Last accessed on 1st June 2018.

[7] Smart Community Alliance, Japan. Available from https://www.smart-japan.org/english/. Last accessed on 1st June 2018.

[8] KIDUKU, Fijitsu, Japan and Ireland. Available from http://www.fujitsu.com/global/news/pr/archives/month/2013/20130628-01.html.

[9] Smart Homes, U.K. Available from http://www.strath.ac.uk/esru/research/smarthomes/. Last accessed on 1st June 2018.

[10] Ghayvat H, Mukhopadhyay S, Liu J, Babu A, Alahi MEE, Gui X. Internet of things for smart homes and buildings. *Australian Journal of Telecommunications and the Digital Economy*. 2015;3(4):33–47.

[11] He D, Chan S, Guizani M, Yang H, Zhou B. Secure and distributed data discovery and dissemination in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*. 2015;26(4):1129–1139.

[12] Ghormare S, Sahare V, Editors. Implementation of data confidentiality for providing high security in wireless sensor network. 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India. IEEE, 2015.

[13] Ghayvat H, Liu J, Mukhopadhyay SC, Gui X. Wellness sensor networks: A proposal and implementation for smart home for assisted living. *IEEE Sensors Journal*. 2015;15(12):7341–7348.

[14] Venkatasubramanian KK, Banerjee A, Gupta SKS. PSKA: Usable and secure key agreement scheme for body area networks. *IEEE Transactions on Information Technology in Biomedicine*. 2010;14(1):60–68.

[15] Poon CC, Zhang Y-T, Bao S-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*. 2006;44(4):73–81.

[16] Li J, Zhang Y, Chen Y-F, Nagaraja K, Li S, Raychaudhuri D, Editors. A mobile phone based WSN infrastructure for IoT over future internet architecture. 2013 IEEE International Conference on Cyber, Physical and Social Computing, Green Computing and Communications (GreenCom), and Internet of Things (iThings/CPSCom), Beijing, China. IEEE, 2013.

[17] Dargie W. Dynamic power management in wireless sensor networks: State-of-the-art. *IEEE Sensors Journal*. 2012;12(5):1518–1528.

[18] Castagnetti A, Pegatoquet A, Le TN, Auguin M. A joint duty-cycle and transmission power management for energy harvesting WSN. *IEEE Transactions on Industrial Informatics*. 2014;10(2):928–936.

[19] Smart smoke detector. Available from https://www.tomsguide.com/us/best-smart-smoke-detectors,review-4472.html. Last accessed on 1st June 2018.

[20] Smart humidity monitor. Available from https://www.amazon.com/AcuRite-Thermometer-Digital-Hygrometer-Humidity/dp/B004K8RF10/ref=br_lf_m_7jtxmhgy5w2c7f3_ttl?_encoding=UTF8&s=home-garden. Last accessed on 1st June 2018.

[21] Smart thermostat. Available from https://www.amazon.de/ecobee-EB-STATE4-01-ecobee4-Thermostat-THERMOSTATS/dp/B06W2LQY6L. Last accessed on 1st June 2018.

[22] Motion Sensors. Available from https://www.officeworks.com.au/shop/officeworks/p/elgato-eve-wireless-motion-sensor-inewindmot. Last accessed on 1st June 2018.

[23] Video cameras. Available from https://www.amazon.com/Monitor-Camera-Temperature-Two-Way-Operating/dp/B06XJQH4CD. Last accessed on 1st June 2018.

[24] Alam MR, Reaz MBI, Ali MAM. A review of smart homes: past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*. 2012;42(6):1190–1203.

[25] Suryadevara N, Mukhopadhyay SC, Wang R, Rayudu R. Forecasting the behavior of an elderly using wireless sensors data in a smart home. *Engineering Applications of Artificial Intelligence*. 2013;26(10):2641–2652.

[26] Suryadevara NK, Mukhopadhyay SC. Wireless sensor network based home monitoring system for wellness determination of elderly. *IEEE Sensors Journal*. 2012;12(6):1965–1972.

[27] Lotfi A, Langensiepen C, Mahmoud SM, Akhlaghinia MJ. Smart homes for the elderly dementia sufferers: identification and prediction of abnormal

behaviour. *Journal of Ambient Intelligence and Humanized Computing*. 2012;3(3):205–218.

[28] Fleury A, Vacher M, Noury N. SVM-based multimodal classification of activities of daily living in health smart homes: sensors, algorithms, and first experimental results. *IEEE Transactions on Information Technology in Biomedicine*. 2010;14(2):274–283.

[29] Robles RJ, Kim T-h, Cook D, Das S. A review on security in smart home development. *International Journal of Advanced Science and Technology*. 2010;15(1):456–61.

[30] Virone G, Alwan M, Dalal S, Kell SW, Turner B, Stankovic JA, *et al.* Behavioral patterns of older adults in assisted living. *IEEE Transactions on Information Technology in Biomedicine*. 2008;12(3):387–398.

[31] Van Kasteren T, Englebienne G, Kröse BJ. Activity recognition using semi-Markov models on real world smart home datasets. *Journal of Ambient Intelligence and Smart Environments*. 2010;2(3):311–325.

[32] Kamilaris A, Trifa V, Pitsillides A, editors. HomeWeb: An application framework for Web-based smart homes. 2011 18th International Conference on Telecommunications (ICT), Ayia Napa, Cyprus. IEEE, 2011.

[33] Adib F, Mao H, Kabelac Z, Katabi D, Miller RC, Editors. Smart homes that monitor breathing and heart rate. Proceedings of the 33rd annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea. ACM, 2015.

[34] Portet F, Vacher M, Golanski C, Roux C, Meillon B. Design and evaluation of a smart home voice interface for the elderly: acceptability and objection aspects. *Personal and Ubiquitous Computing*. 2013;17(1):127–144.

[35] Perumal T, Sulaiman MN, Mustapha N, Shahi A, Thinaharan R, editors. Proactive architecture for Internet of Things (IoTs) management in smart homes. 2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE), Tokyo, Japan. IEEE, 2014.

[36] Samuel SSI, Editor. A review of connectivity challenges in IoT-smart home. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman. IEEE, 2016.

[37] Kelly SDT, Suryadevara N, Mukhopadhyay SC. Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE Sensors Journal*. 2013;13(10):3846–3853.

[38] Soliman M, Abiodun T, Hamouda T, Zhou J, Lung C-H, editors. Smart home: Integrating internet of things with web services and cloud computing. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, UK. IEEE, 2013.

[39] Bing K, Fu L, Zhuo Y, Yanlei L, Editors. Design of an internet of things-based smart home system. 2011 2nd International Conference on Intelligent Control and Information Processing (ICICIP), Harbin, China. IEEE, 2011.

[40] Mandula K, Parupalli R, Murty CA, Magesh E, Lunagariya R, editors. Mobile based home automation using Internet of Things (IoT). 2015 International

Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, India. IEEE, 2015.

[41] Darianian M, Michael MP, Editors. Smart home mobile RFID-based Internet-of-Things systems and services. 2008 ICACTE'08 International Conference on Advanced Computer Theory and Engineering, Phuket, Thailand. IEEE, 2008.

[42] Li B, Yu J. Research and application on the smart home based on component technologies and Internet of Things. *Procedia Engineering.* 2011;15: 2087–2092.

[43] Kang B, Park S, Lee T, Park S, Editors. IoT-based monitoring system using tri-level context making model for smart home services. 2015 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA. IEEE, 2015.

[44] Wu C-L, Tseng Y-S, Fu L-C, editors. Spatio-temporal feature enhanced semi-supervised adaptation for activity recognition in IoT-based context-aware smart homes. 2013 IEEE International Conference on Cyber, Physical and Social Computing, Green Computing and Communications (GreenCom) and Internet of Things (iThings/CPSCom), Beijing, China. IEEE, 2013.

[45] Bourobou STM, Yoo Y. User activity recognition in smart homes using pattern clustering applied to temporal ANN algorithm. *Sensors.* 2015;15(5): 11953–11971.

[46] Jie Y, Pei JY, Jun L, Yun G, Wei X, editors. Smart home system based on iot technologies. 2013 Fifth International Conference on Computational and Information Sciences (ICCIS). IEEE, 2013.

[47] Gaikwad PP, Gabhane JP, Golait SS, editors. A survey based on Smart Homes system using Internet-of-Things. 2015 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC), Chennai, India. IEEE, 2015.

[48] Chi Q, Yan H, Zhang C, Pang Z, Da Xu L. A reconfigurable smart sensor interface for industrial WSN in IoT environment. *IEEE Transactions on Industrial Informatics*. 2014;10(2):1417–1425.

[49] Moir T, editor. From science fiction to science fact: A Smart-House interface using speech technology and a photo-realistic avatar. 2008 M2VIP 2008 15th International Conference on Mechatronics and Machine Vision in Practice, Auckland, New Zealand. IEEE, 2008.

[50] Lecouteux B, Vacher M, Portet F, editors. Distant speech recognition in a smart home: Comparison of several multisource ASRs in realistic conditions. *Interspeech 2011*. Florence. 2011.

[51] Skouby KE, Lynggaard P, Editors. Smart home and smart city solutions enabled by 5G, IoT, AAI and CoT services. 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India. IEEE, 2014.

[52] Collotta M, Pau G. Bluetooth for Internet of things: a fuzzy approach to improve power management in smart homes. *Computers & Electrical Engineering*. 2015;44:137–1352.

[53] Amadeo M, Campolo C, Iera A, Molinaro A, Editors. Information Centric Networking in IoT scenarios: The case of a smart home. 2015 IEEE International Conference on;Communications (ICC), London, UK. IEEE, 2015.

[54] Zhang Y, Raychadhuri D, Ravindran R, Wang G. ICN based Architecture for IoT. IRTF contribution, October 2013, pp. 1–15.

[55] Coelho C, Coelho D, Wolf M, editors. An IoT smart home architecture for long-term care of people with special needs. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy. IEEE, 2015.

[56] Hossain MM, Fotouhi M, Hasan R, editors. Towards an analysis of security issues, challenges, and open problems in the internet of things. 2015 IEEE World Congress on Services (SERVICES), New York, NY, USA. IEEE, 2015.

[57] Internet of Things research study. Available from http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf. Last accessed on 1st June 2018.

[58] Santoso FK, Vun NC, editors. Securing IoT for smart home system. 2015 IEEE International Symposium on Consumer Electronics (ISCE), Madrid, Spain. IEEE, 2015.

[59] Li X, Lu R, Liang X, Shen X, Chen J, Lin X. Smart community: an internet of things application. *IEEE Communications Magazine*. 2011;49(11):68–75.

[60] Lu R, Lin X, Zhu H, Liang X, Shen X. BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*. 2012;23(1):32–43.

[61] Li X, Lu R, Liang X, Shen X, editors. Side channel monitoring: packet drop attack detection in wireless ad hoc networks. 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan. IEEE, 2011.

[62] Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O, editors. Network-level security and privacy control for smart-home IoT devices. 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2015.

[63] Dorri A, Kanhere SS, Jurdak R, Gauravaram P, Editors. Blockchain for IoT security and privacy: the case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 2017.

[64] Lee C, Zappaterra L, Choi K, Choi H-A, editors. Securing smart home: Technologies, security challenges, and security requirements. 2014 IEEE Conference on Communications and Network Security (CNS), San Francisco, CA, USA. IEEE, 2014.

[65] Apthorpe N, Reisman D, Feamster N. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic. arXiv preprint arXiv:170506805. 2017, pp. 1–6.

[66] Nag A, Mukhopadhyay SC, Kosel J. Flexible carbon nanotube nanocomposite sensor for multiple physiological parameter monitoring. *Sensors and Actuators A: Physical*. 2016;251:148–155.

[67] Nag A, Afasrimanesh N, Feng S, Mukhopadhyay SC. Strain induced graphite/PDMS sensors for biomedical applications. *Sensors and Actuators A: Physical*. 2018;271(1):257–269.

[68] Afsarimanesh N, Mukhopadhyay SC, Kruger M. Sensing technologies for monitoring of bone-health: A review. *Sensors and Actuators A: Physical*. 2018;274:165–178.

[69] Devices A. AD5933: Impedance Analyzer. Internet: Analog Devices [cited 4th September 2017]. Available from http://www.analog.com/media/en/technical-documentation/data-sheets/AD5933.pdf. Last accessed on 1st June 2018.

[70] Mankar J, Darode C, Trivedi K, Kanoje M, Shahare P. Review of I2C protocol. *International Journal.* 2014;2(1):1–6.

[71] Thingspeak. Thingspeak. 2017 [cited 26th August 2017]. Available from https://thingspeak.com/.

[72] Website A. Ciao. 2017 [cited 26th August 2017]. Available from https://www.arduino.cc/en/Reference/Ciao. Last accessed on 01.06.2018.

[73] Afsarimanesh N, Alahi M, Mukhopadhyay S, Kruger M. Smart Sensing System for Early Detection of Bone Loss: Current Status and Future Possibilities. *Journal of Sensor and Actuator Networks*. 2018;7(1):10.