A Literature Review of IoT Technologies for Home Automation

Submitted by,

Mukund Vinay Agarwal - 2017AATS0380G
Ashwin Kumar K - 2017B5A81034G
Dhruv Garg - 2017B4A30409G
Divyanshu Singh - 2018AAPS0673G

Prepared in partial fulfillment of EEE F411 Internet of Things

Under guidance and supervision of
Dr. K R Anupama
Assistant Professor, Department of EEE,
BITS Pilani KK Birla Goa Campus

Contents

List of Figures

List of Tables

I. Introduction

With the advancement in technology, standards of the human living conditions are also increasing. The Internet of Things allows us to increase these standards at a minimum cost, by providing an integrated mesh network of house appliances which gives the inhabitants access to certain data in the house and the ability to control some parameters remotely. A categorization of articles we have come across on IoT applications on intelligent smart homes is given in Fig 1.

In this literature survey we have looked at some particular aspects of the Intelligent Iot-driven Smart Homes and tried to cover them as extensively as we could. After a general discussion on smart-home architecture including the basic components, cloud computing and voice assistants, we try to discuss how Smart Homes can help caregivers. Then we focus on energy management in a smart home network and using this try to focus on ensuring security of the network. Finally we look at how Cognitive IoT based networks are the next step in Smart Homes.

II. Intelligent home architecture

Intelligent homes use connected home IoT devices to enhance the quality of living for its users. An intelligent home can even learn about residents to improve performance. IoT systems range from simple designs like control of lights and appliances. To this, the security of the house can be added. Safety of the house to check for gas leaks, fire alarms etc., can also be added. Also, features to manage the energy budget can be added.

A smart home system takes care of

- Home Automation and Ambience control
- Energy and Cost Management
- Health and monitoring
- Safety and Security

Modern homes usually have several appliances such as TVs, refrigerators, music systems, washers/dryers etc. Managing and controlling these appliances is cumbersome as each appliance has its control/remote control. For e.g., smart washers/dryers can be controlled remotely and notify when the process is complete. Smart thermostats allow the controlling temperature of rooms and use several learning algorithms to predict user preferences. Smart refrigerators keep track of item is low on stock. Smart TV's allow users to search and stream videos and movies from the Internet on a local storage drive. Searching TV channel schedule to watch programs on demand. Smart homes also have intruder alert systems that use cameras and PIR, and other motion detection sensor. In the case of intruders detected – the system alerts the user while also alerting the local police station. Smoke/gas detection systems can be used for protecting homes from fires or gas leakage. Smoke sensors, gas detectors (CO, LPG) leakage alerts the user through SMS as well as alerts the local authorities.

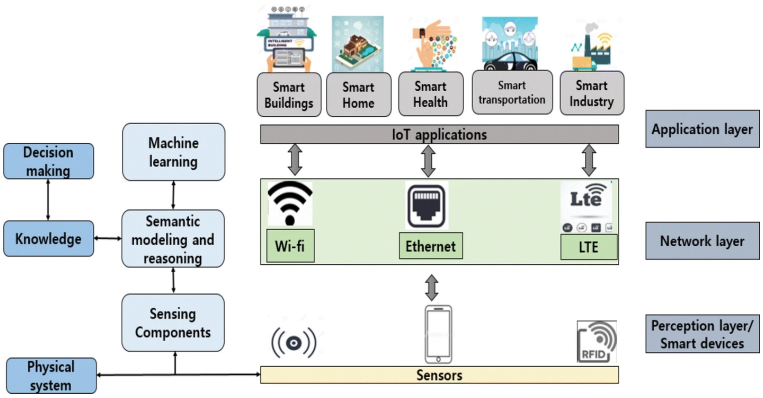

Figure 2. CIoT-Net: a scalable cognitive IoT based smart city network architecture [43]

A. Home automation platforms

Home automation softwares facilitate control of common home appliances, from a UI which could be a webpage, a smartphone app, or a tablet installed in the house. They have a special significance because they provide a common interface for the user to control multiple devices. Depending on the advancement, some platforms can even allow users to do very complex tasks by running customized scripts written by the user. As these softwares bring different kinds of devices, they generally support a variety of communication interfaces like Zigbee, Wi-Fi, BLE,XMPP, etc. The access control is made easier, remote and effective.

Now, there are two major categories of Home automation softwares that a user gets. First is the closed source, where the user would get most of the things professionally set-up. In these cases, one issue that could occur is the brand limited

devices. For example, Microsoft HomeOS works only on Windows, and not on Android or iOS. Similarly, if one chooses Samsung SmartThings, the devices that will be connected to the smartphone app will all have to be Samsung, and the Voice Assistant will be Bixby. But this also becomes an advantage as the control is highly optimized over the devices.

The second category is open source. Now, open source softwares are free to use, and they do not brand limit the users. Because of their generic nature, they might not always be optimized for the appliances they control, but will always give a basic amount of control. Major open source home automation platforms include openHAB, Home Assistant, OpenMotics, Jeedom, ioBroker, AGO control, etc.

B. Design of an intelligent smart home assistant

An intelligent home assistant is a one which responds according to the owner's movement in the home. As soon as the owner enters the house, all the sensors activates and it results on the illumination of all the lights in the house. Switching on of the AC, playing music on one say, automatic opening of the door, heating the water for bathing, and many more things can be done easily by the smart home assistant on the go. All of the components in a house are linked to a centrally controlled system. The owner of the smart home would have full access to the smart home on his smartphone even he his outside his home. To access one's home remotely, many options such as Internet, Bluetooth, GSM or wireless technology can be used. The overall system design can be divided into four modules.

Those are –

1) Speech Recognition Module
2) Power Control Module
3) Remote Control Module
4) Core Control Module

1) Speech Recognition Module: The voice input given by the operator is converted by the microphone from speech signal to the electric signal. This signal is further transferred to the speech recognition module which converts the analog signal in digital form and then this signal is transferred to the system. Further, it's upto the system to take the decisions with the help of the relay-based power control module.

Here the STT engine takes the recorded speech as an input and transforms it into written texts. Further, the TTS engine does exactly the opposite of it.

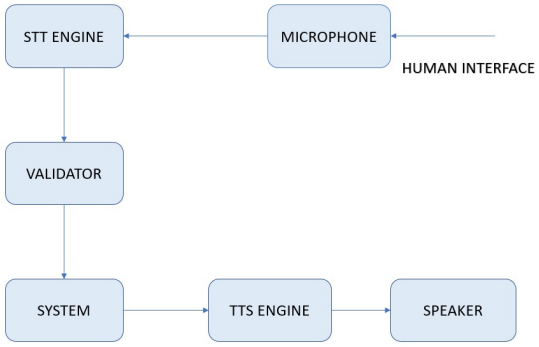

Figure 3. Flow chart of Speech Recognition Module

2) Power Control Module: A relay-based module responsible for switching on and off any of the smart home appliance device. It requires the input from raspberry pi or any similar tool related to it and based upon the input given by the tool, it switches on/off any of the device.

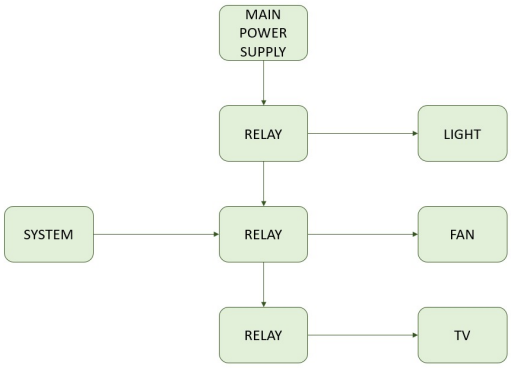

Figure 4. Flow chart of Power Control Module

3) Remote Control Module: The raspberry or its alternative based system is helpful in storing the current status of the devices into a file and ultimately save them into a server in the cloud. All these device statuses can be fetched from the android or Web applications to display for the users. If any of the status of the device is changed by the owner on the web or on the android it

automatically changes the status of the specific device on the cloud server.

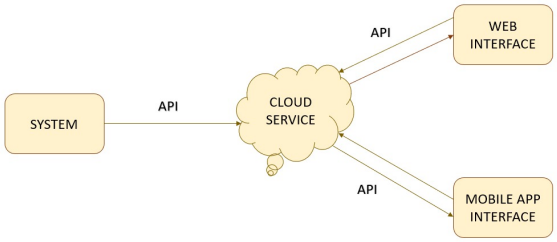

Figure 5. Flow chart of Remote Control Module

4) Overall system: The combination of all the modules discussed above contributes to the making of the overall system. This overall system has the core modules included in it in the form of various program-based applications.

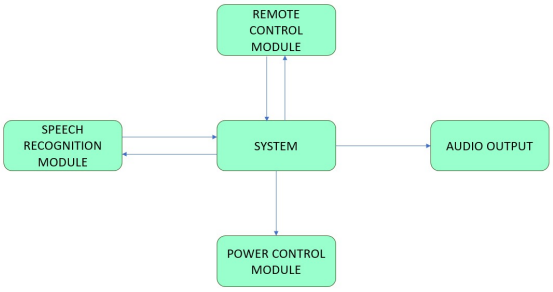

Figure 6. Flow chart of Overall system

C. Security systems for Smart Homes

One major application of IOT in Homes is the power of monitoring the premises from anywhere. Smart security systems are highly customizable and available as do-it-yourself kits or as full-blown setups that include professional installation and monitoring. Therefore, customers have a choice in systems where they can either monitor the house themselves or can have it monitored by third parties on payment basis. There's also options in which one can have individual devices (like motion sensors, door locks, security cameras) rather than dedicated security systems which can be monitored via smartphones or tablets. As any general system would, the smart home security system can be connected to the Wi-Fi router of the house, giving access to customers remotely.

1) Ensuring Low Power Consumption : : In a perfect world, all home security components would use the same wireless standard to communicate with the main hub, but factors such as power requirements, signal range, price, and size make it virtually impossible to settle on just one. For example, smaller components such as door/window sensors typically use Z-Wave or Zigbee technology because they don't require a lot of power and can be powered by smaller batteries. They also operate in a mesh topology and can help extend the range of networked devices. However, neither protocol provides the bandwidth that you get with Wi-Fi, which is why it is usually used in security cameras to provide smooth video streaming, and in other devices that require a fat pipe. Moreover, Z-Wave and Zigbee devices are connected and controlled using a hub, while Wi-Fi devices can be connected directly to your home network and controlled with an app. Finally, Z-Wave and Zigbee devices use AES 128 encryption, and since they operate in a closed system with a dedicated hub, they offer more security than Wi-Fi devices.

2) A few Intelligent features : : With advancement in the intelligent IoT systems, more and more features are coming up. These features might be simple in nature but have a significant effect on the lives of people. For example, as soon as the smoke alarm goes off, all the doors should be unlocked. Or maybe the cameras could start recording as soon as a particular sensor goes off. Clearly, the first one will help in saving lives in case of fires and the second will simply save up the memory usage, electricity usage, therefore, giving monetary advantages to the customer. All these with the advantage of easy modifications in the system using smartphones, give the users a lavish security system at a minimal cost. Another important feature to be noticed is the Video Doorbell which offers an easy way to see who is at your door without having to open or even get close to the door. These devices connect to your Wi-Fi network and will send an alert when someone approaches your doorway. They'll record video when the doorbell is pressed or when motion is detected, and usually offer two-way audio communication that allows you to speak with the visitor from anywhere via your phone. Another famous technology to be looked at here

is, IFTTT. IFTTT derives its name from the programming conditional statement "if this, then that." What the company provides is a software platform that connects apps, devices and services from different developers in order to trigger one or more automations involving those apps, devices and services. This can allow the user to not necessarily go for a particular company for all the components needed in the system. The users as per their requirements can go for door locks, motion sensors, smoke detector systems of different companies and use IFTTT to bring them to a common platform. This especially comes in handy to people trying to install the system on their own. So,many companies also give the IFTTT support. A comprehensive table of commercial smart home devices and their feature is present in Table 14.

III. Healthcare oriented Intelligent Home Systems

The technology of Smart Homes (SH), as an instance of ambient assisted living technologies, is designed to assist the homes' residents accomplishing their daily-living activities and thus having a better quality of life while preserving their privacy. The smart home is equipped with a collection of software and hardware components put together to monitor the living space, and infer/understand the behavior of its residents while preserving privacy.

Rise of aged population and the following need of supporting healthcare systems that are dependable and affordable. Elderly homes also face huge financial pressures ,being responsible for providing formal care as well as healthcare services to the residents individually. Statistically, the healthcare costs are almost similar between hospitals and care-homes.

Smart Homes technology is considered as a way to reduce living and care costs and is also looked up to as a technological panacea for improving the quality of living for people with care needs. It has been applied for many purposes (Miskelly 2001) [39] like energy saving, security and safety, fall detection, light management, smoke and fire detection etc. using various solutions such as video monitoring, alarms, smart planners and calendars, reminders, etc. Equipped with sensors, actuators and eventually cameras to collect different types of data about the home and the residents, Smart-Home can enable automatic systems or caregivers to control the environment on behalf of the residents, predict their actions and track their health condition.

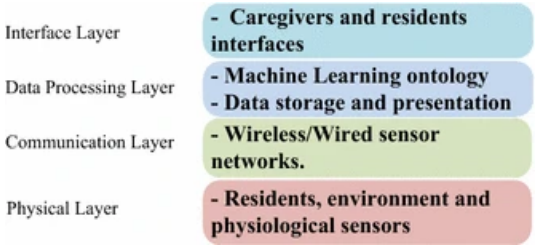

Figure 7. The layered architecture of an SH[7]

Each layer of the system has its own function and comes with its own challenges to be dealt with. Data is collected as the physical layer by sensors, transmitted through the communication layer to the processing unit in the processing layer where it is analysed for activity recognition and behaviour patterns discovery. The outcome of the analysis in the form of specific information, alerts or warnings may be communicated through the interface layer to various stakeholders (resident, caregivers, resident's relatives).

A. Sensors Hardware

These are the Hardware component of the entire Intelligent Home system, and involve integration of sensors and associated actuators within a single network that represents the home as a Virtual System over the Internet. Many communication technologies and protocols to integrate the home devices and sensors in the home are available such as Bluetooth, ZigBee and PLC. Sensors provide data as either discrete or continuous data states/streams, largely depending on the environmental factors and activity being monitored. In particular sensors have commonly been seen to capture the following data :

- Strain and pressure
- Position, direction, distance and motion
- Light, radiation, temperature and humidity
- Type of material (e.g., solid, liquid and gas)
- Sound – Image and video

– State of the object (e.g., present, not present)
– Physiological measurements (e.g., blood sugar, blood pressure)

Through the deployment of sensors around the objects,home and environment, the SH-systems infers: **Activities of the residents ; States of the objects ; States of the environment**.

Types of Sensors:

A) Discrete state

Simple state sensors that can return a binary output of an event happening such as opening and closing of doors, detecting motion in an area/room and accordingly notifying the smart-home system.

Commonly used sensors:

- Passive-Infrared Sensors (PIR): Used to detect motion,can be used to identify occupancy-status of rooms and is commonly part of security systems.
- Contact-Switch Sensors: Typical use to find open/close state of doors like cabinets,fridge. Packaged with pressure sensors, can be used to detect occupancy such as when a person sits on a chair in a room.
- Radio Frequency Identification(RFID): Identify object-tags or people with unique IDs and reading any associated data.

The Intelligent system can attempt to infer what activities the resident is performing, by inferring from a combination of these discrete parameters and identify abnormal behaviour. Such as cooking may be inferred by detecting occupants in the kitchen coupled with opening and closing of the fridge door

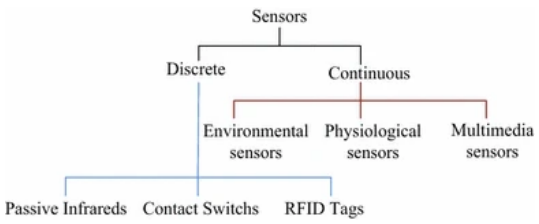

Figure 8. classification of sensors[7]

B) Continuous State sensors:

Generated data is usually complex, such as data streams, images, sounds, real-numbers etc.

Types-

- Environmental: capture data such as light, humidity, pressure, noise etc.
- Physiological : Part of wearable sensors that can create a Body-Area-Network on the wearer. Monitors health parameters such as blood glucose, blood pressure, ECG, EEG, EMG, pulse etc.

mPHASIS (Kulkarni and Ozturk 2011)[31] is an end-to-end healthcare Information-system that utilizes the BAN sensors to measure health parameters. The caregivers have access to the monitored data, are given alerts on patients health and medicine-schedules.

- Multimedia : Consist of mainly Video cameras , microphones etc. Audiovisual recognition can be the most efficient way to monitor patients activities like climbing and falling and confirm if medicines have been administered correctly.

Another system, called COACH,(Mihailidis et al. (2008)[17]) was proposed to assist the elderly with dementia through the process of washing hands. COACH uses video frames to discover the hand position relying on the partially observable Markov decision processing model (POMDP). The system features a multimedia guide and also alerts the caregivers when the person is in a risky situation as identified by the system (e.g., when the person is not moving, the sink is full). A list of Sensors used by various studies is presented in Table 15

B. Communication Network and Infrastructure

This forms the backbone of the hardware layer by connecting sensors and gateways together to enable the flow of information through the Intelligent Home. It carries the monitored data from the installed sensors to the data sink(coordinator) and forwards the control data to the actuators in the smart home system.

Network of sensors/actuator to data sink or coordinator

- LPW -Low Powered Wireless networks (e.g., z-wave,LoRa, zigbee, bluetooth, RFID)
- PLC -Power line communication standards (e.g., X10)
- PAN -Personal computer networking protocols (e.g., WIFI)

- MTS or UMTS -Universal Mobile Telecommunications systems

1) Low Powered Wireless networks: These protocols are designed so as to sustain a network of devices/sensors that are energy constrained. These devices generally spend most of the time in power saving mode, which could otherwise break the network connectivity.

Few LPW standards are:

1) ZigBee: very prominent wireless protocol used in off-the-shelf products as well as Do-it-Yourself Kits by many tinkerers and teaching aids. It operates on the 2.4GHz band, and gives a data-rate upto 250kbps. The maximum transmission range possible is 75m if the transmitter is powerful enough. It has been deployed in many Home-based IoT applications such as-
   a) U-Health - Used 12 types of wireless sensors to monitor health parameters of the elderly.The sensors were ZigBee based that transmit the data through the phone to a server that could visualize the data for the caregivers (Lee et al. 2009[32]) . Participants reported 8.5 on 10 for satisfaction
   b) Unattended Autonomous Surveillance (UAS)-Van Hoof et al. (2011)[59] developed a system to aid mild-stage dementia patients. They deployed an array of ZigBee based sensors in living-rooms,bedrooms and kitchen.The system tracked patients' sleep, movement, falls etc. It could detect and alert the caregivers in the case of any patient falling.
2) Bluetooth: Extremely low cost LPW solution that is suitable for PAN and BAN. It supports a maximum bandwidth of 1Mbps over the 2.4GHz signal-band and a range of 10m. But this is not commonly used for smart-homes as it supports fewer devices as well as data-rates when compared against ZigBee and WiFi, as pointed out by Lee et al. (2007)[33]
3) RFID: This is a system of tags and computer-based readers that automatically identifies the tags and supports frequency ranges in low,high and ultra-high. The reading range is directly proportional to the frequency used. It can be used passively for recognizing residents with tags and an active RFID system can be created for environment monitoring (Yamazaki (2006)[65]).

2) Power line communication standards: PLC technologies allow the networking over the available Electrical terminals in the home. Although this is cost effective as it reuses existing power lines, most wired solutions are very restricted to deploy on large scales. Thus most IoT systems such as smart-homes usually deploy a mixed network of wired and wireless communications.

Following are few standards for PLC networks:

1) X10: This is an Internationally accepted protocol which allows devices to communicate over the existing Electrical house wiring. It can complement a wireless network to cover the whole house. Rantz et al. (2008) deployed an X10 sensor network for a retirement home to monitor daily activities and health.
2) Home-Plug: Are enhanced versions of X10[(Hazen 2008)][24] by the Home-Plug Power-Line Alliance that supports a bandwidth of 200Mbps upto 350m indoor power-line reliably without packet-drops.
3) KNX: It is a heterogeneous protocol for smart buildings and has incorporated Internet-Protocol along with BatiBUS, EIB and KNX-RF into a single package (Tompros et al. 2009)[57]. This allows KNX to support Twisted-Pair, power-lines and Radio-Frequency for transmission.It allows one to combine Wi-Fi with low power wireless protocols such as ZigBee,Z-wave (Viani et al. 2013)[61].

3) Mobile Telecommunications systems: These networks are now widespread with the advent of smartphones and are built to handle massive data-loads and a multitude of devices. These networks support multimedia data transmission such as videos and web-pages. As these networks are extremely pervasive and necessary, they can be exploited for a Smart-home network.

Salvador et al.(2005)[50] implemented a MTS and Internet services-based system for out-of-hospital follow-up of cardiac patients ,called Airmed-cardio. Every patient has a portable mon-

itoring setup and a smartphone that transmits the data through the MTS, which is then monitored by the hospital.

C. Data and Knowledge Engineering:

This is the part of an Intelligent Home System and any other Internet-of-Thing enabled technology that gives them the power of cognition and intelligent behaviour. All Internet-of-Thing applications collect tonnes of data which is then sent to servers/cloud for data processing and analysis. Prior to analysis, the data undergoes Pre-Processing and Cleansing that may be performed locally(Edge computing) or at the cloud. After the data is prepared, analysis is done to classify,interpret activities like- mining behavioral patterns, recognizing activities, detecting abnormal behaviour etc. After analysis, Intelligent home takes decisions and performs actions accordingly such as sending alerts,booking appointments etc.

Aims of and focus areas of Intelligent algorithms in healthcare:

- Data Visualization : present data that tracks the resident's health correlated with their activities
- Analysis and Identifying potential health anomalies and accordingly notifying the invested people
- Visualize progress of any disease such as monitoring tiredness Setting reminders and prompt residents to complete medications, exercises, food
- Aid residents in performing tasks that may be difficult for them , such as getting down the stairs, calling for help

The common computational models used for activity recognition in SHs will be highlighted and related studies will be summarized in Table 16

1) Decision Tree: This approach aims to model the relationships between the input data and the resulting output. Used for classification purposes with discrete outputs by use of class labels. The logic-structure consists of nodes that represent features and branches that represent the values of the features. The leaf nodes represent the class labels The resultant trees are used to create Rules, that the Smart-Home system can use to classify the current-state of residents as safe or at potential risk by calculating the class labels. Such a system is also known as Rule-Based-System(RBS).

Trees can be built through an induction process by running algorithms on a dataset. Some known algorithms used are - TDIDT/ID3, C4.5, CART, MARS, and CHAID. Trees can be generated by recursive algorithms that grow the tree and algorithms that prune the tree dynamically. Algorithms like C4.5 and CART employ both: growing and pruning of the tree. It is important to note that the accuracy of any algorithm is not absolute, but rather varies case-to-case basis.

Example:

1) In Prossegger and Bouchachia (2014)[44]- the authors applied decision trees to model activities of daily living in a multi-resident context. An extension of ID5R, called EID5R, was proposed where the leaf nodes are multi-labeled. E-ID5R induces a decision tree incrementally to accommodate new instances and new activities as they become available over time. To evaluate the proposed algorithm, the ARAS dataset which is a real-world multi resident dataset stemming from two houses was used. E-ID5R performs differently on activities of both houses: for house A whose data is quite challenging, the classification rate was modest (40 %), while for house B the rate approached 82 %.
2) C4.5 based implementations :
    a) Isoda et al. (2004)[26] - aimed to classify the actions of residents as a function of their location and information of the objects they touch. The data was collected using RFID for sensing objects, while pressure sensors were used to pinpoint the location of the residents. In all, the classifier achieved a greater than 90% accuracy. Ravi et al. (2005)
    b) [47] - Focused on differentiating an individual's movement activities such as walking, moving over stairs, running, and even brushing their teeth. The device employed were wearable sensors such as accelerometers. It was observed that C4.5 achieved 97.29 %

when trained and tested on data from the same user over many days. An accuracy of 98.53 % was achieved when C4.5 was trained and tested on data stemming from many users and over many days and 77.95 % when trained and tested on data not from the same day.

2) Fuzzy Logic : A fuzzy set as "a class of objects with a continuum grades of membership". Such a set is characterized by a member-mapping which assigns a value in the continuous interval from 0 to 1, that denotes how closely related are the objects. Fuzzy sets and logic by Zadeh (1965)[21] was an expansion to the classical set theory. In this manner, Fuzzy Logic is a method of reasoning that resembles human linguistics and reasoning; as it considers all intermediate possibilities between binary values of YES and NO. The smart-home Rule-Based-Systems can then be expanded to work on Fuzzy If-else paradigm, example; "Turn off AC when room is at a comfortable temperature" condition can be created that understands the comfortable temperature ranges of each individual. Here the input data first gets "Fuzzified" before being processed by an RBS Inference-Block, and the output may need to be "Defuzzified" prior to being translated into a Real-World action using . The system generates confidence-levels while making decisions.

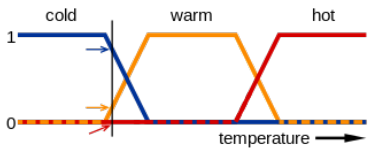

Figure 9. Temperature mapping to fuzzy set

The figure maps temperature to a fuzzy set of qualitative 'linguistic-expressions' consisting of cold,warm and hot. The arrows in the figure may be interpreted as intermediate states of slightly-warm , 'not-hot' etcetera.

Fuzzy RBS to recognize different activities, have been made using classifiers such as:

1) In-depth view of common fuzzy classifiers was found in Bouchachia A (2011)[11] .
2) iDome by Hagras et al. (2004[22]) was a smart environment monitoring project that used fuzzy logic for implementing a RBS controller. The classifier rule outputs were function mappings based on the preferences of the residents in a sensor equipped dormitory flat. The dataset was generated over 2 months with 280 rules.
3) IFS (Incremental Fuzzy-classification System) ,a dynamic classifier based on Generalized fuzzy min-max neural networks (GFMMNN) was introduced by Bouchachia A (2011)[11] .
4) Class0, eClass1, k-NN, NB and HMM were implemented by Ordonez et al. (2013)[42] which concluded that evolving classifiers performed better even with large datasets.
5) GT2FC stands for Growing Type-2 Fuzzy Classifier, which is an online self-learning and uses data streams was pioneered by Bouchachia and Vanaret (2014)[12]. It has been proposed for ambient-intelligent applications such as Smart-home that learns and recognizes the activities of its residents. The accuracy achieved was 81.6% and outperformed other classifiers on the iDome dataset.

3) Artificial Neural: Networks Neural networks consist of a network of connected nodes that each can perform a few mathematical operations on some inputs-numbers. The uniqueness of this network is that it is highly interconnected so as to initiate the neurons connections in a human brain by cascading the inputs and outputs of the nodes. Every node or 'artificial' neuron assigns weights to the inputs that it receives from the previous nodes. The ANN consists of layers of such densely connected nodes and attempts to 'tweak' the assigned weights to match final outputs with an expected output which is known as ' learning'. Multiple parameters such as connection-types and activation functions are used to shape the layered-structure and connections of the ANN while applying different 'rules' influence its learning behaviour.

Connection types- Feed-Forward Networks, Recurrent-Neural Networks etc. Learning Rules: Hebbian rule, Perceptron learning, Back-Propagation etc. Activation functions : Sigmoidal, Hyperbolic-Tangent, etc.

ANN can be used for activity classification, control of appliances, anomaly detection as well as dependable activity prediction in a smart home

environment. In healthcare based smart home applications, ANN can be used for diagnose and monitor chronic illness as well as building medical decision systems. An example for these are found in (Khan et al. 2001[29]; Lisboa and Taktak 2006[35]; Er et al. (2010)[18].)

Some well used combinations of these ANN-parameters give rise to the following broad types:

- MLP : Multi-Layer Perceptron
- ESN : Echo State Networks
- RBFN : Radial Basis Function Networks

A few use cases:

- (Mozar 1998[40]) ,used MLP neural Network to control Energy Consumption in accordance with the lifestyle of the residents and relied upon the Back-Propagation learning Algorithm
- MavHome project (Cook et al. 2013b[16]), an MLP based framework was proposed to detect activity anomalies and identify repetitive tasks performed by residents by inferring data from environmental sensors and contact-switch-sensors.
- An online learning system (Rivera-Illingworth et al. (2005)[49]) used a Recurrent-Neural-Network that recognised activities such as sleeping,eating, computer-usage and abnormal behaviour. The Online-Mode of operation ,which was facilitated by the Evolving Connectionist System (ECoS) framework, allows a deployed network to expand the number of sensors and thus the scope of activity detection.
- One-Pass Neural Network (OPNN) was employed by Li et al. (2008)[45], for activity recognition that also ran online. The control dataset was room completely set up with sensors, and the participant residents were asked to list their activities to produce the Activities of Daily Living(ADLs) for the dataset. Detection of abnormal behaviours was done by creating an additional layer of the network.

4) Naive Bayes Classification: This classifier runs on simple probabilistic models based on Bayes' theorem to make decisions. The classifier considers the inputs as independent variables and creates a probability boundary to take decisions. Due to being a probabilistic algorithm, NBC working is simple,traceable and gives a higher degree of control to the designer. NBC classifications have been employed in monitoring environments both with and without visual sensing-data, and reached an accuracy of 89% in 2 independent studies. Tapia et al. (2004)[56] -Visual data targeting Phone-use, Drinking water and Dining Messing et al. (2009)[37].

5) Hidden Markov Models: Hidden Markov models (HMMs) are the lego blocks of computational sequence analysis.They are used for making probabilistic models of linear sequence 'labeling' problems.They baseline is that we can build complex models just by drawing an intuitive picture.We imagine an HMM generating a sequence. For eg : Activities that can be linked together in a smart home Door Closed-AC switched on - Fridge open- Water taken - Light closed -House lift opened.

Algorithm:

Visit a state - emit a residue from the state's probability distribution . Choose the next state to visit according to the state's transition probability distribution. Two strings of information are generated : underlying state path (the labels) and observed sequence each residue being emitted from one state in the state path. Based on the observed sequence, we infer the hidden state path or hidden Markov chain.

In smart homes,the model can learn behavior patterns of users and provide services to residents automatically. As a result, different values of daily temperature sections, motion sensory activities and Wi-Fi based activity mapping are characterized as hidden variables, which guide user activities.

6) Conditional Random field: Conditional Random Fields are based on 'Discriminative graphical Models' in contrast to above mentioned generative classifiers (Hidden Markov) and are used to find hidden states and transitions from the observed data sequences. CRF primarily works on only Conditional Probability calculations rather than Joint-Probability. It is also flexible enough to accept arbitrary and dependent relations between the sequences of observations. Unlike HMM, CRF also discards the assumption of independent variables, allowing it to capture virtually any relationships between an observation-variable and the hidden-states.

Amongst the probabilistic models, CRF has been seen to achieve highest accuracy in activity recognition. CRF has outperformed HMM, NBC as well as the HSMM variant for multiple activity datasets(ADLs) in two separate comparative studies namely in Kasabov (2007)[2], van Kasteren et al. (2010) [60]

7) Emerging patterns: Emerging patterns are sets of items whose frequency changes significantly from one dataset to another.They can be utilised to discover distinctions inherently present amongst a collection datasets and are a great way for constructing accurate classifiers. Instance 1: {location =kitchen, object = stove} is an EP for the activity "cooking" The set of EPs of an activity constitute the activity model for the activity.

Emerging Patterns (EPs) (Gu et al. 2009)[46] were used to model and discriminate the activities.It also shows how activity models can be built from sensor readings using EPs. A real-world data set was collected from wearable sensors (RFID-wristband readers and iMote2 sets) by 4 people. In all 26 common ADLs such as coffee making, tea making, oatmeal making, shaving etc. have been considered and EPs were then generated for each activity and using time-slice accuracy to recognize activities through intervals of time, an average accuracy of 85.84 % was achieved for different activities.

8) Ontological modeling: Ontology is a way to model the properties of a given domain and how they are related by defining a set of concepts and categories that represent the subject. Activity ontologies describe the hierarchy of activities, activity types and their relationships using languages like OWL and RDF. Ontological reasoning is used to recognize activities by identifying contextual information such as sensor reading, location of persons and objects, properties of objects, etc.

The following summarises a few papers on the same :

- Chen and Nugent (2009)[14] - Described an algorithm for recognizing activities using ontologies. By aggregating sensor observations along a timeline, a specific situation that corresponds to an unknown activity could be reached. For example, the activation of the contact sensors on a "cup" and "milk bottle" can link the "cup" and "milk" to the unknown activity through a concept "hasContainer" and "hasAddings" properties - like "hasContainer(cup)" and "hasAddings(milk)". By matching this situation against activity ontologies, the activity class that mostly overlaps with the situation (e.g.,"MakeDrink") is considered to be the actual activity.
- Riboni et al. (2011)[48] - Evaluate the effectiveness of the ontological approach based on the dataset described in van Kasteren et al. (2008), and showed that ontological techniques underperform data-driven techniques like HMM in absence of temporal reasoning. But when ontological techniques were extended with temporal information, their effectiveness (80.3 % accuracy) becomes comparable to HMM (79.4 % accuracy).

9) Context aware reasoning : Context-aware systems are concerned with the acquisition of context gathered from sensors and adapt their reactions to the behavior based on the recognized context using reasoning techniques. It highlights the significance of contexts to recognize the environmental conditions within the living space to help make the smart home system intelligently interactive and self-adaptive to ultimately ease user's tasks. There exist several approaches for context modeling and reasoning such as Unified Modelling Language, Object-oriented Models, key-Value models, and domain/web ontologies. The latter enables the system to define contexts semantically and share common knowledge of the structure of context among users, devices, and services (Gu et al. 2004)[55].

Some studies that used Context-aware Reasoning-

- Helal et al. (2005)[25]- Introduced a reference model for healthcare context-aware SHs. The context was generated by a set of sensors and actuators that were managed through OSGi (Open Service Gateway initiative) service bundles. System objects represented the sensors and actuators in the environment and were modeled along with contexts using ontologies. Authors presented two mere applications of "Smart Floor" and "Smart Plug" to prove the effectiveness of the system.
- Wongpatikaseree et al. (2012)[63] -

Introduced a context aware activity recognition system. An ontology was exploited to model the context which is obtained through a set of sensors. To handle various activities of daily living, especially in ambiguous situations, the context is augmented with information of some simple activities such as watching TV, relaxing and sleeping, were simulated.

- Riboni and Bettini (2011)[64]- Implemented a hybrid of ontology and statistical context-aware activity. Data from activities such as walking, brushing teeth, writing on a blackboard and hiking were collected via a phone GPS and Accelerometer, and an accelerometer wristband on an Android platform. The activity recognizer relied on an ontological reasoning which is combined with statistical classification to recognize activities and gave an accuracy of 93.44%

IV. Energy management solutions

Using energy efficiently in smart homes saves money, enhances sustainability and reduces carbon footprint at large. As a result, the need for intelligent energy management is on the rise for smart homes and smart cities in general. The lack of low cost, low maintenance and easy to deploy technology has limited a large-scale deployment of such systems. The large amount of data collected throughout different cities of a country presents multiple challenges in data storage, organization, and analysis. Internet of Things (IoT) technology and Big Data are the most sought out solutions to solve these challenges. IoT technologies can provide a ubiquitous computing platform to sense, monitor and control household appliances energy consumption on a large scale. This data is collected with the help of many different wireless sensors installed in residential power monitoring units. Similarly, Big Data technology can be utilized to collect and analyze large amounts of data [6]. Data analytics on this data using a business intelligence (BI) platform plays an essential role in energy management decisions for homeowners and the utility alike. The data can be monitored, collected and analyzed using predictive analysis and advanced methods to actionable information in reports, graphs and charts. Thus, this analyzed data in real-time can aid homeowners, utilities, and utility eco-systems providers to gain significant insights into smart homes' energy consumption. The energy service providers can use the power consumption data available with an analytics engine to provide flexible and on-demand supply with appropriate energy marketing strategies. Being aware of their consumption behaviour and having a close interaction with the electricity utilities can adjust and optimize home users power consumption and reduce their electricity bills.

A. Energy Harvesting and Management

In order to have an effective cost-saving system, it is necessary to monitor and control the operation of residential loads depending on the aggregate power consumption over the desired period, the peak power consumption, the effect of weather/atmospheric conditions and consumption slab rates. This is where the combination of IoT technology, Big Data analytics and BI comes into play for implementing energy management solutions on a local and national scale. Finally, as an additional advantage, IoT also enables seamless remote access control of home devices where the customers get online access to the ON/OFF usage pattern of in-home appliances via a personal computer or a mobile phone.

Bharat et. al.[9] focused on the advantages of home automation such as - reduced installation cost, system stability, easy extension, aesthetically benefited and integration of mobile devices.

Farzana et. al. [53] in their research proposes an implementation of smart home automation system by dividing our regular household appliances into two categories, low load and some scheduled high load appliances. After automation and scheduling, a solar system power supply has also been incorporated that can supply power to some appliances and reduce power consumption from national grid. This system also provides a detail analysis on energy management which has been developed by measuring power consumption throughout a year in different seasons.

Another interesting approach by for implementing energy efficient automation is presented by Michael C. Mozer in [40], where they have developed a home system that essentially programs

itself by observing the lifestyle and desires of the inhabitants, and learning to anticipate and accommodate their needs.The system controls basic residential comfort systems-air heating, lighting, ventilation, and water heating. They call the system ACHE. ACHE has two objectives.

- One is anticipation of inhabitants needs. Lighting, air temperature, and ventilation should be maintained to the inhabitants comfort; hot water should be available on demand. When inhabitants manually adjust environmental setpoints, it is an indication that their needs have not been satisfied and will serve as a training signal for ACHE. If ACHE can learn to anticipate needs, manual control of the environment will be avoided.
- The second objective of ACHE is energy conservation. Lights should be set to the minimum intensity required; hot water should be maintained at the minimum temperature needed to satisfy the demand; only rooms that are likely to be occupied in the near future should be heated; when several options exist to heat a room , the alternative minimizing expected energy consumption should be selected.

They archive the optimal control by defining an average energy cost function as

$$J\left(t_0\right)=\mathrm{E}\left[\lim_{\kappa\to\infty}\frac{1}{\kappa}\sum_{t=t_0+1}^{t_0+\kappa}d\left(x_t\right)+e\left(u_t\right)\right]$$

Where $J\left(t_0\right)$, is The expected average cost, starting at time t_0 , $d\left(x_t\right)$ is the discomfort cost associated with the environmental state x at time t, and $e\left(u_t\right)$ is the energy cost associated with the control decision u at time t

The goal is to find an optimal control policy (a mapping from x_t to decisions u_t) that minimises the expected average cost.

Il-Young Joo et. al. [28] proposes a distributed optimization algorithm for scheduling the energy consumption of multiple smart homes. In the proposed approach, home energy management's centralized optimization problem is split into a two-level optimization problem, one corresponding to the local home energy management system (LHEMS) and the global home energy management system (GHEMS) at the second level. Controllable household appliances (like an air conditioner, washing machine) are listed in the LHEMS within users preferred appliance scheduling and comfort level while the energy storage system (ESS) and power trading between households are listed in the GHEMS. In a simulation study, the proposed distributed algorithm shows almost equivalent performance to the centralized algorithm in terms of the electricity cost and the consumer's comfort level. The impact of different network topologies on the proposed algorithm was also analyzed. The result provides insight into the selection of the optimal network arrangement to achieve electricity cost saving.

Junyon Kim et. al. [3] proposed a very simple and appropriate idea on smart home which includes internal home appliances and their internal connectivity. They called this model HEMS(Home Energy Management System) model using Internet of Things (IoT).

Zhao et al. [66] in their paper propose a smarter model on scheduling system that can be useful on our home automation system design assignment.

Haque et al. presented an optimized standalone green hybrid system to supply electricity in an island of Bangladesh called Saint Martin[20].

F Shabnam [52] talked about eco-friendly cellular network where base stations of cellular network will harvest energy and trade the excess harvested energy to electricity grids.

Various studies have been steered in the application of IoT environment for HVAC control and scheduling methods to optimize HVAC energy consumption [[51], [19], [54]]

B. Node energy management

Apart from papers that talk about using IoT to optimise power consumption and financial aspects of a house as a whole, techniques to minimise the IoT device power are discussed in the following paper.

The authors of [15] discuss a fuzzy logic based mechanism that determine the sleeping time of an IoT devices in a home automation environment based on BLE. The proposed FLC determines the sleeping time of field devices according to the battery level and to the ratio of Throughput to Workload (Th/Wl). Simulation results reveal that using the proposed approach the device lifetime is increased by 30% with respect to the use of fixed sleeping time.

C. Smart Grid Architecture

Various frameworks describing a Smart Grid architecture have been proposed in the literature. The most widely adopted and adapted model by far is the reference model proposed by the U.S National Institute of Standards and Technology.[58]

Here the authors describe the Smart Grid as a set of seven interconnected domains. The first four domains (Bulk Generation, Transmission, Distribution and Customers) are responsible for the generation, transmission and distribution of energy but also for ensuring the two way communication between the customer side and the Advanced Metering Infrastructure (AMI). NIST's conceptual model inspires the rest three entities (Markets, Operations and Service Providers).

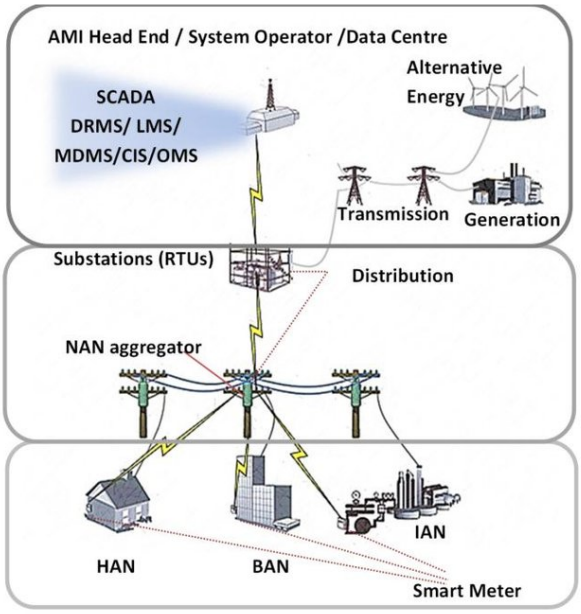

Figure 11. A multi-layered conceptual model of the Smart Grid's architecture. As described by NIST[30]

At the bottom layer of this model, one can find Home Area Networks (HANs), Building Area Networks (BANs) and Industrial Area Networks (IANs) i.e. wired or wireless networks in customer premises (homes, buildings or industrial areas) that interconnect appliances with smart meters and energy management devices, responsible for reporting the premise's consumption to the grid at any given time while also carrying messages from the grid back to the premise. Komninos et. al [30] breifly cover this Smart Grid Architecture in their paper.

The Smart Grid gives the consumer the opportunity to become a producer of energy as well as a consumer. By installing distributed energy resources at his premises, a customer can generate energy which he can sell to the grid at times when the demand surpasses the supply. Furthermore, by using his plug in electrical vehicle as a battery, a customer not only can store but also import energy from the grid at urgent times. Thus protecting it from damages caused by overloading.

One of the main advantages of smart grids is trans-active energy, where distributed energy resources, e.g. smart meters, develop towards Internet-of-Things (IoT) devices, enabling prosumers to trade energy directly, without the need of involving any centralised third party. The expected advantages in terms of cost-effectiveness would be significant, and thus technical solutions are constantly being developed and tested, and major utility companies plan large-scale deployment. However, introducing transactive energy in the smart grid entails new security threats, such as forging energy transactions. Federico et al. [36], in their paper, introduce an infrastructure to support reliable and cost-effective transactive energy, based on blockchain and smart contracts, where functionalities are implemented as fully decentralised applications. Energy transactions are stored in the blockchain, whose high replication level ensures stronger guarantees against tampering. According to transparent rules implemented as smart contracts, energy auctions are carried out, hence visible to all involved actors. Threats deriving from known vulnerabilities of smart meters are mitigated by temporarily keeping out exposed prosumers and updating their devices as soon as security patches become available. A smart contract is the back bone of many block chain based technologies where a contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code, thus eliminating the need for trust between the two parties.

Beyond academic works, several startups and companies work-ing on transactive energy and blockchain exist. Exergy [1] hasbeen the first company who applied blockchain to a transactivegrid by delivering the Brooklyn Microgrid, the world's firstever energy blockchain transaction platform. Electron [4], aUK startup, applies the blockchain

technology to the energysector, for building more efficient, resilient and flexible sys-tems. They offer a smart contract-based platform for energytrading, smart meter data privacy and facilities for energy andgas switching.

D. Communication

A HEMS requires a reliable communication network using WSN that can transport the consumption details and consumer load behavior periodically. In [[5], [41], [13]], an implementation of a HEMS Unit in a Wireless Sensor Network using a ZigBee Module to communicate with sensor nodes, is presented. The system monitors the device consumption data and sends control signals to end nodes during peak load hours. However, the lifetime of a WSN network deteriorates with time due to the deployment of new sensors in the network. Additionally, Han et al. in [23] introduced a system for monitoring power consumption using ZigBee as the communication protocol in a WSN. However, in this system the data was collected and aggregated solely by the home server which could lead to data loss in case of a system failure. Moreover, a bridge between ZigBee and TCP/IP stack would be required to connect this system to a community of homes. The above mentioned WSN networks have been extended to wider ranges in the IoT paradigm utilizing the GSM/GPRS networks to remotely control the end-devices in [[62], [38]].

V. Security for IoT systems

With the advent of smart homes, due to increased connectivity between a home system and many other large-scale systems, it is important that no malicious softwares enters the system and causes any kind of corruption. Let us consider this with the example of smart homes and smart grids. An energy aware household is expected to optimize the power budget used whilst also not slacking on comfort of the residents. This requires communication not only with the smart grid and the house, but also within all entities in the smart house. With all the communication depending on Information Technology, the system becomes vulnerable, which if exploited could not only damage the infrastructure of the home system but also the Smart Grid, which will have a large-scale impact. This also means that with the rise in Smart Grids, the role of Smart Homes and their residents becomes increasingly important.

A. Aspects of System Security

The following are the 6 aspects which are used while considering security of a system:

1) Confidentiality: only authorized personnel should have access to the data
2) Integrity: assurance that the accuracy and consistency of the data is maintained. Any and all changes in the data are detected.
3) Availability: Any network resource should be available to authorized entity.
4) Authenticity: of the communicating parties involved i.e., all communicating parties must be validated and the information sent by them must indeed be sent by them
5) Authorization: access control of each entity must be defined in the network.
6) Non repudiation: undeniable proof should exist for any claim of any entity

B. Impact Evaluation

Any security attack can be divided into categories based on whether the attack affects the system:

- Passive: Here the threat is only attempting to take information from the system network, without affect its resources. This information could be valuable and be used in different ways to plan a more disastrous attack. In dealing with such attacks, one focuses on prevention rather than detection, as that can be very tough.
- Active: Here the attack actively attempts to damage/affect the system network resources or operation. The most common amongst these attacks are masquerading, replay, message modification, denial of service and malicious software.

Now based on the impact of the attack to the system, the FIPS 199 standards can be used categorizing the attacks as Low level, Moderate level and High level, which in themselves fairly explain their damage extents.

The architecture of the Smart home system is divided into internal and external systems, where,

in this case, the Energy Service Interface (ESI) is in contact with the smart grid, and manages communication with the external system. And the Energy Management System (EMS) manages the internal system.

C. An outline of the assumed architecture

The architecture of the Smart home system is divided into internal and external networks, where, in this case, the Energy Service Interface (ESI) is in contact with the smart grid, and manages communication with the external system. And the Energy Management System (EMS) manages the internal system.

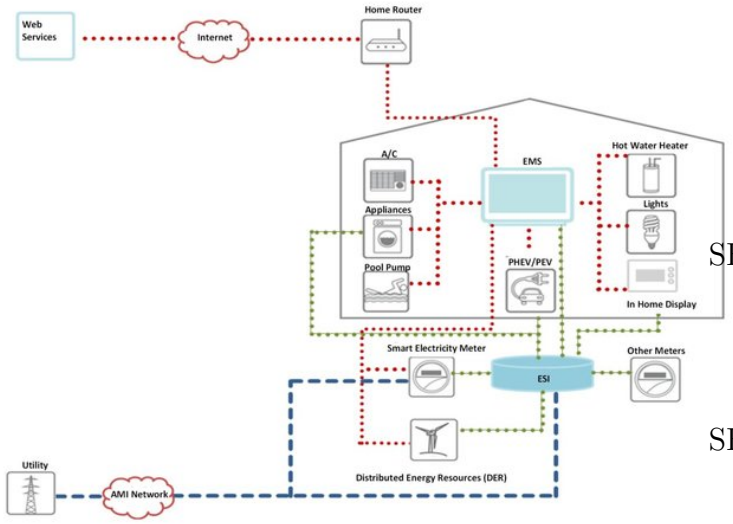

Figure 12. An overview of a Smart Home's architecture, internal and external environments.[30]

D. Smart Home Attacks

Broadly categorizing, the major possible attacks possible on the Smart Home system are in the following ways, when considered with regards to communication with a Smart Grid:

SH1) Attacks threatening successful device energy-consumption reporting – When energy consumption of data is collected at very short intervals, eavesdropping on such an information could be used to infer a lot about the lifestyle of the residents, hence create a major risk to privacy. Needless to say, how this data can be used to plan a more severe attack on the resident (e.g.: burglary, kidnapping). In the same place if it is managed to send false, or replayed data to the EMS, a false extra financial burden can be created for the consumer. This could also be achieved by impersonating the EMS rather than only "piggybacking" the network. (Generally low impact)

SH2) Attacks aiming Energy Import/Export signal at ESI - As the ESI is an entity in direct communication with the grid, any kind of message modification in the import export communication at a large scale could significantly impact the grid. Repudiation is also an important threat under this scenario since we expect the customer to be collaborating with an ESP for the management of his DERs due to his lack of experience. In such a case the customer should not be able to suggest that his ESP did not react when it should have/ or reacted when it shouldn't have. (Generally moderate Impact)

SH3) Physical meter tampering/reversal or removal – Mischievous customers try to tamper with the meter to decrease the bill, which needs to be stopped. (Generally Low impact)

SH4) Attacks against remote home monitoring and control – These basically include attacks where-in an adversary may impersonate the customer to control the devices in different ways (either switching on/off all devices or maybe modifying the messages). These attacks could have a low impact or may even be life threatening depending on the device(s) being abused. There is also the case of device impersonation where the commands sent remotely by the user are somehow directed to a device other than they were intended for. Therefore, Non-repudiation becomes a major factor in dealing with such attacks.

SH5) Attacks aiming the request for energy usage data -Eaves dropping on the detailed bill of energy consumption by the user is again a direct attack on the users' privacy, so this is another part where security protocols must be implemented. Table 17 gives a comprehensive list of

the smart home security issues with respect to a smart grid. It can be used as a basis for analyzing issues possible whenever we include another system in our analysis.

E. Security countermeasures

1) Confidentiality: : Cryptography is the most basic technique for achieving confidentiality. There are two types of cryptographic algorithms, Symmetric and Asymmetric. Symmetric algorithms (such as the standards AES and TDES) are expected to be used for the purpose of data encryption within the Smart Grid. Asymmetric algorithms on the other hand, (such as the approved RSA, DSA, ECDSA etc.) are expected to be used for the purpose of digitally signing messages.

2) Privacy:: With the deployment of smart meters, it is clear that through the data collected by the smart meter a lot could be known about the consumer, thus causing fear. Privacy can be achieved by the following ways: Anonymization: The data and its source have their link removed before the data reaches its destination for computation. Trusted Aggregators: Trusted third party can handle aggregation of metering data and its forwarding to the smart grid utility. Homomorphic Encryption Perturbation Models : Introduction of noise of known distribution Verifiable Computation Models Data Obfuscation Techniques: : Battery-based approaches that aim to conceal the amount of energy consumed by a premise by buffering or releasing their energy load.

3) Integrity:: One way to ensure integrity is using the cryptographic hashing techniques, which are designed for high integrity assurance in traditional networks. When using such techniques the sending side uses a hash function to compute the checksum of the message to be sent and attach it to the original message. Upon receiving the message, the receiving side applies the same hash function to the message and compares the resulting hash to the hash attached in the original message. Should the two hashes match, integrity is verified (i.e. it is proven that the message contents have not been altered in transit as a result of e.g. a message modification attack). Bhattarai et.al in [10], present their own lightweight digital watermarking technique as a simple, low-cost and efficient way to ensure defense against false data injection attacks. Digital watermarking is a technique of embedding digital data inside real time meter readings, with the watermark carrying unique information about the owner of the reading. The purpose of the watermark is to validate the integrity of data. Watermarked data are sent from the meter to the utility through high speed unsecured networks that are prone to false data injection attacks. To ensure the successful detection of these attacks , the meters use low rate and secured channels to securely transmit the watermarks. The utility thus receives both the watermarks and the watermarked data, in order to correlate them and detect false data injection attacks Furthemore, Load Profiling, Timestamps, Sequence Numbers, etc are other techniques that can be used to ensure high integrity assurance.

Fig 13 shows the various ways in which countermeasures can be implemented for different factors of security.

Confidentiality and Privacy
▪ Symmetric/Asymmetric Encryption Algorithms (eg. AES/RSA/ECC) ▪ Anonymization ▪ Trusted Aggregators ▪ Homomorphic Encryption ▪ Perturbation Models ▪ Verifiable Computation Models – Zero Knowledge Proof Systems ▪ Data obfuscation
Integrity
▪ Cryptographic Hashing Techniques (eg. SHA-3) ▪ Digital Watermarking ▪ Adaptive Cumulative Sum Algorithm ▪ Installation of known secure PMUs in network ▪ Load Profiling ▪ Timestamps ▪ Sequence Numbers ▪ Session Keys ▪ Nonces
Authenticity
▪ Keyed cryptographic hash functions (eg. HMAC) ▪ Physically Unclonable Functions ▪ Hash based authentication codes ▪ MAC-attached and HORS-signed messages
Non Repudiation
▪ Mutual Inspection with Smart Meters ▪ Unique keys for customer-AMI communication ▪ AMI transaction logging
Availability
▪ Alternate Frequency Channels according to hardcoded sequence ▪ Frequency Quorum Rendezvous ▪ Anomaly Based IDSs ▪ Specification Based IDSs
Authorization
▪ Attribute Based Encryption ▪ Attribute Certificates ▪ Attribute Based Access Control System based on XACML

Figure 13. An overview of security counter measures by goal.[30]

VI. Cognitive IoT as the future intelligent home

IoT systems from multiple domains such as ambience-control, home-security, and energy management are interconnected and constitute an intelligent home that provides comfort and convenience to users. The next step is personalization and adaptation to the intricacies of the inhabitants' behaviour. Here, we find Cognitive Computing to be a possible solution. Cognitive computing relies on the approach to training AI to function with human brain-like thinking. It learns from people their psychology, environment, voice, and social media to provide reasoning abilities like a human using IoT sensors such as headbands, wearables and phones. With the rapidly increasing number of connected devices, the data being generated is grouped as Structured and Unstructured, with the latter set being far more humongous in comparison. This is where the AI techniques used in Cognitive Computing undoubtedly have the advantage as they can be trained upon both structured and unstructured data and achieve higher accuracy as the data diversifies, truly imitating human cognition. [43]

IBM has come up with a cognitive computing system, known as Watson, which demonstrated machines' ability to think like humans. Watson learns data from documents with no human intervention and supervision and expresses itself like humans using natural language processing. Without internet access, Watson was ranked champion against human competitors in the show titled "Jeopardy!" in 2011. IBM Watson is also used as a commercially deployed Smart Home System, which is able to learn about the residents' behaviour and then take actions based on the analysis; that is, it does not have to be programmed to take all the actions. It can decide on its own and accordingly take specific actions based on the behavioural pattern it has learnt about the resident.

VII. Conclusion

While this survey paper does not claim to be exhaustive, it gives a reasonable overview of the techniques and technologies involved in smart homes. In this literature survey, we looked at some particular aspects of the Intelligent Iot-driven Smart Homes and tried to cover them as extensively as possible. After a general discussion on smart-home architecture, including the essential components, cloud computing and voice assistants, we tried to discuss how Smart Homes can help caregivers. Then we focused on energy management in a smart home network and tried to find articles focusing on the security of the network. Finally, we looked at how Cognitive IoT based networks are the next step in Smart Homes.

As such, SHs as a technology is not only a research topic, but it is actively being developed as a product in the market. Because it is versatile, it can be applied for various purposes like telecare, telehealth, comfort, energy-saving, etc. These applications share the same design principles but differ in terms of practical requirements. Each targeted application comes with its own and typical requirements that SHs have to consider. When developing SHs for a particular application, there are many choices, and therefore one has to take the specificity of that application into account. In other words, developing an SH system for healthcare is not the same as for comfort. Keeping this in mind, to highly optimise a system depending on the users specification there is usually a tradeoff between some of these domains. Hence through this literature survey, we tried to build a holistic view of all these domains upon which we shall develop our design project.

References

[1] Exergy - technical white paper,2017.https://exergy.energy/wp-content/uploads/2017/11/exergy-whitepaper-v7.pdf.

[2] *Evolving Connectionist Systems*. Springer London, 2007.

[3] Hems (home energy management system) base on the iot smart home. *Contemporary Engineering Sciences*, 9:21–28, January 2016.

[4] Electron.http://www.electron.org.uk. 2018.

[5] M. Abo-Zahhad, S. M. Ahmed, M. Farrag, M. F. A. Ahmed, and A. Ali. Design and implementation of building energy monitoring and management system based on wireless sensor networks. In *2015 Tenth International Conference on Computer Engineering Systems (ICCES)*, pages 230–233, 2015.

[6] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar. A smart home energy management system using iot and big data analytics approach. *IEEE Transactions on Consumer Electronics*, 63(4):426–434, 2017.

[7] Mohsen Amiribesheli, Asma Benmansour, and Abdelhamid Bouchachia. A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 6(4):495–517, March 2015.

[8] Mohsen Amiribesheli, Asma Benmansour, and Abdelhamid Bouchachia. A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 6(4):495–517, March 2015.

[9] S. Bharath and M.Y. Pasha. Iot-home automation. . *International Journal of Computer Technology and Research*, 5:4–6, April 2017.

[10] S. Bhattarai, L. Ge, and W. Yu. A novel architecture against false data injection attacks in smart grid. In *2012 IEEE International Conference on Communications (ICC)*, pages 907–911, 2012.

[11] Abdelhamid Bouchachia. Fuzzy classification in dynamic environments. *Soft Computing*, 15(5):1009–1022, May 2011.

[12] Hamid Bouchachia and Charlie Vanaret. Gt2fc: An online growing interval type-2 self-learning fuzzy classifier. *IEEE Transactions on Fuzzy Systems*, 22:999–1018, 08 2014.

[13] J. Byun, I. Hong, B. Kang, and S. Park. Implementation of an adaptive intelligent home energy management system using a wireless ad-hoc and sensor network in pervasive environments. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6, 2011.

[14] Liming Chen and Chris Nugent. Ontologyâbased activity recognition in intelligent pervasive environments. *IJWIS*, 5:410–430, 11 2009.

[15] M. Collotta and G. Pau. Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes. *Computers & Electrical Engineering*, 44:137–152, 2015.

[16] D. J. Cook, M. Youngblood, E. O. Heierman, K. Gopalratnam, S. Rao, A. Litvin, and F. Khawaja. Mavhome: an agent-based smart home. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003. (PerCom 2003).*, pages 521–524, 2003.

[17] Stephen Czarnuch and Alex Mihailidis. The design of intelligent in-home assistive technologies: Assessing the needs of older adults with dementia and their caregivers. *Gerontechnology*, 10:165–178, 12 2011.

[18] Orhan Er, Nejat Yumuşak, and Feyzullah Temurtas. Chest diseases diagnosis using artificial neural networks. *Expert Systems with Applications*, 37:7648–7655, 12 2010.

[19] K.F. Fong, V.I. Hanby, and T.T. Chow. Hvac system optimization for energy management by evolutionary programming. *Energy and Buildings*, 38(3):220–231, 2006.

[20] K. Foysal Haque, N. Saqib, and M. S. Rahman. An optimized stand-alone green hybrid grid system for an offshore island, saint martin, bangladesh. In *2019 International Conference on Energy and Power Engineering (ICEPE)*, pages 1–5, 2019.

[21] J. A. Goguen. L. a. zadeh. fuzzy sets. information and control, vol. 8 (1965), pp. 338–353. - l. a. zadeh. similarity relations and fuzzy orderings. information sciences, vol. 3 (1971), pp. 177–200. *Journal of Symbolic Logic*, 38(4):656–657, 1973.

[22] Hani Hagras, Victor Callaghan, Martin Colley, Graham Clarke, Anthony Pounds-Cornish, and Hakan Duman. Creating an ambient-intelligence environment using embedded agents. *Intelligent Systems, IEEE*, 19:12–20, 12 2004.

[23] J. Han, C. Choi, W. Park, I. Lee, and S. Kim. Smart home energy management system including renewable energy based on zigbee and plc. *IEEE Transactions on Consumer Electronics*, 60(2):198–202, 2014.

[24] Mark E. Hazen. The technology behind HomePlug AV powerline communications. *Computer*, 41(6):90–92, June 2008.

[25] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, and E. Jansen. The gator tech smart house: a programmable pervasive space. *Computer*, 38(3):50–60, 2005.

[26] Y. Isoda, S. Kurakake, and H. Nakano. Ubiquitous sensors based human behavior modeling and recognition using a spatio-temporal representation of user states. In *18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004.*, volume 1, pages 512–517 Vol.1, 2004.

[27] Z. Jiang, L. Lu, X. Huang, and C. Tan. Design of wearable home health care system with emotion recognition function. In *2011 International Conference on Electrical and Control Engineering*, pages 2995–2998, 2011.

[28] I. Joo and D. Choi. Distributed optimization framework for energy management of multiple smart homes with distributed energy resources. *IEEE Access*, 5:15551–15560, 2017.

[29] Javed Khan, Jun Wei, Markus Ringnér, Lao Saal, Marc Ladanyi, Frank Westermann, Frank Berthold, Manfred Schwab, Cristina Antonescu, Carsten Peterson, and Paul Meltzer. Khan j, wei js, ringner m, saal lh, ladanyi m, westermann f, berthold f, schwab m, antonescu cr, peterson c, meltzer psclassification and diagnostic prediction of cancers using gene expression profiling and artificial neural networks. nat med 7: 673-679. *Nature medicine*, 7:673–9, 07 2001.

[30] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys Tutorials*, 16(4):1933–1954, 2014.

[31] Prajakta Kulkarni and Yusuf Ozturk. mphasis: Mobile patient healthcare and sensor information system. *Journal of Network and Computer Applications*, 34(1):402–417, 2011.

[32] Hak Jong Lee, Sun Hee Lee, Kyoo-Seob Ha, Hak Chul Jang, Woo-Young Chung, Ju Young Kim, Yoon-Seok Chang, and Dong Hyun Yoo. Ubiquitous healthcare service using zigbee and mobile phone for elderly patients. *International Journal of Medical Informatics*, 78(3):193–198, 2009.

[33] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and wi-fi. In *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2007.

[34] Hui Li, Qingfan Zhang, and Peiyong Duan. Intelligent fuzzy agent for intelligent inhabited environments. In *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery*. IEEE, 2009.

[35] P.j.g Lisboa and Azzam Taktak. The use of artificial neural networks in decision support in cancer: A systematic review. *Neural networks : the official journal of the International Neural Network Society*, 19:408–15, 06 2006.

[36] Federico Lombardi, Leonardo Aniello, Stefano De Angelis, Andrea Margheri, and V. Sassone. A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids. 01 2018.

[37] R. Messing, C. Pal, and H. Kautz. Activity recognition using the velocity histories of tracked keypoints. In *2009 IEEE 12th International Conference on Computer Vision*, pages 104–111, 2009.

[38] G. Mingming, S. Liangshan, H. Xiaowei, and S. Qingwei. The system of wireless smart house based on gsm and zigbee. In *2010 International Conference on Intelligent Computation Technology and Automation*, volume 3, pages 1017–1020, 2010.

[39] Frank G. Miskelly. Assistive technology in elderly care. *Age and Ageing*, 30(6):455–458, 11 2001.

[40] M. Mozer. The neural network house: An environment that adapts to its inhabitants. 1998.

[41] N. Nguyen, Q. Tran, J. Leger, and T. Vuong. A real-time control using wireless sensor network for intelligent energy management system in buildings. In *2010 IEEE Workshop on Environmental Energy and Structural Monitoring Systems*, pages 87–92, 2010.

[42] Fco. Javier Ordóñez, José Antonio Iglesias, Paula de Toledo, Agapito Ledezma, and Araceli Sanchis. Online activity recognition using evolving classifiers. *Expert Systems with Applications*, 40(4):1248–1255, 2013.

[43] Jin-ho Park, Mikail Mohammed Salim, Jeong Hoon Jo, Jose Costa Sapalo Sicato, Shailendra Rathore, and Jong Hyuk Park. CIoT-net: a scalable cognitive IoT based smart city network architecture. *Human-centric Computing and Information Sciences*, 9(1), August 2019.

[44] Markus Prossegger and Abdelhamid Bouchachia. Multi-resident activity recognition using incremental decision trees. In Abdelhamid Bouchachia, editor, *Adaptive and Intelligent Systems*, pages 182–191, Cham, 2014. Springer International Publishing.

[45] Markus Prossegger and Abdelhamid Bouchachia. Multi-resident activity recognition using incremental decision trees. In Abdelhamid Bouchachia, editor, *Adaptive and Intelligent Systems*, pages 182–191, Cham, 2014. Springer International Publishing.

[46] H. Pung, T. Gu, and D. Zhang. Toward an osgi-based infrastructure for context-aware applications. *IEEE Pervasive Computing*, 3(04):66–74, oct 2004.

[47] Nishkam Ravi, Nikhil Dandekar, Preetham Mysore, and Michael Littman. Activity recognition from accelerometer data. volume 3, pages 1541–1546, 01 2005.

[48] D. Riboni, L. Pareschi, L. Radaelli, and C. Bettini. Is ontology-based activity recognition really effective? In *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 427–431, 2011.

[49] Fernando Rivera-Illingworth, Victor Callaghan, and Hani Hagras. A neural network agent based approach to activity detection in ami environments. pages 92–99, 07 2005.

[50] C. H. Salvador, M. P. Carrasco, M. A. G. de Mingo, A. M. Carrero, J. M. Montes, L. S. Martin, M. A. Cavero, I. F. Lozano, and J. L. Monteagudo. Airmed-cardio: a gsm and internet services-based system for out-of-hospital follow-up of cardiac patients. *IEEE Transactions on Information Technology in Biomedicine*, 9(1):73–85, 2005.

[51] Jordi Serra, David Pubill, Angelos Antonopoulos, and Christos Verikoukis. Smart hvac control in iot: Energy consumption minimization with user comfort constraints. *The Scientific World Journal*, 2014:161874, Jun 2014.

[52] F. Shabnam. Analysis of energy harvesting techniques for mobile networks. In *2019 IEEE Region 10 Symposium (TENSYMP)*, pages 784–788, 2019.

[53] F. Shabnam, T. U. Islam, S. Saha, and H. Ishraque. Iot based smart home automation and demand based optimum energy harvesting and management technique. In *2020 IEEE Region 10 Symposium (TENSYMP)*, pages 1800–1803, 2020.

[54] Tacklim Lee, Seonki Jeon, Dongjun Kang, Lee Won Park, and Sehyun Park. Design and implementation of intelligent hvac system based on iot and bigdata platform. In *2017 IEEE International Conference on Consumer Electronics (ICCE)*, pages 398–399, 2017.

[55] Tao Gu, Zhanqing Wu, Xianping Tao, H. K. Pung, and Jian Lu. epsicar: An emerging patterns based approach to sequential, interleaved and concurrent activity recognition. In *2009 IEEE International Conference on Pervasive Computing and Communications*, pages 1–9, 2009.

[56] Emmanuel Munguia Tapia, Stephen S. Intille, and Kent Larson. Activity recognition in the home using simple and ubiquitous sensors. In Alois Ferscha and Friedemann Mattern, editors, *Pervasive Computing*, pages 158–175, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[57] Spyridon Tompros, Nikolaos Mouratidis, Halid Hrasnica, and Michael Caragiozidis. A novel power line network architecture for managing the energy resources of the residential environment. In *2009 IEEE International Symposium on Power Line Communications and Its Applications*. IEEE, March 2009.

[58] National Institute of Standards and Technology U.S. Department of Commerce. *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 [Online] Available : http://www.nist.gov/public_affairs/releases/upload/smartgrid_interop y_final.pdf.*

[59] J. van Hoof, H.S.M. Kort, P.G.S. Rutten, and M.S.H. Duijnstee. Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users. *International Journal of Medical Informatics*, 80(5):310–331, May 2011.

[60] Tim van Kasteren, Gwenn Englebienne, and B. Krose. Transferring knowledge of activity recognition across sensor networks. pages 283–300, 01 2010.

[61] Federico Viani, Fabrizio Robol, Alessandro Polo, Paolo Rocca, Giacomo Oliveri, and Andrea Massa. Wireless architectures for heterogeneous sensing in smart home applications: Concepts and real implementation. *Proceedings of the IEEE*, 101(11):2381–2396, November 2013.

[62] J. Wang, J. Huang, W. Chen, J. Liu, and D. Xu. Design of iot-based energy efficiency management system for building ceramics production line. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, pages 912–917, 2016.

[63] Konlakorn Wongpatikaseree, Mitsuru Ikeda, Marut Buranarach, Thepchai Supnithi, Azman Osman, and Yasuo Tan. Activity recognition using context-aware infrastructure ontology in smart home domain. 11 2011.

[64] Konlakorn Wongpatikaseree, Mitsuru Ikeda, Marut Buranarach, Thepchai Supnithi, Azman Osman, and Yasuo Tan. Activity recognition using context-aware infrastructure ontology in smart home domain. 11 2011.

[65] Tatsuya Yamazaki. Beyond the smart home. In *Proceedings of the 2006 International Conference on Hybrid Information Technology - Volume 02*, ICHIT '06, pages 350–355, USA, 2006. IEEE Computer Society.

[66] Zhuang Zhao, Won Cheol Lee, Yoan Shin, and Kyung-Bin Song. An optimal power scheduling method applied in home energy management system based on demand response. *ETRI Journal*, 35(4):677–686, 2013.

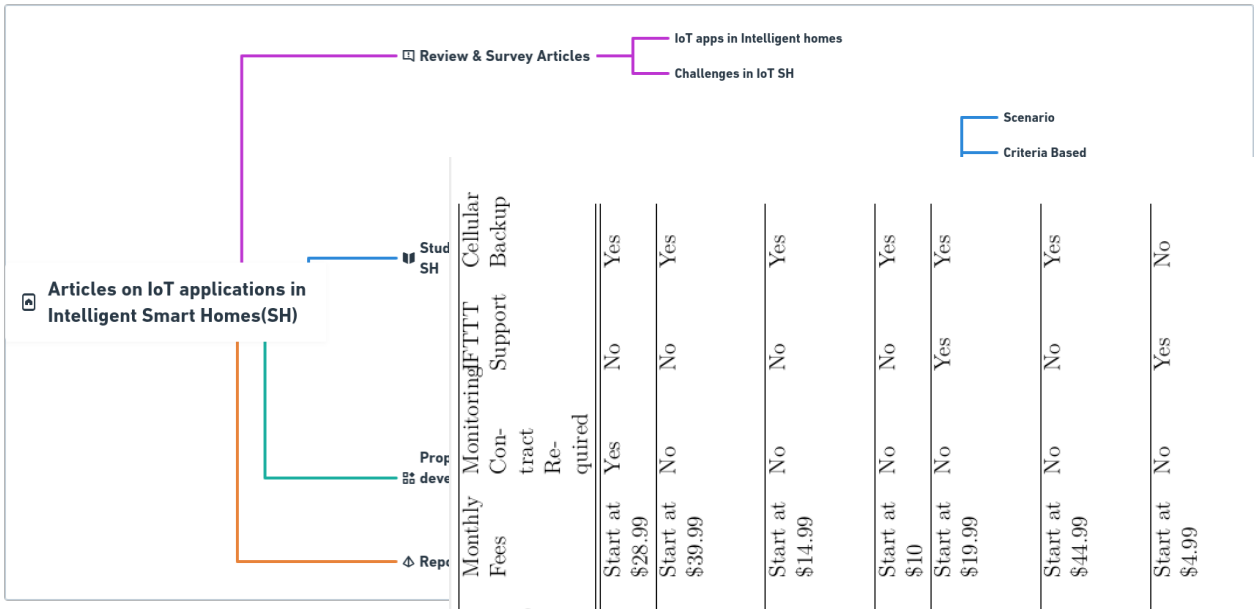

Figure 1. An overview of all the articles w
applications in Intelligent Smart Homes

Device Name	Z-Wave / Zig-Bee	Voice Assistant Compatibility	Upfront Costs	Professional Installation Required	Power Outage Backup	Monthly Fees	Monitoring Contract Required	IFTTT Support	Cellular Backup
ADT Pulse	Yes	Amazon Alexa	Start at $49	Yes	Yes	Start at $28.99	Yes	No	Yes
Vivint Smart Home	Yes	Amazon Alexa, Google Assistant	Start at $99	Yes	Yes	Start at $39.99	No	No	Yes
SimpliSafe Home Security System	No	Amazon Alexa	Start at $229	No	Yes	Start at $14.99	No	No	Yes
Ring Alarm Security Kit	Yes	Amazon Alexa	Start at $199	No	Yes	Start at $10	No	No	Yes
Blue by ADT Home Security System	Yes	Amazon Alexa, Google Assistant	Start at $149.99	No	Yes	Start at $19.99	No	Yes	Yes
FrontPoint Safe Home	Yes	Amazon Alexa, Google Assistant	Start at $99	No	Yes	Start at $44.99	No	No	Yes
Honeywell Smart Home Security Starter Kit	Yes	Amazon Alexa, Google Assistant	Start at $449	No	Yes	Start at $4.99	No	Yes	No
Wyze Sense Starter Kit	No	Amazon Alexa	Start at $19.99	No	No	None	No	Yes	No
Abode iota All-In-One Security Kit	Yes	Amazon Alexa, Google Assistant	Start at $299	No	Yes	Start at $8	No	Yes	Yes
Nest Secure	No	Google Assistant	$399 as tested	No	Yes	Start at $19	No	No	Yes

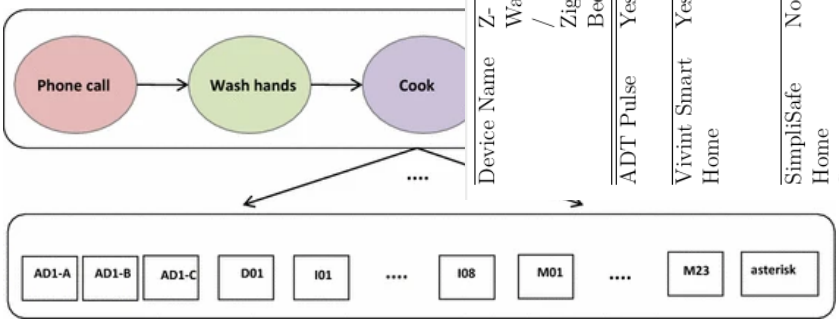

Figure 10. Activity modeling using HMM [7]

Reference	Sensors	Activiti
Yamazaki (2007)	Video cameras, microphones, floor pressure,motion, RFIDs	Watching TV, tracking perso
Patel et al. (2008)	Air pressure	Not menti
Rantz et al. (2008)	Video cameras, bed pressure, stove door CSS, motion	Cooking, sleepin in the ho
Viani et al. (2013)	Signal strength of wireless devices	Not menti
Wilson and Atkeson (2005)	Motion detectors, Pressure mats, CSSs, RFIDs	Eating, bathing, toileting, cookin TV
Baker et al. (2007)	Accelerometer, Blood pressure readings, microphones, heart rate, temperature	Movement, bloo changes, speec
Intille et al. (2005)	Infra-red cameras, microphones, pressure mats, motion, water and gas flow, light switches	Cooking, soci sleeping, cleanin workin
Noury and Hadidi (2012)	Motion	Not applic
Riedel et al. (2005)	Video cameras	Getting hom watching TV, ea watching TV,
Le et al. (2008)	Motion, CSSs	Bathing, dressing eating
Wood et al. (2008)	Heart rate, movements, ECG, pulse oximeter, weight, pulse monitoring	Toileting, sle showering, eat drinking, wa
Cook et al. (2013a)	Motion, CSSs	Bathing, walkin eating, relaxing, hygiene, sleepin medicin
van Kasteren et al. (2008)	Motion, CSSs	Toileting, shower and drinking,

Table 2: Sensors used by various studies [7]

Figure 15. Sensors used by various studies [7]

References	Algorithm	Target	Resu
Mozer (1998) [40]	ANN (MLP)	ADL (general)	–
Cook et al. (2013b) [16]	ANN (MLP)	ADL (general)	Acti
Rivera-Illingworth et al. (2005)	ANN (EcoS)	ADL(healthcare)	Anor % Ac 89.14
Li et al. (2008) [34]	ANN (OPNN)	ADL (healthcare)	Acti
Lotfi et al. (2012)	ANN (ESN)	ADL (healthcare)	Abn 93–9
Isoda et al. (2004) [26]	DT (C4.5)	ADL (general)	Acti 90–1
Ravi et al. (2005) [47]	DT (C4.5)	ADL (general)	Acti 57–9
Manley and Deogun (2007)	DT (ID3)	Resident's location	Mea 4.9m data
Hagras et al. (2004) [22]	ISL (fuzzy)	ADL (general)	280
Hagras et al. (2007) [49]	Fuzzy type-2	ADL (general)	RMS
Bouchachia (2011) [11]	GFMMNN (fuzzy?ANN)	ADL (general)	Curr 0.01
Andreu and Angelov (2013)	Evolving fuzzy classifiers	ADL (general)	F-me
Bouchachia and Vanaret (2014) [12]	GT2FC (fuzzy)	ADL (general)	81.65 label
Chua et al. (2009)	HMM	ADL (healthcare)	90.75 recog % ob recog
van Kasteren et al. (2010) [60]	HSMM	ADL (general)	F-me
Gu et al. (2009)	EPs	ADL (general)	85.84 by ti
Riboni et al. (2011)	Ontological approach	ADL (general)	80.3

Table 3: Algorithms used by various studies [7]

Figure 16. Algorithms used by various studies [7]

Scenario :	Possible Threads	Security Goals Compromised
SH1	Eavesdropping (N) Traffic Analysis (N) Message Modification (N) Replay Attack (N) EMS Impersonation (SH)	Confidentiality Integrity Authenticity
SH2	Repudiation (N) Message Modification(N) Replay Attack (N)	Non repudiation Integrity Authentication
SH3	Tampering/Reversal/ Removal of Meter (SH) Illegal Software Modification/Update(SH)	Authentication Integrity
SH4	Customer Impersonation (N) Device Impersonation (SH) Message Modification(N) Replay attack(N) Repudiation(N)	Integrity Non repudiation Authentication
SH5	Customer Impersonation(N) Eavesdropping/Message(N) Interception (N) Message Modification(N)	Confidentiality Integrity Authenticity

Table 4: Smart Home Security Issues [30]

Figure 17. Smart Home Security Issues [30]