University of Oslo
Master Thesis (draft v0.9)

Integrating Energy Devices through BasicInternet

Syead Nusrat Nur
(Student nr. 590304)
syeadnn@ifi.uio.no

October 2, 2018

Abstract

Integration of Internet of Things (IoT) devices into the home is currently quite cumbersome. This thesis presents a novel approach on integrating devices, e.g. washing machines, heat pumps and other devices. The starting point is an open but limited Wi-Fi Network, called the Information Internet or InfoInternet[1]. The approach lets the device find an/the open Wi-Fi Network, connects to the network, announces itself to the Internet, and gives the owner the opportunity to take control of the device. The thesis will bring the concept into a prototypical solution and evaluates aspects like security and transfer-of-ownership.

Keywords: IoT, Smart Home, Wi-Fi, IoT Security, Information Internet

[1] e. g. BasicInternet, http://basicinternet.org/

Contents

List of Figures

1 Introduction

In recent years the world has been going through a paradigm shift in terms of the communication system. So far we had the Internet of Servers, Personal Computers and Portable Digital Devices (PDAs) etc. But now the Internet has been extending its footprint on to almost every aspect of our life, on to every "thing" or device of the world surrounding us. These things are getting more and more intelligent, communicating with each other on the Internet making the world around us surprisingly autonomous without requiring any human intervention. Every home is getting smarter, every system is getting automated with emerging technologies and every grass-root sensor network is automatically communicating, controlling itself and getting controlled over the Internet within a brand new framework - the framework of the Internet of Things (IoT).

Some of the IoT devices generally used at homes are the energy devices, devices that consumes energy, for example, washing machines, heat pumps, dish washers etc. Nowadays, these 'things' are getting smarter and smarter. They have been being equipped with new technologies, for example, wireless radios supporting IEEE 802.11 (Wi-Fi), IEEE 802.15.4 (ZigBee, 6LoWPAN), Bluetooth Low Energy (BLE) etc. to connect themselves to the home network and the Internet etc[1]. So now after buying an energy device, the owner can configure it manually to integrate it to the home network or smart home automation systems. However, this integration process is still quite cumbersome requiring a lot of manual intervention.

Another big concern that comes with anything connected wireless or online is the security. Hence, IoT devices being wireless and connected to the Internet are also subject to the threats from the open waters of the ocean of hackers and eavesdroppers[2]. As a result, when designing a new wireless solution, the designers must pay special attention to the security aspects of the solution.

This thesis will present a new way as to how this integration process can be automatized ensuring security so that the device itself can do the integration to the Internet at the first time power on and give the owner the opportunity to claim its ownership, integrate it in their home automation systems, personalize it and control it in a secured way.

1.1 Motivation

****Why this topic is important**
Home automation is something that has invaded our lives quite heavily in recent years. This is what makes our homes so-called "Smart Homes" easing people's lives. Home automation systems do a lot of things in the household autonomously which we have been doing manually. For example, it will control the brightness of the lights in the house automatically based on the need in bedrooms or living rooms or with voice commands from the users. The climate of the house will be controlled automatically based on the need of cold air, hot air or humidity. Household appliances are also joining the rally for automatic running and control e.g. washing machines, dishwashers, refrigerators etc.

The extraordinary level of home automation is due the fact that modern society has been witnessing a revolution in the technologies. Homes are now connected to the Internet all the time rendering the houses as "connected homes" as depicted in figure 1 by Home Appliances World [3]. The revolution in wireless communication technologies is pushing the idea forward ever faster. However, if we skim through the history, we see that home automation has always been under constant improvement. Early systems were mostly meant for saving labor - e.g. washing machines, dishwashers etc. Later, we saw new technologies bringing new ideas making people's lives easier still. Examples include refrigerators, radios, televisions etc.

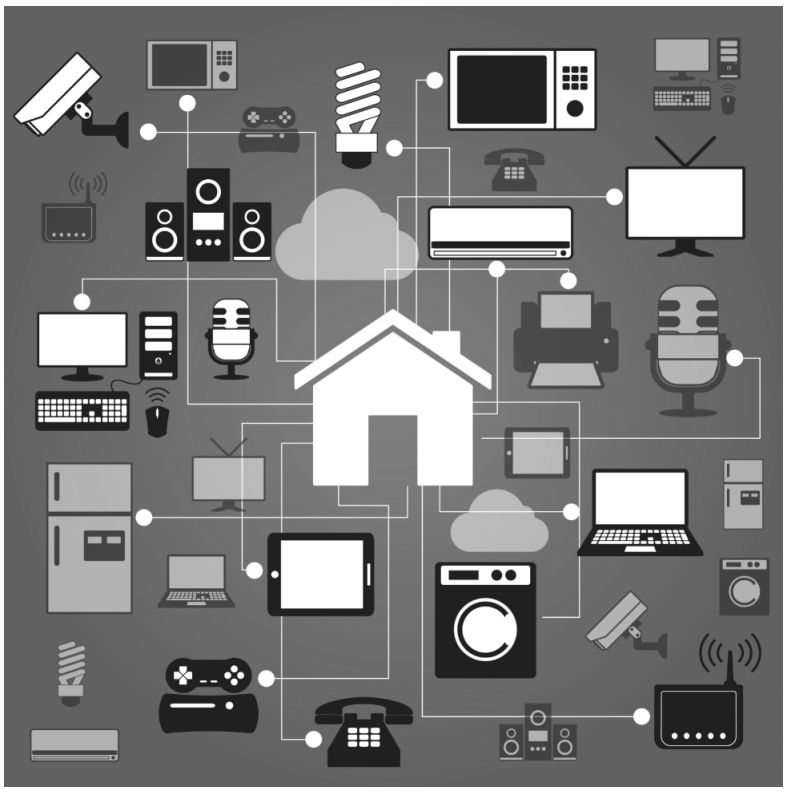

Figure 1: Schematic diagram of a modern Smart Home or Connected Home by Home Appliances World [3]

Now these household appliances that made our homes easy to live have been going through further improvement in recent years. Now these appliances are getting smarter and can control themselves through communication with other systems. can interact with other devices in order to work autonomously. For example, they can turn themselves on or off or control themselves to run a service based on some triggers communicated from the Internet or other systems. Hence the communication between the appliances are the key to the recent development. This is what has been making our homes "Smart Homes".

However, there are many challenges which still require solutions for the smarter

operation of these smart devices. One of the challenges that still exists for a smart washing machine, for example, is that after buying the machine, the owner/user of the machine has to integrate the machine with a lot of manual work. This is a cumbersome process and requires a lot of time to configure it whereas this integration process should be automatic without requiring manual intervention. This thesis will propose a solution for this.

Another big concern for these smart devices which are connected to the Internet is the security. The users of these machines want to be sure that no attacker or hacker is able to hack into the washing machines or the home automation systems. Recently there has been reports of security holes in connected smart light bulbs that can be used by the hackers to hack the passwords of the household Wi-FI network[4]. It reiterates that proper security is a prerequisite of the IoT framework. This thesis also analyses the security aspects of the proposed approach as ensures that only the authorized person (buyer/user) is able to access the machine and use it.

This section introduced the high-level motivation of the project. Next section will stated the problem statement, the following sention will define the engineering methods which will be employed for the thesis.

1.2 Problem Statement

For the analysis of the home appliance integration process in the thesis, we choose the washing machine as the home appliance.

The washing machines are currently of 2 types - legacy and smart. The legacy washing machines are operated manually. They don't have any automation and networking capability. The user powers up the machine manually, loads the clothes to wash and presses the button manually for the machine to start washing. On the other hand, smart washing machines came out recently and they have some level of automation and networking capability in them such as Wi-Fi and NFC.

The smart washing machines available now-a-days do not work in an autonomous way when it comes to integrating them in the Smart Homes. Still the users need to do a lot of manual work in order to integrate them. In many cases it's not even possible because in those cases the washing machines do not support Wi-Fi, for example, and only supports NFC, for example.

However, if we have a smart washing machine and we connect them to a wireless network and to the Internet, they are required to be kept secured from the untrusted access.

The goal of the current thesis would be to design a user-friendly and convenient process to integrate the smart washing machines to the Smart Homes while ensuring that this is cost effective and scalable. The solution will also ensure that the highest level of security is in place.

This section outlined a high level overview of the goal of the thesis. It will be detailed out in section 2.

1.3 Method of Engineering Design

A design process is a systematic and often iterative strategy of solving a problem with certain constraints and criteria. The result would be to develop multiple solutions based on study and analysis of the problem and narrow down to the possible solution to satisfy human needs and wants. In engineering end of the vast spectrum of design processes lies the Engineering Design Process (EDP) where engineers use mathematical and scientific tools in the process. On the artistic end of the spectrum, graphic designers may use some other methods to choose colors, contrasts etc to achieve the desired appeal of the product.

We concentrate on the method of Engineering Design Process (EDP) to work with the problem at hand. In the literature the engineering design method is described more or less the same or similar way by engineering community. But in order to follow it, the five-step process suggested by the Museum of Science, Boston, Massachusetts will form the basis of the process as described in the book by Karsnitz et al.[6]. Figure 2 in page 7 presents an overview of the whole EDP as described in the book.

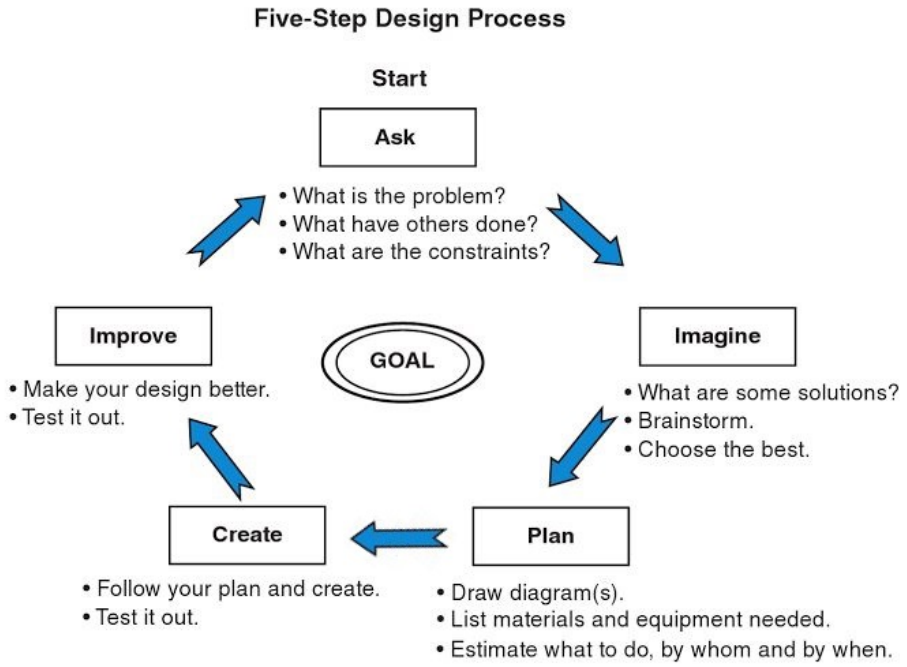

Figure 2: Engineering Design Process developed by Museum of Science, Boston (ref. Karsnitz et al.)

The process entails the following steps going in cylces: **ask**, **imagine**, **plan**, **create**, **improve**. We first set up a **goal** that we would like to achieve. Then

ask questions: what is the problem? What has others done? What are the constraints? Then in the **imagine** step, we brainstorm on the problem and develop some solutions and we choose the best one. At this point, we move on to the **plan** phase, create a detailed plan as to how to implement the solution. We divide the problem into multiple parts, draw schematic diagrams to help plan the parts out. As list of materials and equipment needed for this and also the resource requirements are put in place. Then we follow the plan and implement the solution in the **create** step. Finally, we evaluate the outcome with the **goal** and test it to find if there it satisfies our targets in the **improve** phase. If we see that we can improve the solution, move to the first step again and ask the questions again and the whole process repeats in an iterative fashion.

1.4 Outline of the Thesis

Since we are following this method of EDP in this thesis, the later organization of this paper are as follows. In section 1.2, the **goal** of the thesis is outlined. The **imagine** step is covered in chapters 2 and 3 examining different options for the solution to narrow down to the best one. In chapter 4, the **plan** for the solution is presented and in chapter 5, the **create** part is covered. Finally in chapter 6 the whole solution is evaluated to cover the **improve** step with a security analysis of the solution.

In the next chapter, I will go through the proposed scenario for a secure IoT setup of the integration of a smart washing machine to the smart home.

2 Secure Device Setup Scenario

Today's smart homes are equipped with myriads of IoT devices which can interact with one another through a local network or the Internet. In this paper, we are proposing a secure, convenient, cost efficient and scalable way for the smart washing machines to be integrated in the smart homes with minimum interaction from the owner. In this chapter, a high level scenario will be proposed/discussed. In addition, the requirements of the solution will be elaborated and technological challenges will be introduced.

2.1 High Level Scenario

A typical scenario for the solution is the case where the smart washing machine comes with ~~Wi-Fi/~~ wireless radio capability. Hence it can be connected to ~~the home Wi-Fi network/~~ an Internet Access Point (AP). A high level scenario for integrating a smart washing machine is proposed to be implemented as shown in figure 3.

There are two premises of concern in this scenario as figure 3 illustrates - buyer premises and seller/vendor premises. The buyer premises consists of the smart washing machine which the user buys from the seller and a ~~Wi-Fi Access Point (Wi-Fi AP)/~~Internet AP. On the other hand, in the seller/vendor premises, we have the seller's Authentication Server (AS). These two premises will be

connected through the Internet with the help of the ~~Wi-Fi AP/~~Internet AP available at the buyer's premises.

The high level steps to integrate the smart washing machine to the smart homes would thus be as follows.

1. When the user buys the smart washing machine, the vendor/supplier will provide him a user authentication token as a proof of the ownership of the device. Later the user/buyer has to use this token on the vendor's web portal to claim the machine which he is buying now.

2. The user then gets the machine transported to his home where it is supposed to be integrated.

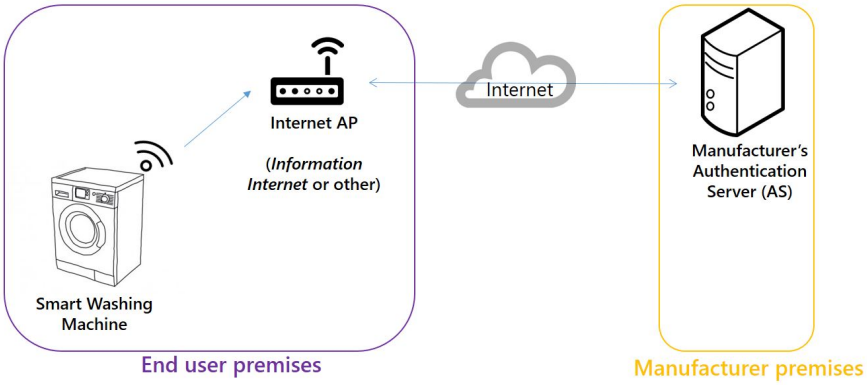

Figure 3: High level scenario for integrating a smart washing machine with the help of an Internet AP ~~with secure device setup~~

3. Now the user connects the machine to the power and turns it on. The device then starts its ~~Wi-Fi~~ wireless radio and tries to find an open but limited ~~Wi-Fi~~ wireless network with connection to the Internet, the so-called 'Information Internet' e.g. BasicInternet, if available. If no such ~~Wi-Fi~~ wireless network is available, then the washing machine can be configured manually to connect to an available secure ~~Wi-Fi~~ wireless network with Internet access.

4. After connecting to the ~~Wi-Fi~~ wireless network, the device declares its presence and availability in the ~~local area network/~~ network. ~~Using the vendor's portal or the smartphone app~~ the device reaches the vendors portal and authenticates itself with the seller's/vendor's Authentication Server using the authentication token of the user which the user had received during the purchase of the washing machine. Hence the owner claims the ownership of the machine in the portal and takes its full control.

5. Next the owner configures the machine as he wants, administers it online and controls the machine using his smartphone/portal.

These five high level steps introduce the process which will be elaborated with detailed description of the proposed protocols in each step. We will present the reasons why we would choose the protocols that we choose analyzing the relevant works by the scientific community and the industry in chapter 3. In the next section we will put forth the requirements or target of the solution. Other solution scenarios will be discussed also.

2.2 Requirements

This thesis proposes a smart integration process of the smart washing machines. For this we have targeted some requirements to be met in the solution. These requirements are presented in this section. Later in chapter 6, these requirements will be evaluated against the final solution.

2.2.1 Convenience

The word 'convenience' means 'the quality of being useful, easy, or suitable for someone' [7]. Current integration process of the smart washing machines can be improved to make the process easier for the users eliminating complicated steps making the system more useful. The proposed integration process is required to be easy enough so that the user can avoid cumbersome manual work to integrate the machine in his smart home. The process needs to be automated and hazard-free so that anyone can use the process with ease.

2.2.2 Cost Efficiency

'Cost efficiency' means 'a way of saving money, or of spending less money' [8]. Due to the inclusion of a lot new technologies, both hardware and software, modern systems tend to be more and more costlier. However, one of the targets of the proposed integration process will be that it will be cost efficient. It will introduce the solution with features that will be effective, but at the same time will limit the cost. The existing features of the smart washing machine will also be reused efficiently.

2.2.3 Security

Since most of the smart devices use wireless networks and the Internet, ensuring security is very critical. The proposed solution will ensure that the device and all the communications that is done among the vendor's server, the device and the user's smartphone are secure from all forms of security threats and attacks.

2.2.4 Scalability

Scalability is the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged to accommodate that growth [9]. The requirement of the proposed solution is to be scalabale. The solution works irrespective of however many users are needed. The solution will not be limited only for few users. The functionalities does not cease to work if the user load increases.

Another aspect of the system that demands scalability is the method used for authentication - both smartphone-based and portal-based approach are required to be scalable. The flexibility of the use of wireless technologies - Wi-Fi, Mobile Network, ZigBee etc is currently out of scope. The solution will be based on Wi-Fi only.

2.3 Technological Challenges

[WIP]
*Information about Wireless network, Device connectivity, Announcement etc.

Advancement in wireless technologies brings about a lot of ease in human life. Last couple of decades have witnessed a tremendous growth in wireless technologies. Now people can use phone on the go connected to the Internet all the time through 3G (UMTS, HSDPA, HSPA+) and 4G (LTE, WiMAX) telecommunications technologies. Wi-Fi is ubiquitous in home and office environments giving people unprecedented flexibility and ease for day-to-day work.

Following that line, device-to-device communication and "Internet of Things" are the growing focus of the research and development communities. Home automation and energy management is also a part of it. This is where our thesis comes into picture. Some of the technological challenges that we have to tackle are listed below.

3 Technology Background

[WIP]
This thesis provides a new way of integrating a smart washing machine to the home energy system hardly requiring any interaction from the user during this process. The thesis provides a framework describing how this can be achieved.

***Paragraph: technology, the following areas are addressed: 1 bullet per area - what is done in each of the areas (high level view) - what you are doing "why"*

***In each of the technology areas, have at least 3-4 scientific articles (references) - dominant protocols, challenges, ..*
- (aspect is not so important for my thesis, so I just refer to literature for further analysis)
- red line: focus on this, that .... (main issues, addressed here; minor issues, left aside, transferred to further work)

3.1 Networking Capabilities of Smart Devices

In order to work in a Smart Home system and to the Internet, the smart devices need to connect to have the capability of networking. The field of IoT connectivity has been expanding very quickly and there are already a lot of options as the the scientific community has been standardizing many wireless technologies.

Mainetti et al. pointed out that the network connectivity for IoT devices can be of IP-based or non-IP-based[10]. They could be wired or wireless. In our case, it's not practical to employ the wired solution since the washing machines generally are located in the bathroom or kitchen far away from the home Ethernet ports and home router kits. Hence, we will now discuss about the options available for wireless access technologies for the washing machine to connect to the network and the Internet.

3.1.1 Review of Wireless Access Technologies for IoT

Akpakwu et al. surveyed the existing wireless technologies for IoT. They classified the technologies in 3 types - long-range, short-range and cellular[11]. ***Table 1 in page 12 summarizes most of the relevant wireless technologies. Additionally it also lists the frequency bands they use and categorizes them on the basis of whether their availability as open standards.

The long-range wireless technologies include LoRa, Sigfox, Ingenu-RPMA, DASH7, Weightless etc. They are also called Long Range Wide Area Network (LPWAN) technologies. Many of these technologies are proprietary and not openly available. These wireless technologies overwhelmingly uses the ISM bands.

Examples of short-range are Bluetooth, Bluetooth Low Energy (BLE), Thread, ZigBee, Wi-Fi etc. Most of these 2 types of technoglogies use freely available ISM frequency bands for wireless communicaton. These technologies are based on various works of IEEE 802.15 working group. BLE, Thread, ZigBee etc. are suitable for low power, small, battery-run peripheral devices whereas Bluetooth and Wi-Fi are more for the high-end devices which do have such power limitations.

Type	**Wireless Technology**	**Frequency Band**	**Source**
Long range	LoRa, Sigfox	ISM	Proprietary
Long range	Ingenu-RPMA	ISM	Proprietary
Long range	DASH7, Weightless	ISM	Open
Short range	Bluetooth, BLE	ISM	Open
Short range	ZigBee	ISM	Open
Short range	Z-Wave, Thread	ISM	Proprietary
Short range	Wi-Fi	ISM	Open
Cellular	GSM, WCDMA, LTE	Licensed	Open
Cellular	EC-GSM-IoT, LTE-M, NB-IoT	Licensed	Open

Table 1: Various wireless access network technologies for IoT.

The cellular wireless technologies include the widely available GSM, UMTS or LTE networks mostly used for mobile telecommunications. They also include newly specified LPWAN versions of these technologies designed especially for low power IoT devices: EC-GSM-IoT based on GSM, LTE-M and NB-IoT based on

LTE which are optimized for low power requirement[11]. GSM, UMTS or LTE would draw much more battery power than their IoT counterparts and hence would make them non-ideal for many of the IoT devices running on batteries. The good thing about these technologies are that they are widely available in all kinds of terrains and run on licensed spectrum which means they can ensure better quality of service than their ISM band counterparts.

3.1.2 Feasibility Study of Wireless Technologies

Table 2 in page 14 rates the wireless technologies on different aspects of the technologies analyzing their feasibility for the solution of the current problem. The ratings are given in 3 categories - **Not so good (-1), Reasonable (0) and Good (+1)**. Finally all the ratings of a wireless technology are summed to provide the overall raring.

Before we move into the feasibility study, let's see how many cases could there be when it comes to the wireless networking for the current problem.

A. Washing machine is located at the same house as the owner/user

B. Washing machine is located at a different place than the house of the owner/user

In the first case (case A), the washing machine is located inside the house where the owner lives. In this case, it is highly likely that a home Wi-Fi AP is available managed by the owner - either open or protected. In this case, the we would prefer Wi-Fi over all the other available wireless technologies. One of the reasons would be that Wi-Fi is ubiquitous and widely available in almost every household, even we could find many open/guest Wi-Fi networks which is one of the original requirements of this thesis. Moreover, Washing machines are always connected to power and hence the power they need for running Wi-Fi radios is abundant and not a problem.

The challenge with some of the other short range low power wireless technologies based on IEE 802.15.4, for example, ZigBee, Z-Wave, Thread etc. is that the peripheral IoT devices connected using these technologies need a hub which in turn must be connected to the Internet directly or via Wi-Fi, cellular or other long range technologies. This is what *Zachariah* et al. termed as "the gateway problem" of IoT[12]. The good thing about Wi-Fi, in this respect, is that it makes an IP-based local area netowrk (LAN) and hence the smart washing machine would avoid "the gateway problem" to convert the data between Wi-Fi and other protocols. The phones and portal laptops would easily reach the washing machine both while in the house and outside.

Now, for the second case (case B), the washing machine is actually located far from the house the owner lives in. In this case, we can have several sub-cases:

i. washing machines of all the apartments of an apartment building or housing society are housed in a common laundry room.

ii. the housing society has a common washing machine service housed in a common laundry room serving all the apartments and the apartment owners are required to book their time before they can use those common washing machines

iii. the owner of the washing machine actually lives in a house little far away from where the washing machine is kept

In all these sub-cases of case B, the washing machine is not served by the Wi-Fi network of the owner's house and hence Wi-Fi would not be the best option for connecting the smart washing machines to the Internet. Long range Low Power Wide Area Network (LPWAN) technologies like LoRa, Sigfox etc. are suitable for these scenarios. However, they are not widely available yet and the technologies are proprietary. Moreover, there are many competing technologies and there is no clear winner yet.

Wireless Technology	**Range**	**Availability**	**Power Consumption**	**Cost**	**Gateway Problem**	**Overall Rating**
LoRa, Sigfox	0	0	-1	0	+1	0
Ingenu-RPMA	0	-1	-1	0	+1	-1
DASH7, Weightless	0	-1	-1	0	+1	-1
Bluetooth	-1	+1	0	0	-1	-1
BLE	-1	+1	-1	+1	-1	-1
ZigBee	-1	0	-1	+1	-1	-2
Z-Wave, Thread	-1	0	-1	+1	-1	-2
Wi-Fi	**-1**	**+1**	**+1**	**0**	**+1**	**+2**
GSM, WCDMA, LTE	**+1**	**+1**	**0**	**-1**	**+1**	**+2**
EC-GSM-IoT, LTE-M, NB-IoT	+1	0	-1	0	+1	+1

Table 2: Evaluation of different networking technologies for the smart washing machine

However, the cellular technologies in these cases would be much more suitable. This is because of several things - firstly, these networks are widely available almost everywhere with high quality of service simply because they run on licensed frequency bands. Secondly, they don't have a "gateway problem" since they are based on IP and directly connects the devices to the Internet. Thirdly, they are highly secured with several layers of security both in the air interface and the backhaul network from the base stations to the Core Network. In addition, the LPWAN versions of the cellular networks are also reasonable to use. However, since these new technologies are not yet widely deployed by the Cellular Network Providers, their usage is currently limited.

One apparent drawback of the cellular technologies is that the UICC/SIM cards need to be inserted into the smart devices for them to be able to connect to the cellular network. This feature is currently not available in any of the smart washing machines. However, washing machine vendors can easily provision an **Embedded UICC** or Embedded SIM card **(eSIM)** in the internal circuitry of the washing machine which is the state-of-the-art solution for cellular IoT, standardized by GSMA[16]. One of the many benefits of eSIM is that multiple SIMs from multiple Cellular Network Operators can be downloaded in or pushed to in the same eSIM at the same time using the 'Remote Provisioning Architecture' of the operators enabling the user to change the operator easily as and when he wishes[17]. However, in order to avoid complex wireless technolgies for downloading the eSIM, it is recommended that the washing machines ship with pre-installed eSIM cards of some telecommunications operator.

The table 2 summarizes the rating on different aspects and the overall rating shows that Wi-Fi and Cellular are tied with overall rating +2 each.

However, since case A prefers Wi-Fi whereas case B prefers cellular, this creates a problem both for the manufacturers and the users when it comes to cost. The manufacturers would not be very enthusiastic about equipping the same smart washing machines with two different wireless technologies at the same time as it would increase the cost of the device. In the same way, the users would not be willing to pay extra monthly subscription fees to the telecoms operators for the cellular network usage in contrast to the fact that Wi-Fi makes a better solution for them available for free or almost free. Hence, we suggest that Wi-Fi is used as the sole solution of the wireless network technology for the problem.

3.2 Availability of Open Internet

The solution of integrating the smart washing machines in smart homes would require the Internet to ease process of integration and easier control. The preferable solution is that the washing machine connects to an open Internet Access Point (AP) like Information Internet.

Information Internet is a new concept conceived by the *BasicInternet Foundation*[5]. The Foundation was established in December 2014 in Norway as a collaboration between The University Graduate Centre (UNIK) and Kjeller Innovasjon AS. The idea is to provide everyone everywhere in the world free Internet access consisting of information only i.e. data and pictures. This is a free-of-cost service but limited in the sense that any services other than basic data and pictures are at premium.

The motivation of this idea was that people have the right for basic information, but people from most of the under-developed countries in the world cannot afford this financially. But basic informational Internet service is basically very cheap compared to premium services like audio, video etc. An example provided by the foundation says that an ISP in Africa can either provide a user 10 months of information or 7 minutes of video: the cost are the same[5]. The foundation's target is to encourage the governments and the ISPs to launch what they called **"BasicInternet"** services free for everyone (using very cheap

boxes as wireless access points) and make the premium services available only for a paid subscription. This would give them a very good business case while the people get benefited.

The Information Internet could be provided through any reasonable and viable access technology. However, according to *BasicInternet Foundation* reports, it is easier and cheaper with Wi-Fi Access Points placed in different locations of the city or town. Another way could be that the mobile telecommunications operators use their ubiquitous mobile networks to allow a limited access to the Information Internet users[5]. In our solution, since we choose Wi-Fi as the access technology, we assume that an open Wi-Fi access point with free Information Internet is available inside the owner's house. However, in case no Information Internet is available, there should be a mechanism in the solution so that the washing machines can connect to the Internet using the open or protected Wi-Fi access points available at the owner's house. This implies that the washing machine has to have the provision to connect to any Open Wi-Fi AP or protected by a password. In the next sections we will discuss how this could be done and propose a solution for our problem.

3.3 Automatic Connection to the Open Wi-Fi

[WIP]
Smart devices like smart washing machines typically does not have place for a keyboard input mainly because the control digital display of the washing machine is normally not so large that manufacturers can install a digital keyboard application in the washing machine. Hence, it is not possible to connect to the Wi-Fi directly from the washing machine since there is no way to input the letters for the Wi-Fi password. The WPS solution is not preferable because it is not recommended due to its severe vulnerability when it comes to security.

However, smart washing machine vendors uses many different ways to conncect to the Wi-Fi. One of the state-of-the-art solutions for connecting the devices to the Wi-Fi is to generate a temporary Wi-Fi Access Point in the washing machine itself and use a smartphone app to connect washing machine to the Home Wi-Fi using the temporary Wi-Fi. Many smart home vendors use this technique to connect to the smart devices to the Wi-Fi, for example, TP-Link Smart lights, Smart Plugs etc., Smamsung EcoBubble, Samsung Crystal Blue smart washing machines, LG Smart ThinQ washing machines etc. However, this technique has some security holes that have recently been surfaced and hence we would not use this mechanism.

It would be better if Washing machines could have a functionality to connect to the open Wi-Fi automatically. This would be very difficult to implement because an external crowd-sourced database in the Internet is required for the washing machine to communicate as the US Patent for the WeFi app case tells us[15].

We propose that the washing machines have the digital keyboard so that the password can be typed into the washing machine and this is how the washing

machine connects to the Wi-Fi Access Point. However, in this case the washing machine needs to be claimed by the legitimate owner who are using the same Wi-Fi network or another. For that to work the washing machine needs to announce itself in the network.

3.4 Registration and Announcement of the Device

After the washing machine connects to the Internet AP (Wi-Fi AP), the machine is should be available for the owner so that he can claim the ownership of the machine. To implement this, we the washing machine needs to announce itself in the network so that anyone having the correct device can actually claim the machine.

One way of doing this is that the device announces itself in the Wi-Fi Local Area Network.
*Announcement does not happen in the Internet. Instead the user finds the Washing Machine service in the Energy Device App as a Smartphone App from the Vendor/seller or Energy Device Web Portal.

*Announcement in the Internet (analysed protocols: Jini, Bonjour, UPnP, N-UPnP, Multicast DNS-based Service Discovery (mDNS-SD)

*mDNS-SD is chosen which Bonjour is based on due to its simplicity and security.

3.5 User and Device Authentication

[WIP]
The vendor has the job of identifying a device that he sells with a buyer that owns the device. Various approaches could be applied here such as token-based, username password pair, SMS based etc. Each one has its own challenges.

***Authentication and Ownership*

This is one of the most critical part of the solution. In order to establish a secure connection between the machine and the vendor's authentication server that administers and controls the machine over the Internet via a web portal, the vendor has to provide a mechanism to authenticate the device to its authentication server.

When the user buys the washing machine, he gets a token from the vendor as a proof of ownership of the machine. This token could be a *username-password pair*. It will be used as a User Authentication mechanism to authenticate the rightful owner of the machine so that only the rightful owner of the machine can access the machine online. The owner uses this to log in to the vendor's portal to claim the ownership of the machine in the portal.

***User and Device Authentication - from ch2 to be merged*

[WIP]
As we mentioned earlier, one of the most critical part of the technological challenges that the vendor needs to provide is to provision an authentication process for the devices - that are sold - to the vendor's authentication server when they come on-line using the Internet.
*SMS with the link to the app download or web portal to access the device. Phone number of the buyer is used as the username.

*Code/password from the seller

*AAA protocals - RADIUS or DIAMETER with EAP will be examined.

3.6 Device Management

[WIP]
Once the owner has claimed the machine online, he can now administer and control the machine in several ways -

- Using the online portal
- Downloading an mobile phone application provided by the vendor
- Integrating the machine in their home energy management system that the device is compatible with.

4 Basis for Implementation

[WIP]
After all the discussions and analysis of the technologies from the state-of-the-art, we can visualize how the solution would look like. Figure 4 provides a step-by-step procedure for the solution.

The procedure, still high level, starts when the user buys the Smart Washing Machine from the shop. During purchase he receives a **security token** from the manufacturer with the machine. After transporting the machine home, the user powers it on and the washing machine turns the Wi-Fi radio ON automatically and connects to finds any available Wi-Fi based Information Internet if avialable. If there is none, it finds all the Wi-Fi networks available. After the user provide the Wi-Fi password, the Washing Machine connects to the Internet and establishes a secure TCP connection with the Manufacturer's server, registers there and announces itself to the server.

Now the user uses his smartphone app or manufacturer portal in the home Wi-Fi network to discover the Washing Machine's IP address. He then creates an account in the manufacturer's portal/app and claims the washing machine in the portal/app associating it to his account. He is only allowed to do that if he presses the Security Button located in the Washing Mahine for at least 30 seconds. He also needs to secuity token received when he purchased the machine. Now that the user has taken control of the washing machine, he can now use it at his will using the app or the browser - locally or remotely.

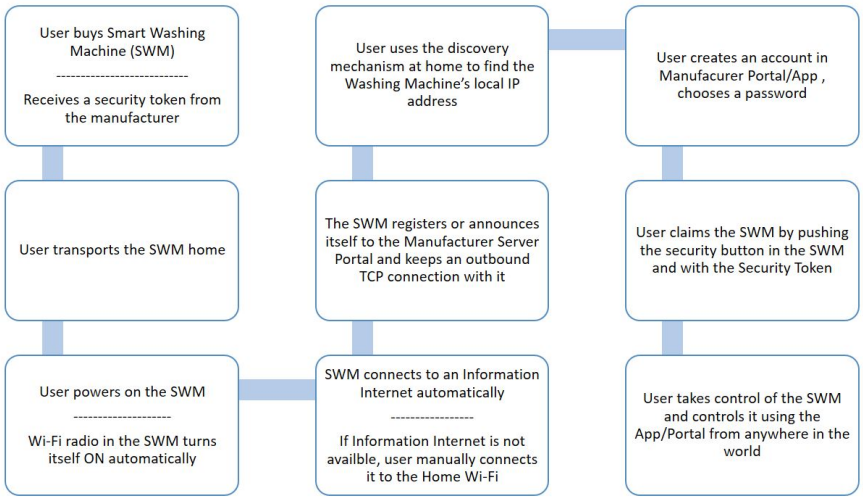

Figure 4: Step-by-step procedure for the solution so far

In the following sections we delve into detail of the different aspects of the solution for implementation.

4.1 Functional Architecture

[WIP]

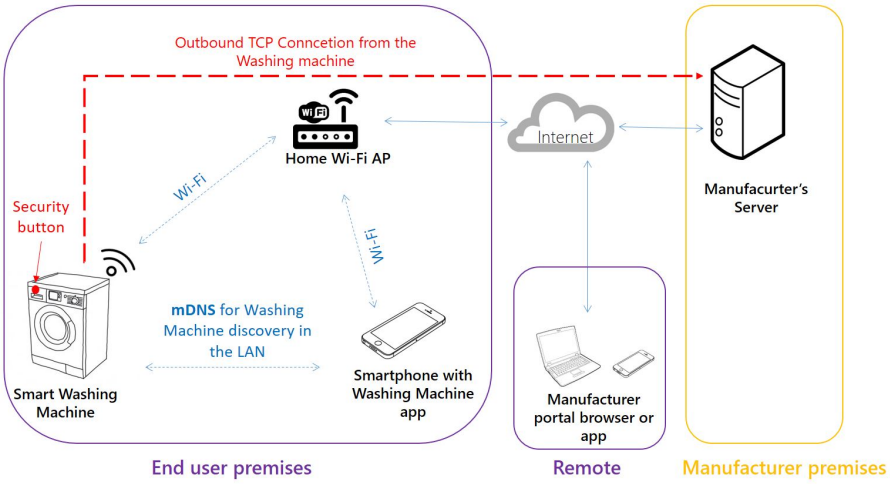

Figure 5: Schematic diagram of the overall process

Functially the solution comprises of the following elements. The schematic diagram in figure 5 summarizes the components and different functional interfaces

of the solution.

i. Wi-Fi enabled Smart Washing Machine

ii. Wi-Fi AP with Internet access

iii. Smartphone with Smart Washing Machine app or Computer with manufacturer portal browser

iv. Manufacturer Server

How the different components interact with each other is summarized in the lader diagram in figure 6.

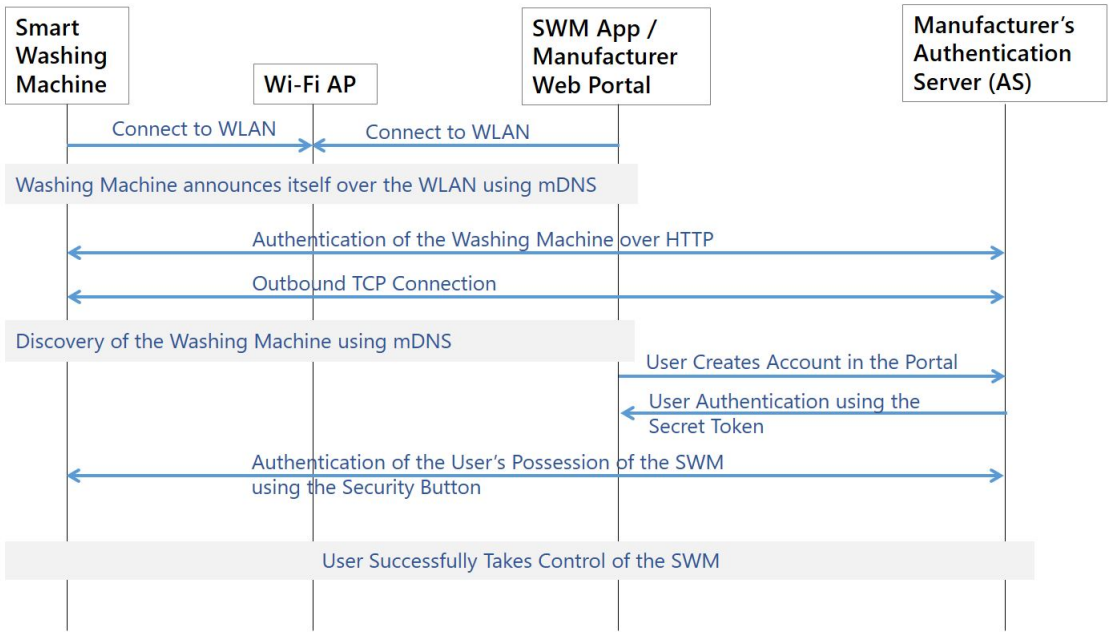

Figure 6: Ladder diagram of the interaction of different participating components in the overall solution

4.2 Scenario 1: Washing Machine in the Owner's Apartment

[WIP]

Wi-Fi: Open Wi-Fi or Internet Lite
The device will be equipped with Wi-Fi capability to connect to the Internet. Once the device is turned on, it will automatically turn on the Wi-Fi and search for a free Wi-Fi network (if available, preferably one with information internet

e.g. BasicInternet) in order to connect to the Internet. It will then access the Vendor Authentication Server to declare that it is available.

5 Security Analysis

Ensuring security of a system involves many different things namely vulnerability assessment, threat assessment and risk analysis. These activities should be repeated peridically to ensure the continual improvement of the security of the system. There are many different industry standards for vulnerability and risk management frameworks for businesses and their IT networks.

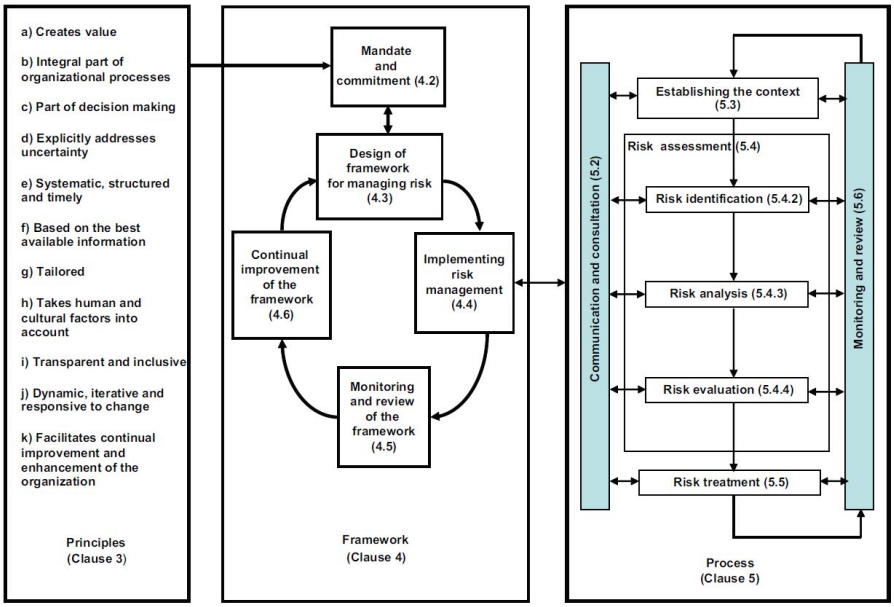

Figure 7: Relationship between principles, framework and process as described in ISO 31000 - Risk Management[18]

5.1 Risk Management Framework

International Organization for Standardization (ISO) published a general purpose risk management framework under ISO 31000 family of standards which is widely used in all types of organizations[18]. ISO published a special framework for IT risk management under **ISO 27000** family of standards. Another international organization, Committee of Sponsoring Organizations of the Treadway Commission (COSO), published a framework for risk management for business enterprises which covers IT also and it is known as **COSO ERM** (Enterprise Risk Management) framework[19]. Information Systems Audit and Control Association (ISACA), an international professional association focused on IT governance, published a major industry standards on IT governance framework like COBIT and Val IT. They added the risk management framework on top

of these standards called **Risk IT**. The ISACA Risk IT framework is based on ISO 31000, ISO 27000 families and COSO ERM[20].

Now, all these frameworks are mainly for business enterprises having an IT network and generally not meant for an isolated network device such as a smart washing machine. However, we can still use the risk assessment frameworks for the security analysis of our smart device. For example, ISO 31000 standard provides principles, a framework and a process for risk management as shown in figure 7. In this paper, I will incorporate the process part from the ISO 31000 framework to identify security risks i. e. the threats and vulnerabilities of the proposed solution and then I will analyze and evaluate the risks associated with these threats and vulnerabilities in the next sections and lastly I comment on the treatment of the evaluated risks.

introduce what you take from ISO 31000 (or ISO 27000 or ISACA)

5.2 Context Establishment

The first thing to do for the risk assessment process of a solution is to establish the context as described in figure 7. Here, the word "context", according to the standard means the objective, parameters for managing the risk, the scope and criteria for evaluation of the risk[18]. In our paper, the objective is that the solution we propose is secure and threats and vulnerabilities are minimized. The scope and criterion of managing the risk are that the solution is not vulnerable to general attack vectors available in the market.

5.3 Risk Identification

The next step is to identify the risks. This is the first step of risk assessment. Now the risks involve two things - threats and vulnerabilities. Vulnerabilities are the internal weaknesses of the system whereas threats are external to the system which utilizes the vulnerabilities to violate the security objective of the system. Every threat has some potential consequences in terms of the security objectives. Risk signifies how likely it is that the severity of the consequences of a threat would be unacceptably high. Before we analyze the risks, first we have to identify the security features, vulnerabilities and threats.

5.3.1 Security Features

Security has been the prime factor the design of the solution. Security is one of the things which has been in the center of design effort. The security features which have been incorporated in the design are listed below -

I. The user gets the Security Token from the manufacturer during the purchase which must be used when the user claims the washing machine from the Manufacturer Server portal.

II. When the washing machine registers or announces itself to the Manufacturer Server portal, it communicates over the TCP with TLS with mutual authentication. Later after the mutual authentication, TLS also ensures confidentiality and integrity of the connection.

III. User has to create an account in the Manufacturer Server portal with a strong password before he can try to claim any washing machine.

optional? your alternatives?

IV. When the user tries to claim a washing machine from the portal, he must push the Security Button located physically in the washing machine for 30 seconds in addition to using the Security Token. This prevents any attacker in the Internet to claim teh machine even if he gets hold of the Security Token.

V. The TLS/TCP connection of the washing machine with the portal is a session initiated by the washing machine (outbound) and not by the portal. This means that there's no need for Port Forwarding in the WLAN at the user premises preventing the vulnerabilities associated with the Port Forwarding.

VI. In order to operate the washing machine online, the user must log in to the portal or the app using his password.

Now, we identify the vulnerabilities and threats in the next sections.

5.3.2 Vulnerabilities and Threats

[WIP]
Even though the design incorporates various security features, there might exist unknown security vulnerabilities in the solution and and threats associated with them. Vulnerabilities are the weaknesses in the solution - both known and unknown. And threats are the external forces or agents which can potentially attack the system utilizing the known or unknown vulnerabilities. However, the known vulnerabilities of the system and threats associated with them are listed below.

a. **Rogue claim:** Someone might get hold of the Security Token and the physical machine. At this point, he can claim the machine and add it to his account and hence can control the machine.

b. **Password brute-force:** Attacker can brute-force the password for user account and take control of the machine.

c. **Certificate theft:** The certificate of the machine is compromised and changed so that a Denial of Service (DoS) attack can be carried out. correct? MITM

d. **Rogue manufacturer:** The Manufacturer Server can be compromised and can be used to exploit the open TCP Connection to do malicious activities to the user device. likelihood (affect every new machine being installed)

This are the known threats and vulnerabilities of the system. There might be unknown ones which can be discovered by the attacker in future. In the next section, we analyze the risks associated with these threats.

5.4 Risk Analysis

[WIP]
A threat becomes a risk if it likelihood of happening and the severity of the consequence both grow higher. Table 3 shows the likelihood and conseguence table of the threats identified in earlier.

use the “usual figures” for risk analysis (graph with axis), colour coding (red, yellow, green), (1), (2), (3) which identify the types of risks

+++	+++	**Likelihood**	+++	+++
+++	+++	**Low**	**Medium**	**High**
+++	**High**			
Consequence	**Medium**	b. Password brute-force	a. Rogue claim	
+++	**Low**	c. Certificate theft d. Rogue manufacturer		

%Table caption above
%Figure caption below

Table 3: Risk analysis of the known threats

describe the details of the figure/table

INTRODUCE: alternative solutions - what will change (f.eks. if no Secure button is on the washing machine)

5.5 Risk Evaluation and Treatment

[WIP]
Risk analysis gives us several risks that are low. These risks can be on the tolerable limit. However, they should be treated and monitored. There's one risk that is medium: Rogue claim. This risk needs to be given priority when it comes to risk treatment.

your suggestion?

6 Evaluation

[WIP]
Evaluation of the solution based on the requirements put forward in chapter 2.

**Evaluation table on convenience, cost efficiency, security and scalability.*

7 Conclusion

[WIP]

procedure: user first has to establish an account _OR_ whether the user first opens an URL on the server, then “identify his washing machine”, connect with the credentials, enters his phone number, and then gets an SMS with the link to the app

References

[1] R. Want, B. N. Schilit and S. Jenson, *Enabling the Internet of Things,* in Computer, vol. 48, no. 1, pp. 28-35, Jan. 2015. doi:10.1109/MC.2015.12

[2] E. Ronen and A. Shamir, *Extended Functionality Attacks on IoT Devices: The Case of Smart Lights,* 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 3-12. doi:10.1109/EuroSP.2016.13

[3] Tiziana Corti, *Connected Home*. Home Appliances World. http://www.homeappliancesworld.com/2015/12/10/home-appliance-2025/connected-home/

[4] A. Chapman, Context Information Security, *Hacking into Internet Connected Light Bulbs*. https://www.contextis.com/blog/hacking-into-internet-connected-light-bulbs

[5] S. Dixit, J. Noll. *Basic Internet Access for All*. http://its-wiki.no/images/e/e9/Basic_Internet_White_Paper.pdf

[6] J. R. Karsnitz, S. O'Brien, J. P. Hutchinson (2013), *Engineering Design: An Introduction* (2nd Edition), Delmar Cengage Learning, ISBN-13:978-1111645823, ISBN-10:1111645825

[7] Oxford Dictionaries. *Convenience* https://en.oxforddictionaries.com/definition/convenience

[8] Cambridge Dictionary. *Cost efficiency.* https://dictionary.cambridge.org/dictionary/english/cost-efficiency

[9] André B. Bondi. 2000. *Characteristics of scalability and their impact on performance.* In Proceedings of the 2nd international workshop on Software and performance (WOSP '00). ACM, New York, NY, USA, pp. 195-203. doi:10.1145/350391.350432

[10] L. Mainetti, L. Patrono and A. Vilei, *Evolution of wireless sensor networks towards the Internet of Things: A survey,* SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, Split, 2011, pp. 1-6.

[11] G. A. Akpakwu, B. J. Silva, G. P. Hancke and A. M. Abu-Mahfouz, *A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges,* in IEEE Access, vol. 6, pp. 3619-3647, 2018. doi:10.1109/ACCESS.2017.2779844

[12] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, and P. Dutta. 2015. *The Internet of Things Has a Gateway Problem.* In Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications (HotMobile '15). ACM, New York, NY, USA, 27-32. doi:10.1145/2699343.2699344

[13] L. Atzori, A. Iera, G. Morabito, *The Internet of Things: A survey*, Computer Networks, Volume 54, Issue 15, 2010, Pages 2787-2805, ISSN 1389-1286. doi:10.1016/j.comnet.2010.05.010.

[14] B. L. R. Stojkoska, K. V. Trivodaliev, *A review of Internet of Things for smart home: Challenges and solutions*, Journal of Cleaner Production, 2017, Pages 1454-1464, ISSN 0959-6526. doi:10.1016/j.jclepro.2016.10.006.

[15] Y. Vardi, S. Scherzer, T. Scherzer, A. Margalit, R. Blaier, Y. Lifchuk (2012). *System and method for mapping wireless access points.* U.S. Patent No. US8126476B2. Washington, DC: U.S. Patent and Trademark Office. https://patents.google.com/patent/US8126476B2/en

[16] GSMA. *eSIM, The SIM for the next Generation of Connected Consumer Devices.* https://www.gsma.com/esim/

[17] GSMA. *Embedded SIM Remote Provisioning Architecture.* Version 1.1. December 17, 2013. Official Document 12FAST.13

[18] ISO, *ISO 31000 - Risk Management*, https://www.iso.org/iso-31000-risk-management.html

[19] COSO, *Enterprise Risk Management — Integrated Framework*, https://www.coso.org/Pages/erm-integratedframework.aspx

[20] ISACA, *Risk IT Framework for Management of IT Related Business Risks*, http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx

---

Mnemonic Notes (rough info to be removed)

Ideas

- Device announcement : Bonjour (used by Apple), Jini
- Put focus on Technology challenges are a short description of different technologies. Then say why you are focusing on this and not on that one.
- Engineering Design Plan devised by Museum of Science, Boston. Karsnitz's book at Google Books.
- Connected Home Schematic http://www.homeappliancesworld.com/2015/12/10/home-appliance-2025/connected-home/

Questions

*From "Methods": In order to be able to implement such a novel solution a lot of things need to come together. These methods encompasses the Internet connectivity of the devices, the vendor of the machine, the machine itself, and the home energy system of the owner. The key aspects that would be taken care of are described below.

- How does Bonjour/Jini work? How can they make things easier?
  * RFC3927 Self-Assigned Link-Local Addressing (Stuart Cheshire), http://zeroconf.org/
  * The 169.254.x.x range of IP addresses is reserved by Microsoft for private

network addressing. If you have a pc set to automatically obtain an IP and you recieve one of these addresses, windows has assigned this because it cannot find a DHCP server within the network subnet. Check to make sure your DHCP server is functioning correctly. If you do not have a DHCP server, you will need to manually set an IP configuration.
* `https://developer.apple.com/bonjour/`

- How LG Smart ThinQ, Samsung EcoBubble, Samsung Crystal Blue implemented this?
  * Wi-Fi network generated by the Smart Device is used to connect the Smartphone! Smartphone is used to connect the smart device to the home Wi-Fi network.
  * TP-Link also used the same to connect the light bulbs. `https://www.youtube.com/watch?v=HxMMCQ3gMSg&t=`

- How Phillips Hue implemented this?
  * With Wi-Fi for Apple HomeKit to connect to the Bridge. The Bridge uses ZigBee to connect to the mesh of light bulbs.

- An HTTP page is announced by Bonjour protocol. Which server do we host this page to? Whirlpool? `https://whirlpool.com/register`

- How the security will be ensured between Portal/App and the AS? TLS built in into the Portal/App will be used.

- `https://en.oxforddictionaries.com/definition/convenience`

- `https://dictionary.cambridge.org/dictionary/english/cost-efficiency`
  a way of saving money, or of spending less money

- Port Forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN).When used on gateway devices, a port forward may be implemented with a single rule to translate the destination address and port. `https://tools.ietf.org/html/rfc2663`
  - The Universal Plug and Play protocol (UPnP) provides a feature to automatically install instances of port forwarding in residential Internet gateways. UPnP defines the Internet Gateway Device Protocol (IGD) which is a network service by which an Internet gateway advertises its presence on a private network via the Simple Service Discovery Protocol (SSDP). An application that provides an Internet-based service may discover such gateways and use the UPnP IGD protocol to reserve a port number on the gateway and cause the gateway to forward packets to its listening socket.

- To identify the threats and vulnerabilities, one of the effective ways is the SWOT Analysis. Here SWOT refers to Strengths, Weaknesses, Opportunities, Threats. Weakness is synonymous to vulnerability. Here, strength and vulnerabilities are the internal factors of the system whereas opportunities and threats are external to the system which affects it.

Not Now

- Authentication Server
- RADIUS/DIAMETER
- TLS for Portal/App to AS security
- mDNS-SD for device discovery in LAN