Integrating Energy Devices through BasicInternet

Syead Nusrat Nur

October 31, 2018

Master Thesis at Department of Informatics

University of Oslo

-Page intentionally left blank-

Integrating Energy Devices through BasicInternet

Syead Nusrat Nur

Student number: 590304
E-mail: syeadnn@ifi.uio.no
syeadnusratnur@gmail.com

Master Thesis at Department of Informatics
University of Oslo

October 31, 2018

Integrating Energy Devices through BasicInternet
Syead Nusrat Nur

http://www.duo.uio.no/

Printed at Reprosentralen, University of Oslo

Abstract

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

Keywords: IoT technologies, Smart home, Wi-Fi, Cellular, Client-server model, IoT security, Risk analysis, Client authentication, Information-Internet

[1]InfoInternet is introduced by the BasicInternet Foundation (`https://basicinternet.info`) on the expectation that people should have the right to access basic information e.g. text and pictures free of cost and described to be a catalyst for achieving the Sustainable Development Goals (SDG) of the Agenda 2030. For more on InfoInternet: `https://its-wiki.no/wiki/InfoInternet`

-Page intentionally left blank-

Preface

This thesis is the final task of the fulfillment of my Masters degree at the Department of Informatics at the University of Oslo and the Department of Technology Systems (ITS)[2].

I would like to thank my supervisor Professor Josef Noll at the Department of Technology Systems (ITS) for guiding me throughout the work and providing invaluable support and constructive criticism. I would also like to thank my co-supervisors Iñaki Garitano, researcher at ITS and Sudhir Dixit, fellow of the BasicInternet Foundation, for being available for guidance and support.

I would also like to thank my family and friends for being supportive throughout the whole process of this Master program.

Syead Nusrat Nur
October 31, 2018

[2]Formerly known as University Graduate Center at Kjeller (UNIK)

-Page intentionally left blank-

Contents

List of Figures

List of Tables

-Page intentionally left blank-

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

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 [4]. 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.

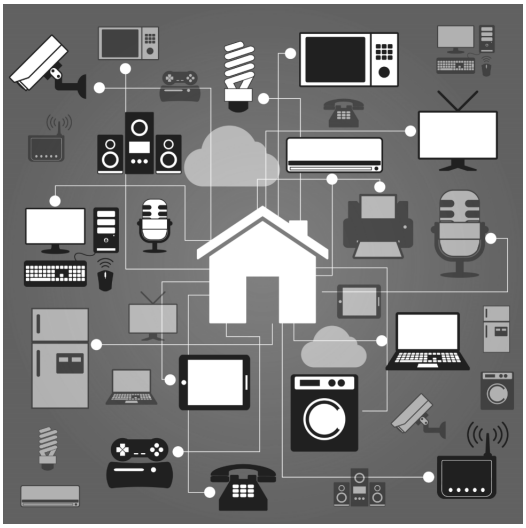

FIGURE 1. **Schematic diagram of a modern Smart Home or Connected Home by Home Appliances World [4]**

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[5]. 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 section 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 analyze how a user-friendly and convenient process to integrate the smart washing machines to the Smart Homes could be built while ensuring cost-effectiveness and scalability and propose a solution. 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.[7]. Figure 2 in page 4 presents an overview of the whole EDP as described in the book.

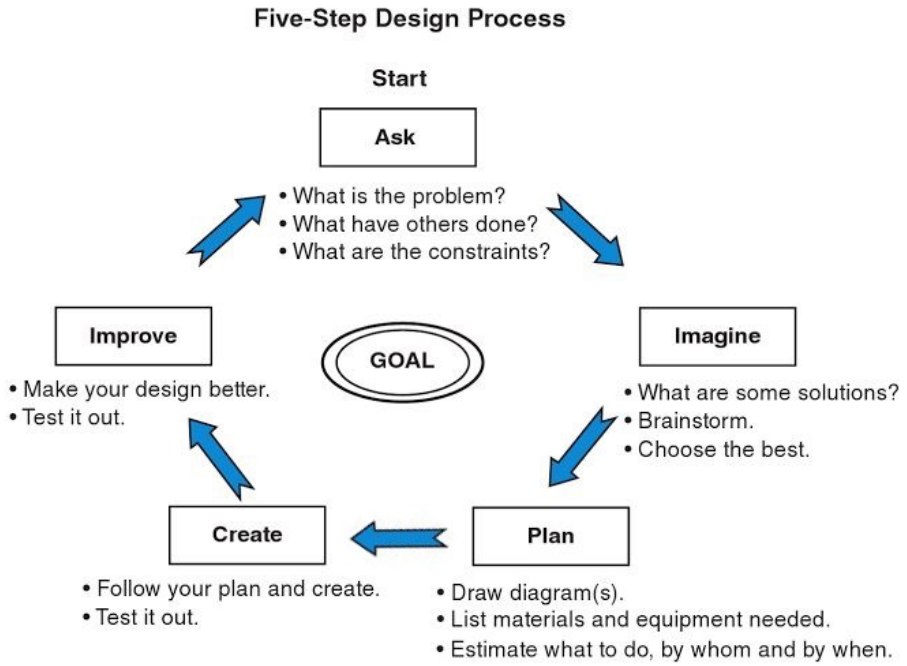

FIGURE 2. **Engineering Design Process developed by Museum of Science, Boston (ref. Karsnitz et al.)**

The process entails the following steps going in cycles: **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.

-Page intentionally left blank-

2 Connecting Home Appliances to 'Internet of Things'

People have been using electronic household appliances, also known as white goods, in their homes for a long time. Today's smart homes are equipped with myriads of home appliances and IoT devices which can interact with one another through a local network or the Internet. Now the household appliances are also getting smarter incorporating themselves into the world of Internet of Things. In this paper, we are analyzing the available technologies and 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 and discussed. In addition, the requirements of the solution will be elaborated and technological challenges will be introduced.

2.1 Scenario: Connecting a Washing Machine

A typical scenario for the solution is the case where the smart washing machine comes with wireless radio capability. Hence it can be connected to 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.

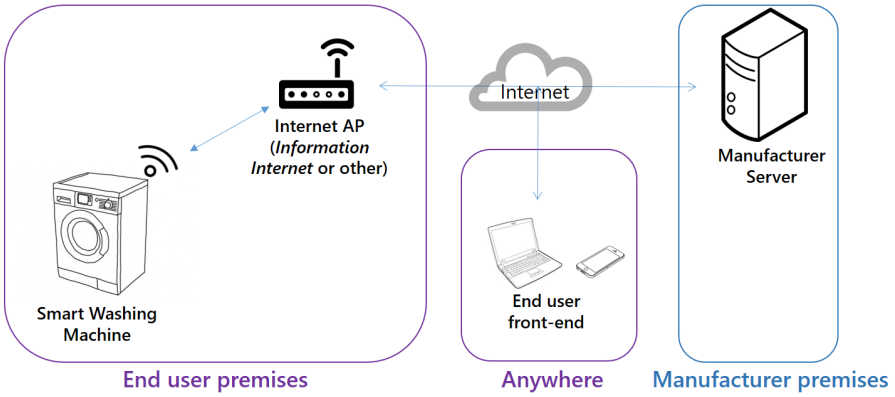

FIGURE 3. **High level scenario for integrating a smart washing machine with the help of an Internet AP**

There are basically two premises of concern in all the scenarios, as Figure 3 illustrates, - **End user premises** and **Manufacturer premises**. The end user premises consists of the Smart Washing Machine (SWM) which the user buys from a selling agent of the manufacturer and a Internet AP (preferably an Information Internet). On the other hand, in the manufacturer premises, we have the Manufacturer Server which act as a middle-ware between the front-end of the end user application for controlling the SWM. These two premises will be connected through the Internet with the help of the Internet AP available at the end user premises. In addition, the end user can control the washing

machine from any network provided that his controlling device is connected to the Internet.

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

STEP 1. When the end user buys the smart washing machine, the supplier registers the user and provides him an authentication token as a proof of the ownership of the device (the washing machine). Later the end user would use this token on the manufacturer's web portal to claim the machine which he buys now.

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

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

STEP 4. After connecting to the wireless network, the device reaches out to the manufacturer's server. After mutual authentication of the device and the server, the server makes the device available for the legitimate user to claim. Now from anywhere with the Internet access, the end user claims his device visiting the manufacturer portal or downloading the smartphone app provided by the manufacturer. For this he uses the authentication token(s) which the user had received during the purchase of the washing machine. Thus, the owner claims the ownership of the machine and takes its full control.

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

These five high level steps introduce the process which will be analyzed and evaluated in detail in terms of the how the these steps can be realized in the design. We will present the pros and cons of the technologies and protocols available as candidates of each step analyzing the relevant works by the scientific community and the industry in chapter 3. Now, in the next section we will put forth the requirements which can extracted from this high level scenario. However, there can be many other scenarios of the solution. The relevant ones will be presented as appropriate.

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' [8]. 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' [9]. 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 [10]. The requirement of the proposed solution is to be scalable. The solution works irrespective of however many users are needed. It also covers practical scenarios of use cases with high level of flexibility. The solution will not be limited only for few users. The functionalities does not cease to work if the user load increases.

2.3 Technological Challenges

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) telecommunications technologies. 5G (NR) is on the horizon to facilitate the development of IoT sector even further. Other IoT wireless technologies like Sigfox, 6LoWPAN etc. also promises great flexibility for the use cases of IoT development. Wi-Fi is ubiquitous in home and office environments, and even in outdoor settings in some cases, giving people unprecedented flexibility and ease for day-to-day work.

On top of these lower layer wireless technologies, we have various other technologies in different higher layers of OSI model to facilitate the communication

in the IoT setting. HTTP, XMPP, MQTT, CoAP are some of the application layer protocols which can serve the required purposes taking the advantage of the reliable connectivity provided by TCP or SCTP in the transport layer or even the faster delivery over connectionless transport protocol like UDP. Moreover, for the security layer these communication protocol stacks can leverage the proven services of TLS, DTLS, IPsec etc. However, one significant challenge is to provision a sophisticated and scalable authentication mechanism to ensure that the authentic devices are managed by the authentic end users. All these different options and functionalities really push the IoT designers to their limits to find the best match of technologies from this vast ecosystem of possibilities.

Following that line, device-to-device (M2M) communication and "Internet of Things" are the growing focuses of the research and development communities in recent years. Home automation and energy management is also a part of it. This is where our thesis comes into picture. How the technological challenges can be resolved in order to design a convenient, cost-efficient, secure and scalable solution of integrating a household appliance to the Internet of Things is the subject matter of the chapters that follow.

3 Analysis of Technologies

Integrating smart devices such as smart washing machine to a modern home and operating them are not trivial tasks. Many cutting-edge technologies need to come together to achieve this. Firstly, the washing machine resides at a place where a suitable networking solution need to be available for establishing an Internet connection. The machine needs to be able to connect to that network easily. Once the machine has the connection to Internet, it needs to establish a communication channel with the user via a front-end application for operational instruction. This communication is proposed to be established via the manufacturer server (middle-ware) located in the manufacturer premises.

Now there are still different aspects which we must put in place for a viable and secure communication between the machine and the user via the manufacturer server. For example, the device needs to be authenticated to the server and vice versa. The user also needs to be authenticated by the server in order for him to claim the correct machine. Finally the administration of the users and management of the device need to be in place.

In this chapter, we will discuss all these design aspects of the solution in great detail building on the technologies available in the art. We will also analyze as to which of the technologies work better for the target solution and propose an end-to-end solution.

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[11]. 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**[14]. 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 known as Long Range Wide Area Network (LP-WAN) technologies and overwhelmingly use the ISM bands. Many of these technologies are proprietary and not openly available.

Examples of short-range wireless technologies are Bluetooth, Bluetooth Low Energy (BLE), Thread, ZigBee, Wi-Fi etc. Most of these 2 types of technologies use freely available ISM frequency bands for wireless communication. They are based on various works of IEEE 802 LAN/MAN Standards Committee[12]. Bluetooth and BLE is based on lower layer standards from IEEE 802.15.1 while ZigBee, Z-Wave, Thread are based on IEEE 802.15.4 Low-Rate Wireless PAN. Upper Layers of Thread are based on IPv6 capable IETF standard 6LoWPAN. Wi-Fi is based on IEEE 802.11 Wireless LAN. 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 are not restricted by such power limitations.

TABLE 1. **Various wireless access network technologies for IoT**

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

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[14]. 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. One of the favorable aspects about cellular technologies are that they are widely available in all kinds of terrains and run on licensed electromagnetic spectrum which means they can ensure better quality of service than their license-free ISM band counterparts.

All these wireless telecommunication technologies are specified by the Third

Generation Partnership Project (3GPP)[13] and approved by International Telecommunication Union (ITU). The standardization of the newest wireless telecommunication technology from ITU and 3GPP, 5G NR, is under way and hence is not commercially available yet[13]. 5G NR is designed to be more suitable for IoT.

3.1.2 Feasibility Study of Wireless Technologies

Now that we have introduced different wireless technologies as candidates for our washing machine, we need to find out which of these technologies are more suitable for our solution. 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 marked in 3 levels - **Not so good (-1), Reasonable (0) and Good (+1)**. Finally all the ratings of a wireless technology are summed to provide the overall rating.

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.

Case A. Washing machine is located at the same house as the end user

Case B. Washing machine is located at a different place than the house of the end user

In Case A, the washing machine is located inside the house where the end user lives. In this case, it is highly likely that a home Wi-Fi AP is available which is also managed by the end user - either open or protected. In this case, Wi-Fi would be deemed preferable 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. Another reason for choosing Wi-Fi would be that washing machines are always connected to power and hence the power they need for running Wi-Fi radios is abundant and there is no restriction for power or battery problem.

The challenge with some of the other short range low power wireless technologies based on IEEE 802.15.4 Low-Rate Wireless PAN, 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 wireless technologies[15]. The good thing about Wi-Fi, in this respect, is that it makes an IP-based wireless local area network (LAN) and hence the smart washing machine would avoid the gateway problem meaning that it would not need to convert the header of the "packets" between IP and non-IP protocols. The phones and laptops with manufacturer portal browser would easily reach the washing machine both while in the house and outside.

Now, for 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:

Sub-case 1. Private washing machines of all the apartments of an apartment building or housing society are housed in a common laundry room.

Sub-case 2. 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 (e.g. 'fellesvaskeri' system in housing societies in Norway).

Sub-case 3. The end user or 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 same Wi-Fi network as that of the end user'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 more suitable for these scenarios. However, they are not widely available commercially yet and most of the technologies are proprietary. Moreover, LPWAN technologies are competing with each other in this landscape and there is no clear winner yet.

Table 2. **Evaluation of different networking technologies for the smart washing machine (Not so good = -1, Reasonable = 0 and Good = +1)**

Wireless Technology	**Range**	**Availability**	**Power Consumption**	**Cost**	**Gateway Required**	**Noisy Channel**	**Data Rates**	**Overall Rating**
LoRa, Sigfox	+1	-1	+1	0	+1	0	-1	+1
Ingenu-RPMA	0	-1	+1	0	+1	-1	-1	-1
DASH7, Weightless	0	-1	+1	0	+1	0	0	+1
Bluetooth	-1	+1	0	0	-1	-1	0	-2
BLE	-1	+1	+1	+1	-1	-1	0	0
ZigBee	-1	0	+1	+1	-1	-1	-1	-2
Z-Wave, Thread	-1	0	+1	+1	-1	0	-1	-1
Wi-Fi	-1	+1	0	+1	+1	0	+1	+3
GSM, UMTS, LTE	+1	+1	-1	-1	+1	+1	+1	+3
EC-GSM-IoT, LTE-M, NB-IoT	+1	-1	0	-1	+1	+1	0	+1

However, the cellular technologies in Case B 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" because they are based on IP and directly connect 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 manufacturers 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[21]. One of the many benefits of eSIM is that multiple SIMs from multiple Cellular Network Operators can be downloaded in or pushed to the same eSIM at the same time using the 'Remote Provisioning Architecture' of the operators which also enables the user to change the operator easily as and when he wishes[22]. However, in order to avoid complex wireless technologies 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 +3 each. The technologies are compared on range, availability, power consumption, cost, topological challenge, noisy channel and data rates suitable for washing machine's communication with the Manufacturer server over the Internet[15, 16, 17]. Technologies that uses widely used ISM bands for example 2.4GHz tends to be noisy and hence received negative points. On the other hand, in our solution, the washing machine needs to transfer a lot of data frequently with the server and hence does not get much help from the technologies which offer very low data rates.

However, since Case A prefers Wi-Fi whereas Case B prefers cellular, this conclusion readily 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 with 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. However, cellular can still be chosen if deemed appropriate.

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*[6]. 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[6]. 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[6]. 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

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[20].

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 Communication Technologies

Now that the washing machine is connected to the Internet, let's see how the different components of the solution would communicate to each other. A typical scenario of the overall topology with IPv4 would look like the Figure 4. In this scenario the washing machine is located in a wireless LAN with a private IPv4 address and the manufacturer server is located in the manufacturer premises with a public IPv4 address. And the smartphone device management application or laptops with manufacturer web portal access can control the service the WLAN as that of the Washing machine or some other WALN or even in a different type of access network e.g. LTE mobile network. In all the cases, the smartphone or the laptop has a private IP address in the local network.

Now in this scenario, the communication between the end points can happen the following way. The end user now located in his office served by the office Wi-Fi take out his smartphone, opens up his washing machine app and starts a washing cycle in the washing machine by pressing a button in the app. This command needs to reach the washing machine through the Internet. En route to the washing machine which is located at the end user's house, the command reaches the manufacturer server first with a secure connection. At this point, the manufacturer server (MS) needs to push the command to the end user's washing machine. However, because the washing machine in a LAN which in general uses Private IPv4 address ranges and outbound Network Address and Port Translation (NAPT) technology[30], the LAN will not accept any inbound traffic or session from the Internet and hence the push will not reach the washing machine. Besides this, the LAN at the house may have a firewall which normally would not allow any unsolicited traffic from the Internet.

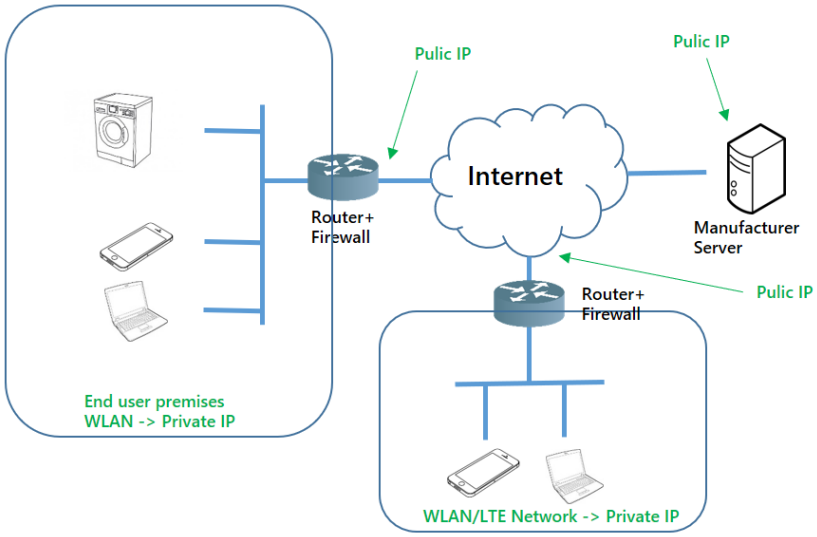

FIGURE 4. **A typical scenario of the overall networking topology with IPv4 encompassing all endpoints**

For security reasons, LANs use basic firewalls to restrict incoming traffic from the Internet. Morveover, due to high usage of IPv4 networks, most of the LANs have to use NAT or NAPT so that scarcity of unique IPv4 address space can be overcome. For these reasons, in most LANs it is not possible to send traffic from outside the LANs e.g. from the Internet into the LAN. However, incoming traffic is allowed through opening ports as response to an outgoing connection request. Cellular networks also use NAPT in case of IPv4. Even though IPv6 address space is huge, it is still not widely adopted. However, even IPv6 are adopted in some networks, still they would not allow incoming traffic to the network devices from the Internet and they would be blocked by firewalls etc. Morover, the Internet communication model does not allow the servers to create connection with client, rather the clients are expected to initiate the connection to the server. These are some of the communication problems in our solution which we discussion in the next sections.

3.4.1 Internet Communication Models

Today's Internet is a distributed computing system based on **Client-Server Model** where resources are stored in centralized high performance server machine capable of serving a lot of requests at the same time. On the other hand, clients are the end devices requesting for information and resources from the servers. Servers 'listen' on different transport layer 'ports' and clients initiate sessions with the servers requesting for resources on those open 'ports'. Another model used in the Internet is the **Peer-to-Peer Model** where each device in the network is equal and requests for resources and serves the requests directly. However, this model is limited in use and used only in special cases. In our

solution we will not use this model. We would focus on client-server model.

Within client-server model, there are several ways the end stations or clients communicate with the servers. Two of the most widely used ones are - **Request/Response** and **Publish/Subscribe**. In the Request/Response model, the client requests for resources to the server. On the other hand, in the Publish/Subscribe model, clients subscribe to the server for some 'channels' of information or resources. Then when new information or resources of those 'channels' are published to the server, the server pushes them to the client which have subscribed for those 'channels' of information or resources.

One of the most widely used application layer protocols for communication over the Internet in the client-server model is HTTP (Hypertext Transfer Protocol)[32]. It is a Request/Response protocol. With this protocol the client uses different HTTP methods e.g. GET, POST, PUT, DELETE etc. to retrieve resources from the server, to create or update resources and to delete resources in the server etc. Some of the example protocols using the Publish/Subscribe model is MQTT (Message Queuing Telemetry Transport)[33] and XMPP (Extensible Messaging and Presence Protocol)[38]. MQTT is a simple, lightweight, easy-to-implement application layer protocol suitable for IoT and M2M communications where bandwidth is at premium. XMPP is a XML-based communication protocol for messaging and presence widely used for different use cases including device management and IoT. All these protocols discussed above (HTTP, MQTT and XMPP) run on TCP.

Now that we have discussed how the clients initiate requests to the servers, let's discuss how to solve the problem stated in Section 3.4, how the server pushes the commands to the washing machine located in a Private LAN.

3.4.2 Push/Pull Technologies

To solve the problem of how to push commands from the manufacturer server to a washing machine client in a Private LAN, we need to the push and pull technologies. In **Pull Technology** the client initiate the request and the server responds and closes the connection after the request is served. The reverse process is known as the **Push technology** where the server initiates the delivery of the resources or information to the clients.

Push Mechanisms: Push technology can be implemented in many ways. One of the ways is to run **Periodic Polling** - in every few seconds the client would create a connection to server and using that connection it would send a request to the server checking if there is any command waiting for it in the server. While this method is very simple, but it suffers with latency and many polls returns no resources since most of the times there was no resources in the server for the client. To overcome this problem, many new technologies were proposed. One of them is the **Long Polling**[31]. With this mechanism, when the client makes an initial request, the server keeps the request pending and does not reply to it immediately until there is any data available for the client. When the server pushes the data to the client, the client immediately sends

another request.

Another mechanism is **HTTP Streaming** used in used in HTML5 WebSocket API[31]. In this case, the server does not terminate the connection after serving a request to the client until one of them dies. This enables a real-time full-duplex TCP connection between the client and the server.

Now that we have discussed different mechanisms available for Server Push technology we can recommend some solutions for our problem. Since we require the client to receive any commands immediately sent from the end user application to the server, it is recommended that we use Long Polling to keep a TCP port open for the server to push commands to the client near real-time.

3.5 Mutual Authentication of Device and Server

Internet of things is a place of millions of device out in the field creating a overwhelmingly vast network of devices, sensors, actuators etc. One of the daunting challenges of this vast distributed network is the mutual authentication of the devices and the servers which they connect to. Mutual authentication is required for the manufacturers to be able to ensure that the right end devices connect to the servers and likewise, the devices are certain that they connect to the right server. If this is not implemented correctly, many security issues will surface very quickly and the solution will fail within a short time. The vaster a network is, the vaster becomes the attack surface of the network in terms of security. It's the manufacturers' duty to keep the devices and home network out of security issues as much as they can.

Moreover, since the end devices connect to the Internet over some wireless networking technologies, the mutual authentication of the devices and the servers is even more important. This is because the the wireless network does not have the inherent security of a a wired network. We will analyze state-of-the-art solutions for the device and server mutual authentication in different scenarios.

After the end user buys the washing machine and takes it home and powers it up, the machine connects to the Internet over one of the wireless networking technologies available. Now the device has already been provisioned with the DNS domain name of the Manufacturer Server (MS) which works as an Authentication Server (AS). Say, this is `ms.swm-mf.com`. Therefore, as shown in Figure , the machine resolves IP address of the DNS domain name `ms.swm-mf.com` with an available DNS server and initiates a TCP connection with the manufacturer server through a TCP handshake. However, before or after this communication is established, the washing machine working as a client here must authenticate the Server and the Server must authenticate the client. Afterwards, the two entities may establish key materials and continue a secure connection. One important thing to notice here - the authentication needs to be done after the washing machine has been assigned an IP address, private or public. This means the authentication mechanism must work on top of IP layer or at least at IP layer.

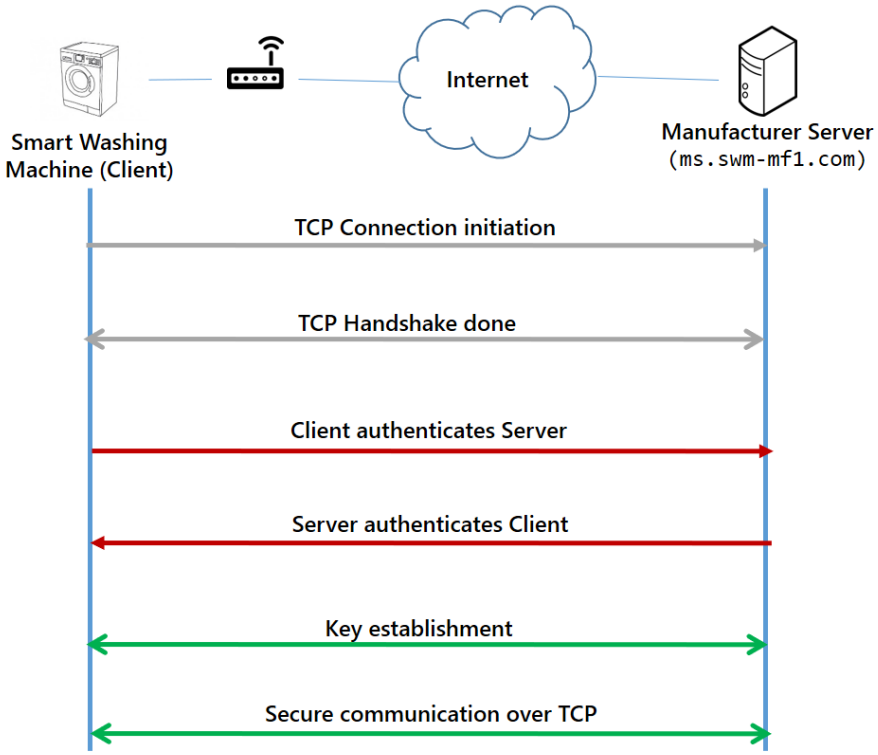

FIGURE 5. **Mutual authentication of the washing machine and the Manufacturer Server**

There are many mechanisms available for mutual authentication in the current art. These mechanisms work in different layers of the TCP/IP protocol stack. However, in terms of the mechanism, we can put them into at least two categories - Challenge-Response based and Certificate based. We will discuss these mechanisms and their usefulness in our solution.

3.5.1 Challenge-Response Based Authentication

In this mechanism, one entity challenges the other one with a challenge and waits for the right response. If the response is right, the first considers that the other entity has been authenticated. The same thing happens the other way around if mutual authentication is required. The challenge could be username-password, biometric system or some other pre-defined questions known only to the client and the server. In general practice, only the servers authenticate the clients and the clients either does not authenticate the Servers or it is done in another higher layer at a later stage[34].

This mechanism of authentication is one of the oldest one and therefore, there exist many different protocols that are based on this mechanism. To give a

few examples which works in Most of the challenge-response authentication protocols work at application layer, for example, CHAP, RADIUS, Diameter, CRAM-MD5, ZKPP, SCRAM etc. EAP is a framework that can work many different methods; however, it works before the IP address is assigned to a node, hence not suitable for our purpose.

Security Issues Earlier protocols of challenge-response based authentication had a lot of security vulnerabilities. For example, anyone would be authenticated who has the password. The passwords were sent in the clear which could easily be intercepted. If the server password database in compromised, then all the passwords of all the users are compromised causing a catastrophic failure of the system. Moreover, these protocols could easily succumb to reply attacks and man-in-the-middle attacks. Later protocols have tried to resolve all these issues by, for example, using a pool of passwords and choosing only a specific one. Servers started using salts and hashing of the passwords to save them in the database whereas clients only send hash of the passwords instead of sending it in the clear.

In our case, if we want to use a challenge-response based mutual authentication mechanism for the client and the server, the client or the server should be able to respond to the challenges autonomously without any help from the end user. This could lead some extra level of automation. Moreover, the management of the mechanism could be somewhat impractical compared to certificate based authentication. For example, the renewal of the shared secret must be secure.

3.5.2 Certificate Based Authentication

The other mechanism for mutual authentication is based on digital certificates or X.509 certificates. In this mechanism a Public Key Infrastructure (PKI) is required in order to create, manage, distribute, store and revoke digital certificates. This mechanism is rooted in the asymmetric key cryptography which can authenticate the other party and can also generate the symmetric keys to be used for confidentiality and integrity protection. The same infrastructure can also be used for other security services like digital signature, non-repudiation etc.

The mechanism entails a pair of keys for each entity - one of them is private and kept secret to the entity itself while the one is publicly known and shared. If the entity Alice signs a message, all the other entities receiving the message can be certain that the message is actually from Alice examining the signature with the public key of Alice. However, the problem is that its not possible to verify that Alice is the true owner of that public key. To solve this, PKI is created where a generally trusted Certification Authority (CA) with a X.509 certificate issued to Alice certifies that the true owner of the public key and hence the corresponding private key is Alice[35].

In our solution, we propose that manufacturer sets up a *private* **Root Certificate Authority** and installs Client Certificates in all the Smart Washing Machines they sell during or at the end of the manufacturing process. Generally

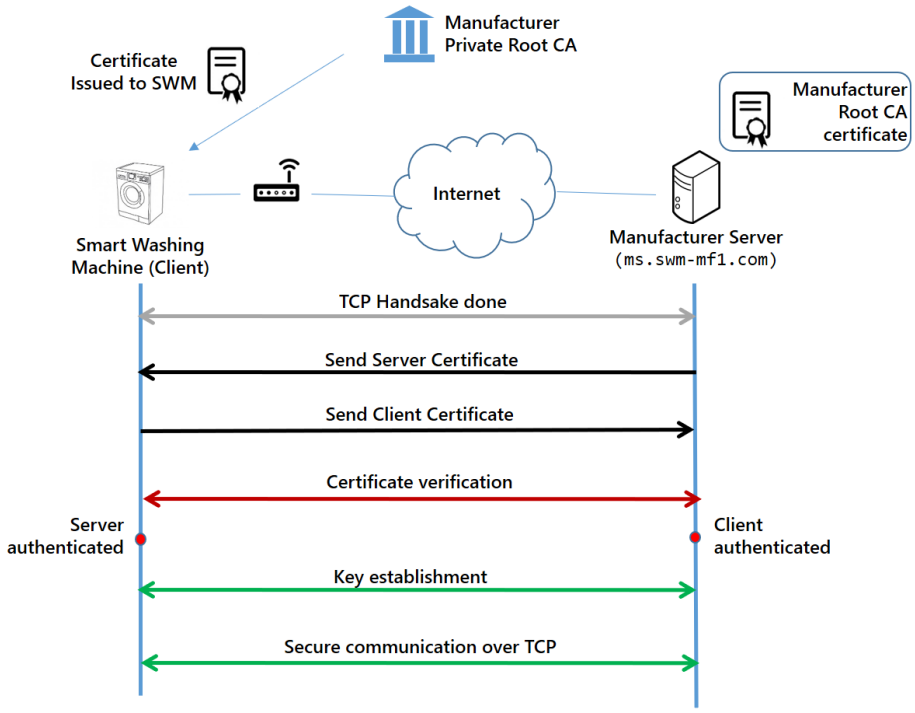

FIGURE 6. **Certificate based mutual authentication of the Washing Machine and the Manufacturer Server**

all the washing machines of the same manufacturer have Unique IDs or Serial Numbers within the manufacturer infrastructure for various purposes. However, this Unique ID could be extended to the form of a domain name and it would be the Common Name (CN) of the subject in the X.509 certificate issued to the washing machine.

Now, the Manufacturer Server will have the Manufacturer Root CA certificate installed in it, hence it trusts this CA. It means that the valid certificates issued by the Manufacturer Private Root CA to the Washing Machines would be trusted by the Manufacturer Server. On the other hand, the washing machine comes with the Root CA certificate of the manufacturer Private Root CA or some other commonly trusted CA which means the washing machine trusts the certificates issued by these CAs. Therefore, the certificate of the Manufacturer Server to be sent to the Washing machines could be signed by the Manufacturer Root CA or the other commonly trusted CA which the Washing Machine trusts. As shown in Figure 6, the mutual authentication is successful when both the washing machine and the manufacturer server successfully verifies the digital certificates provided by the other side. At this point, the communication between the two entities are secure after the symmetric keys have been established in both sides using public key cryptography. Now we discuss the actual protocols which can be used for this.

IPsec Authentication protocols based on digital certificates are IPsec, TLS/SSL, EAP-TLS etc. EAP-TLS is suitable for us since it is designed for device authentication in a LAN and works below IP layer[35]. Internet Protocol Security or IPsec is a family of different authentication, encryption and integrity protection protocols. It is based on authentication protocols ISAKMP or later IKEv2 and it works at the IP layer, hence useful for creating secure VPN tunnels site-to-site or remote-access. Since IPsec works at IP layer, this protocol is one of the most secure protocols and can be used in our solution. However, this could be more expensive than, for example TLS, because IPsec is more resource-intensive on client due to, for example, its use of more overhead and different databases like Security Policy Database (SPD) and Security Association Database (SAD). Nevertheless, IPsec also generates the keys for secure communications between peers using protocols like ESP and AH. IPsec is a very secure protocol for mutual authentication and can be a good choice for our solution.

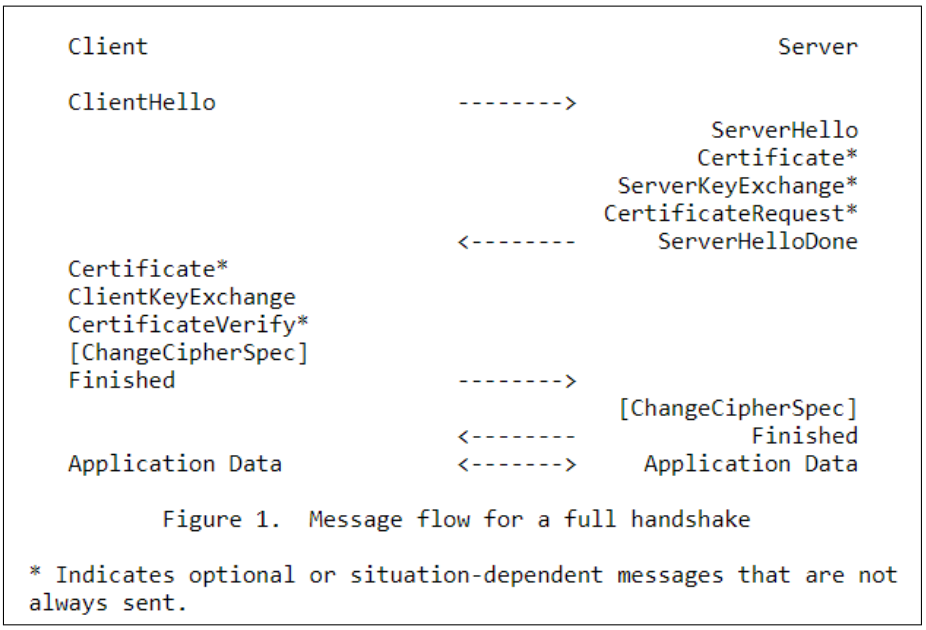

FIGURE 7. **Message flow for a full TLS handshake as specified in RFC 5246[36]**

TLS Transport Layer Security is the most common certificate-based authentication and security protocol in the modern Internet. It's previous versions were known as Secure Sockets Layer (SSL). It works in the transport layer in TCP/IP model or just above transport layer (session layer) in OSI Model. TLS is used on top of commonly used reliable transport protocol TCP[35]. There is another version of this protocol called DTLS or Datagram TLS which is suitable for using on top of the other commonly used but unreliable transport protocol UDP.

TLS is widely used by the web servers for secure browsing, email etc. However, by default only the server authentication is implemented in most, if not all, of these cases and the client authentication is not done, instead user authentication is optionally done in the application layer using mostly Challenge-Response based protocols[36]. Das et al. provides the possible reasons for doing this[37]. The possible reasons could be that (i) client authentication is not required, (ii) computational cost increases, (iii) client needs to buy his certificates from a trusted CA and lastly (iv) user faces less flexibility carrying his certificate if he wants use the same application in different clients. However, for our case these reasons are not valid because, for example, the authentication application in the client machine does not move from machine to machine and the users don't need to buy the certificates, rather the certificates would be issued by the manufacturer themselves. Computational cost should be within the limits allowed by the machine. This is why we already see both the client and Server authentication is used in M2M communication in some cases.

Figure 7 is an snapshot of a full TLS handshake from RFC 5246. We can see here that `CertificateRequest` message from the server and `Certificate` and `CertificateVerify` messages from the Client are not used by default. However, for client authentication this messages must be mandatory. The server must request for a Certificate to the client and the communication will be dropped with an alert message to the client if client fails to provide a valid certificate.

There are several things to ensure when it comes to smooth operation of certificate based authentication mechanism. Certificates issued to Washing Machines should be possible to renew. This is very important in case the certificate is compromised or it's just too old. This renewal process could be done in an automatic fashion periodically which is discussed later in this chapter. On top of this, the certificate should also be possible to renewed on demand. Another important thing is to manage the Certificate Revocation List (CRL) carefully. New alternative standards like the Online Certificate Status Protocol (OCSP) can also be used to minimize bandwidth requirement and managing high-volume operation.

3.6 Registration and Availability of the Device for Claim

After the washing machine connects to the Internet, authenticates itself with the manufacturer server the machine and establishes a secure communication with the server, it should be available for the owner or legitimate end user to claim the ownership of the machine. To implement this, we the washing machine needs to be available in the manufacturer server so that anyone having proper authentication can actually claim the machine. In this section, we discuss the ways this could be implemented.

During purchase the purchaser or the end user must register his phone number or his e-mail address with the seller or manufacturer. Manufacturer or the seller binds the **Unique Identity (UID)** of the machine with the phone number or the email address of the end user or purchaser in the manufacturer server so that it can be used later as a proof-of-ownership.

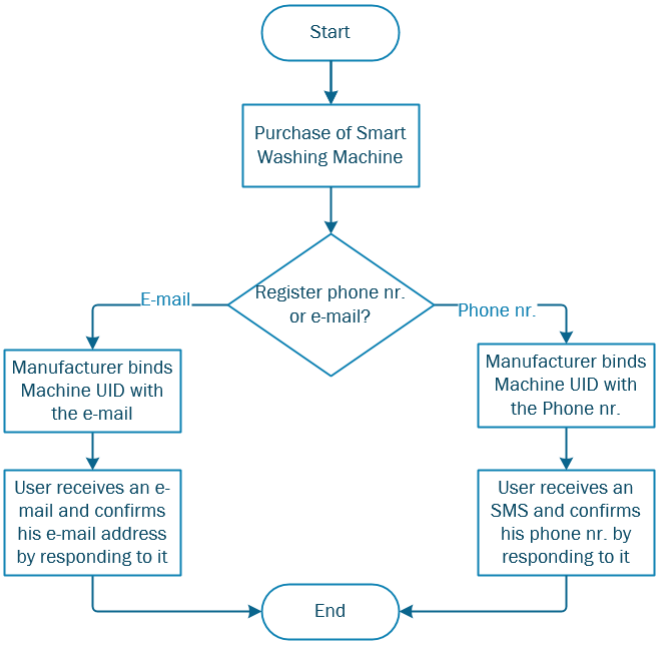

FIGURE 8. **Registration of the Smart Washing Machine during purchase**

Now when the end user tries claim the machine using his phone number or email address, the smartphone app for controlling the washing machine or the manufacturer web portal will present the washing machines available for the end user to claim based on the binding of the UID of the machine and phone number or the e-mail addresss of the end user.

In our analysis, DNS-Based Service Discovery (DNS-SD), Multicast DNS (mDNS) etc. protocols used for service discovery in the Internet or LAN are not deemed necessary for announcement and discovery of the washing machine because, the server can present the washing machines already to the end user based on his e-mail address or phone number. However, if control of the washing machine is intended over the WLAN locally, then they might be utilized.

3.7 User Authentication for Legitimate Claim

The end user will be able to control the machine from anywhere in the world. He will be able to control the machine using a smartphone application provided by the manufacturer or logging on to the manufacturer web portal using an Internet browser. However, the key point here is that he will be able to control the machine irrespective of whether he is under the same LAN as the washing machine in the apartment or he is anywhere outside the apartment LAN connected to the Internet in some other ways as depicted in Figure 3.

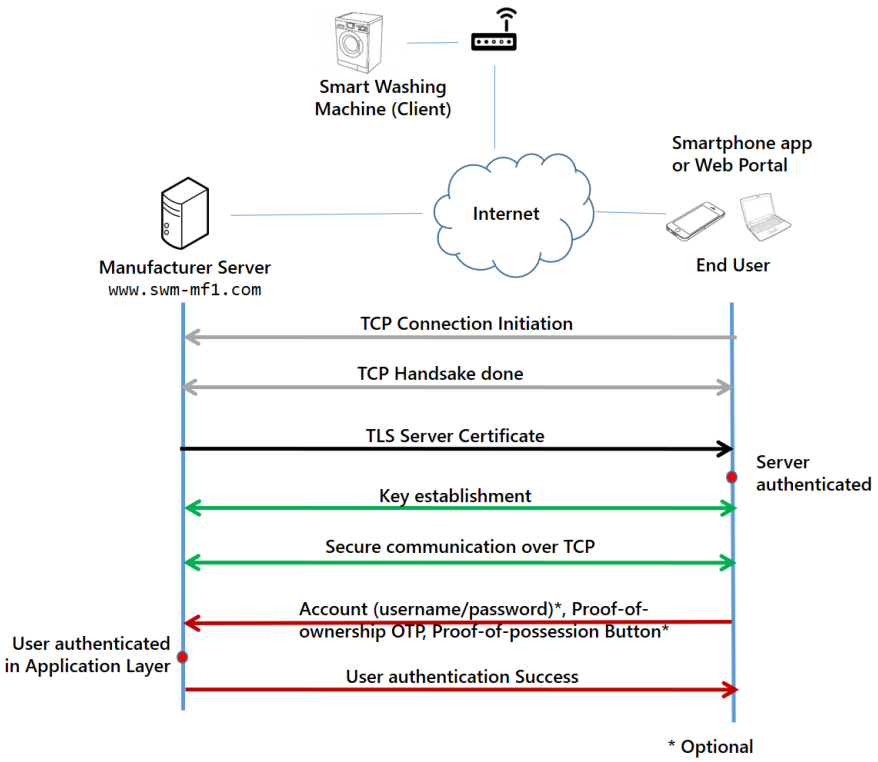

FIGURE 9. **The communication flow between the end user and the manufacturer server in order to claim and control the washing machine**

However, in any case the requirement is that the user is authenticated by the washing machine manufacturer server as the legitimate owner or user of a washing machine before he can control the machine. For this, the overall procedure can be summarized as depicted in Figure 9. Firstly, the user initiates a TCP session with the manufacturer server for a TLS handshake. With TLS the user application or browser authenticates the server and creates key materials for secure connection. Then the user authentication procedure can take place in the application layer using OTP, etc. The steps are further described in the following sections.

3.7.1 Secure Connection between User and Server

In order to control the washing machine, the first thing the user needs to do is to download the washing machine app in his smartphone or visit the web portal of the smart washing machine manufacturer, say, `www.swm-mf1.com` using an Internet browser. Figure 10 shows a flowchart of all the steps associated with the authentication of the user for legitimate claim of the machine. the smartphone application or the web browser will create a secure connection to the Manufacturer Server. This can be achieved by TLS over TCP utilizing the

digital certificate of the Server using a Public Key Infrastructure. Here we don't need to use a client certificate for the authentication of the user's smartphone or browser. The user authentication can be left to the application layer which is discussed afterwards. The use of TLS would ensure that Man-in-the-middle attack, replay attack etc. do not happen in the User-Server communication. In addition, it provides integrity and confidentiality protection for the connection.

3.7.2 Creation of User Account

Before the user can claim and control his washing machine, he will be told to create an account using the app or in the web portal. User's email address or phone number can be used as the username of the account and the user needs to choose a password for his account. Standard secure password policy must be applied so that the account can't be easily compromised. The email address of the user or the phone number should be verified. For this the manufacturer server may send a One-Time-Key by an email to the email address or by an SMS to the Phone number used during the account creation. This step authenticates the user to the manufacturer server.

This step can be implemented as an optional one. The user may go directly to the next step to claim the washing machine using his phone number of e-mail without creating an account. However, it is encouraged that the user creates an account for better administration of the machines settings and administration of other users of the machine.

3.7.3 Proof of Ownership and 2-Factor Authentication

Now that the end user has created an account in the manufacturer's database server, he is ready to claim his washing machine. To ensure that only the legitimate user can claim the machine, a proof-of-ownership mechanism needs to be in place described as follows.

During purchase the user must register his phone number with the seller or manufacturer. Manufacturer binds the **Unique Identity (UID)** of the machine with the phone number or the email address of the end user or buyer in the manufacturer server to be used for the proof-of-ownership. This phone number or e-mail address works as "something the user knows". Now, to allow a **Two-Factor Authentication (2FA)**, user may also receive a **One-Time-Password (OTP)** to be presented each time he claims the machine, as mentioned in Figure 8 before. This will work as "something the user has". Every time the end user tries to claim the machine, an OTP for proof-of-ownership will be sent to his phone number or email. This is especially important if the end user chooses to access the machine without creating an account.

When the end user logs in to the account the application presents to him the washing machine (or washing machines, if he buys more than one using his phone number of e-mail address) which he purchased based on the the phone number or email address which the machines were registered with. Now, if the user created the account with his email address, the washing machine is regis-

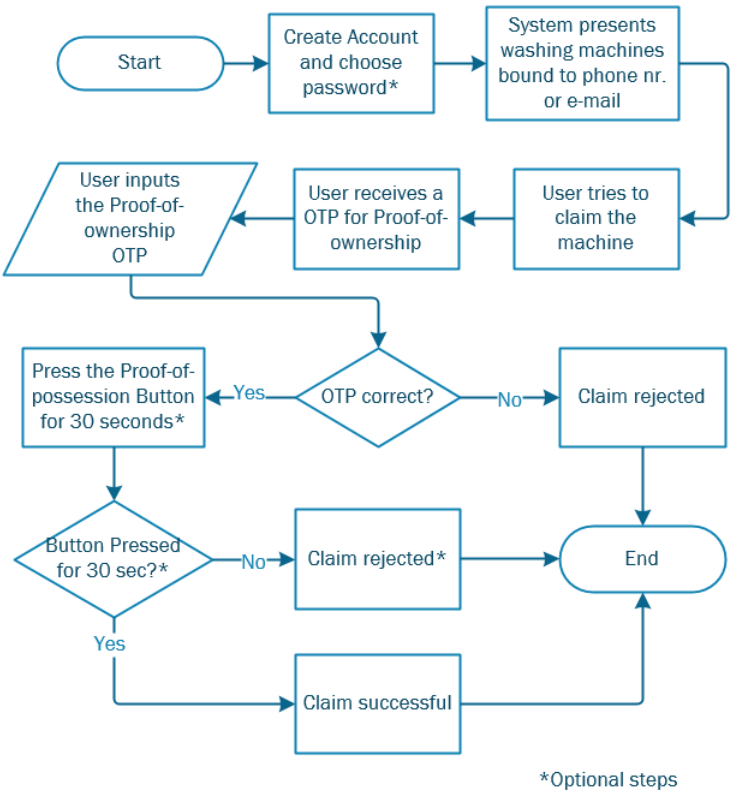

FIGURE 10. **Flowchart of the authentication procedure of the user for legitamate claim of the machine**

tered with his phone number during purchase, the system will not be able to find his washing machine. In this case the system will ask the user to provide his phone number first and it will authenticate the user's phone number before it presents the washing machine to the end user to claim. This authentication can be done using a One-Time-Key sent to his phone as a Short Message (SMS) which the user needs to input to the system. The process will be vice versa if the user registers the machine with his e-mail address and opens the account with his phone number.

At this point, the manufacturer server presents the machine or machines (if the user buys more than one machine under his phone number or email) bound to his name which have not been added to his account yet. During claiming of a new machine, the system may send an OTP for the proof of ownership OTP to e-mail address of the user by an e-mail or to the phone number of the user by an SMS in order to allow the claim of the device. The user has to use that OTP to claim the machine. This step will ensure that only the legitimate users registered with the machine are able to claim the machine. If the code provided by the end user is correct, the system will allow the end user to access the washing

machine using the online platform.

3.7.4 Proof of Possession of Device

One additional layer of security could be optionally added namely the verification of the physical possession of the machine to the end user. The idea is that during the claiming process the user should be able to prove that he has the physical access to the machine. The reason for this important could be the following. If a rogue individual gets access to the phone number or the SIM card of the user, he could claim the machine in his own account and block access to the legitimate user of the machine. This could be viewed as a Denial-of-Service attack. To avoid this kind of attack, a **Proof-of-possession Button** could be placed in a corner of the machine. During the claiming process the user has to press this button for some time (say, for 30 seconds) making the manufacturer server aware that the user who is trying to claim the machine has physical access to the machine and will allow him to add it in his account.

3.8 Device Management and Operation

After the washing machine has been claimed by the end user, he can control the machine from anywhere in the Internet. For that he just need to open his smartphone application for the washing machine and start a washing cycle or stop one etc. During this process, the communication between the Washing machine at his apartment and the smartphone app is brokered by the manufacturer server located in the manufacturer premises. However for the continued smooth operation of the machine, the manufacturer may need to access the device remotely for maintenance and other reasons. In this section, we discuss things related to these issues.

3.8.1 Device Management

In order to ensure continued smooth operation of the device, the manufacturer may need to maintain the device periodically or to troubleshoot the device remotely after a complaint has been raised by the end user. Maintenance of the device includes software upgrade of the washing machine, renewal of the client certificate of the washing machine, change of the domain name of the manufacturer server etc. There are industry standard protocols available for device management. One of the protocols widely used for device management is the CPE WAN Management Protocol (CWMP) specified in Technical Report-069 (TR-069) by the Broadband Forum[39]. This is an application layer protocol based on SOAP and HTTP and runs between a Customer Premises Endpoint (CPE) and a Automatic Configuration Server (ACS) used for remote management of the CPEs.

3.8.2 User Administration

When it comes to scalability of the user of machine, one requirement is that the machine should be possible to be shared between more than one users. This can be implemented easily in the following way. The end user or purchaser who

has the access to the machine can add new users for a washing machine that he has access to. When he adds a new user for the machine, he simply adds the phone number or e-mail address of the new user. The new user has to verify his phone number or email address. Then this new user can access the washing machines as the original user has used. The only different would be that the original user would be an administrative privileged access that this new user may not have until the original user grants that to him. Hence there will be an Access Control mechanism when it comes to multi-user machines. This is in order to avoid rogue users claiming the machine and changeing the administrative settings of the machine denying the access to the legitimate users of the machine.

-Page intentionally left blank-

4 Basis for Implementation

After all the discussions and analysis of the technologies from the state-of-the-art, we can now visualize how the solution would look like. Figure 12 provides a step-by-step procedure for the solution using Wi-Fi. However, there could be several scenarios based on which approach we would choose as will detailed in later part of this chapter. Nevertheless, for a Wi-Fi based approach functionally the architecture of the solution would look the like the schematic diagram in Figure 11 which would correspond to the procedures described step-by-step in Figure 12. Other approaches would differ only slightly when it comes to these two figures. These two figures are elaborated in the following sections. We end this chapter describing the possible scenarios.

4.1 Functional Architecture

For a Wi-Fi based approach, functionally the solution comprises of a few elements as depicted in Figure 11. This schematic diagram summarizes the components and different functional interfaces of the solution. Other approached would differ only slightly.

Functional elements for a Wi-Fi based approach are listed as follows:

- Wi-Fi enabled Smart Washing Machine
- Wi-Fi Access Point (AP) with Internet access
- Smartphone with Smart Washing Machine app or Computer browsing the manufacturer server portal
- Manufacturer Server

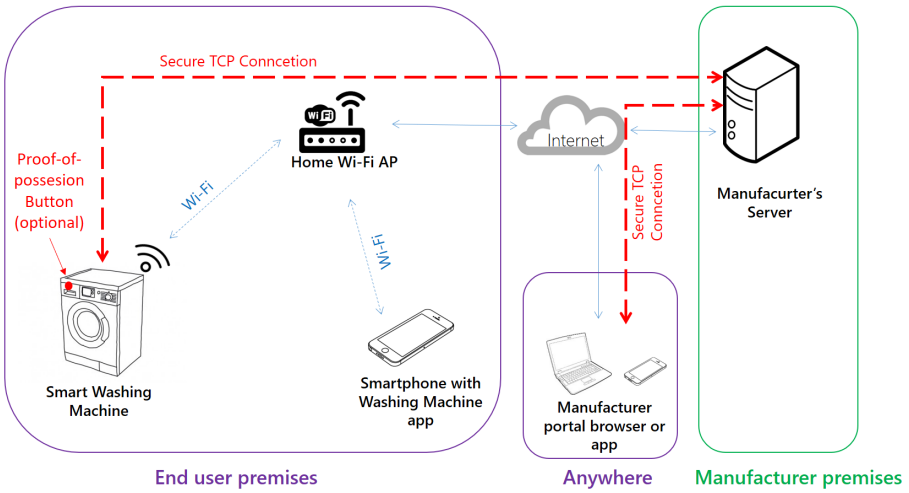

FIGURE 11. **Schematic diagram of the functional architecture of the solution in a Wi-Fi based approach**

The Smart Washing Machine connects to the Wi-Fi AP and gets access to the Manufacturer Server over the Internet. The smartphone with the Smart Washing Machine app connects to the Manufacturer Server over the Internet. Any computer which can access the Manufacturer Server web portal over the Internet using any standard browser could also be used instead of the smartphone app. The computer or the smartphone could be located anywhere in the world using any method of connecting to the Internet. They could also use the the same Wi-Fi AP which the washing machine uses.

4.2 Step-by-step Procedure

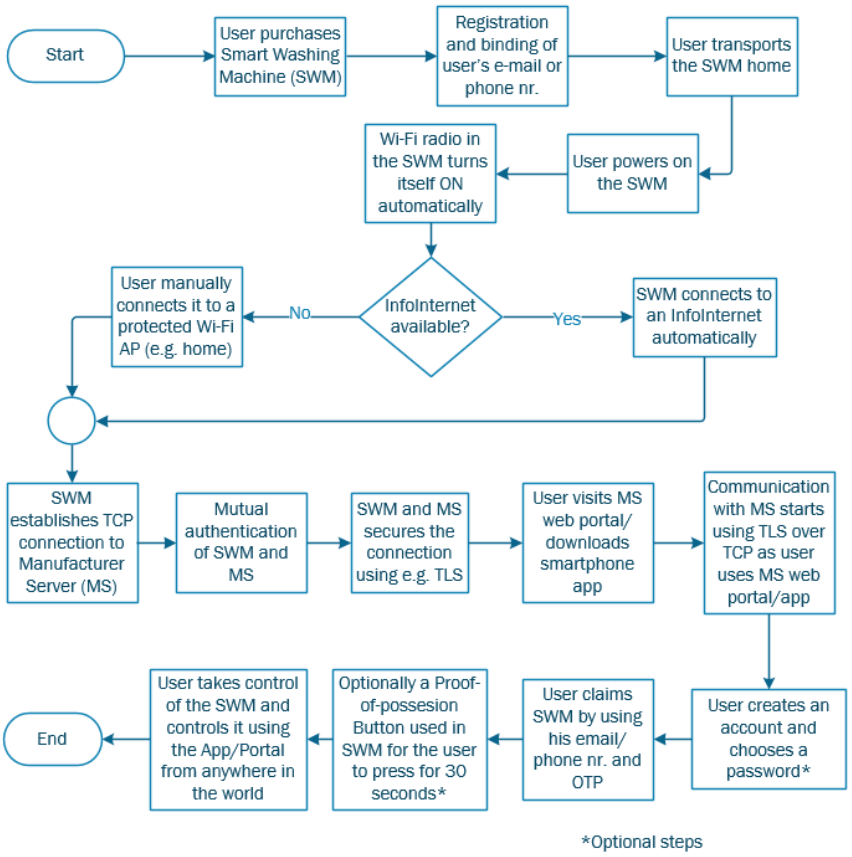

FIGURE 12. **Step-by-step procedure for the solution in a Wi-Fi approach**

As illustrated in Figure 12, for a Wi-Fi based approach the procedure starts when the user buys the Smart Washing Machine from a shop. During the purchase the purchaser or end user registers his e-mail address or phone number so that the manufacturer or the seller on behalf of the manufacturer binds the this information of the user with the Unique ID of the washing machine in the manufacturer database. After transporting the machine home, the end user powers it

on and the washing machine turns the Wi-Fi radio ON automatically and finds and connects to any available Wi-Fi based Information-Internet if available. If there is none, it finds all the Wi-Fi networks available. After the user inputs the Wi-Fi password, the Washing Machine connects to the Internet via the Wi-Fi AP and initiates a TCP connection with the Manufacturer server. Now the mutual authentication of the Smart Washing Machine and the Manufacturer Server happens over TLS or other protocols. After successful mutual authentication procedure a secure connection is established between the two elements. At this point the Smart Washing Machine is available for the legitimate end user to claim and control it via the Manufacturer Server.

The user in the meantime uses his smartphone with access to the Internet downloads the Smart Washing Machine app in his phone. He can also use a computer with an Internet browser to visit the manufacturer server web portal. In either case, whe the user starts using the app, he initiates a TLS handshake with the manufacturer server to create a secure TCP connection. Then optionally he creates an account in the manufacturer's portal/app. Now he starts the procedure of claiming the washing machine(s) in the portal/app associating it to his phone number or e-mail address after it is presented to him by the manufacturer server in the app or portal. The user must go through the user authentication procedure to prove that he is the legitimate user of the machine using the OTP sent to his e-mail or phone. Optionally to ensure the proof of possession of the washing machine he may have have to press the Proff-of-possession Button located in the Washing Machine for at least 30 seconds. With this step the claiming process of the washing machine is finished and 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 anywhere in the world.

4.3 Scenarios for Implementation

As mentioned before, there could be several approaches for the solution. Based on this approaches different scenarios can be identified. The solution would be slightly different is these scenarios. In this section, we describe the approaches based on the analysis of technologies in Chapter 3. One of the important factor for the solution is the choice of the wireless technology. Chapter 3 concluded that two of the wireless technologies are most suitable for the solution - Wi-Fi and Cellular. Additionally based on the availability of the InfoInternet the solution could be implemented in different ways. In the next sections we detail the scenarios.

4.3.1 Scenario 1: InfoInternet with Wi-Fi Connectivity

In this scenario, InfoInternet based on Wi-Fi is assumed to be ubiquitous in the area of usage. Since the Wi-Fi Access Point is open and not protected by any passphrase or other mechanisms, the washing machine would find it and connect to it immediately. This Wi-Fi could also be any Open Wi-Fi other that a declared InfoInternet. For the security of the interface between the washing machine and the manufacturer server, certificate based protocols TLS or IPsec

can be used. In this case the solution follows the functional diagram in Figure 11 and the flowchart in Figure 12.

4.3.2 Scenario 2: Protected Wi-Fi Connectivity

This scenario is expected to be the most commonly implemented one because of the high availability of the protected home Wi-Fi Access Points. In this case, it is assumed that the InfoInternet in not widely available and hence the solution has to rely on protected Wi-Fi access methods (WPA or WPA2) solutions. One of the drawbacks is that the solution requires manual input of the passphrase for the WPA to access the Wi-Fi. For the security of the interface between the washing machine and the manufacturer server, certificate based protocols TLS or IPsec can be used like scenario 1. In this case the solution follows the functional diagram in Figure 11 and the flowchart in Figure 12.

4.3.3 Scenario 3: Cellular Connectivity

This scenario is more suitable for the places where there is no availability of a Wi-Fi network. In these cases, it is more likely that a cellular network based solution would be more practical. However, one drawback is that an eSIM needs to be installed in the machine which would be accompanied by eSIM management. Moreover, the end user needs to purchase a monthly subscription from a cellular operator for using the network which is extra cost item for the end user. However, if a cellular InfoInternet is available, then the end user would bear any cost and this drawback would be removed. An alternative of this approach would be to use a protected Wi-Fi based Washing machine with the smartphone used as a Wi-Fi hotspot. This would remove some of the drawbacks of the cellular approach. Another option could be to use a cellular modem which converts the cellular network into a Wi-Fi LAN.

One of the benefits of this implementation scenario is that cellular is widely available almost all over the world. Another benefit would be that the user does not have to input any passphrase for access to the cellular network. For the security of the interface between the washing machine and the manufacturer server, certificate based protocols TLS or IPsec can be used like scenario 1 and 2. However, in this case the solution would differ slightly from the functional diagram in Figure 11 and the flowchart in Figure 12. Some of the main differences would be that the washing machine connects to a cellular AP instead of a Wi-Fi AP and washing machines turn on their cellular radios instead of Wi-Fi radios etc.

5 Security Analysis

Ensuring security of a system signifies the security risk management and involves identifying, assessing and responding to security risks. This includes vulnerability assessment, threat assessment and risk analysis. These activities should be repeated periodically 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.

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[23]. 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[25]. 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[26].

Now, all those frameworks mentioned above 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. It is also helpful for the manufacturing company's perspective to use one of these frameworks for IT Risk Analysis. For example, ISO 31000 standard provides principles, a framework and a process for risk management as shown in Figure 13.

The Chosen Framework In this paper, we will incorporate the process part from the *ISO 31000 and ISO 27000 frameworks* to identify security risks i. e. the threats and vulnerabilities of the proposed solution and then we will analyze and evaluate the risks associated with these threats and vulnerabilities in the next sections and lastly we discuss the treatment of the evaluated risks.

In Figure 13, the relationship between the principles, the framework and the risk management process has been depicted as specified in the ISO 31000 - Risk Management standard[23]. There are 11 principles that are needed to be considered to help make the risk management effective. The framework involves mandate and commitment and cycle of the following steps - framework design, implement risk management, monitor and review of the framework and continual improvement. The process of the risk management itself starts with the establishment of the context, risk identification, analysis and evaluation as to which risks are acceptable and which are not, and finally risk treatment. All

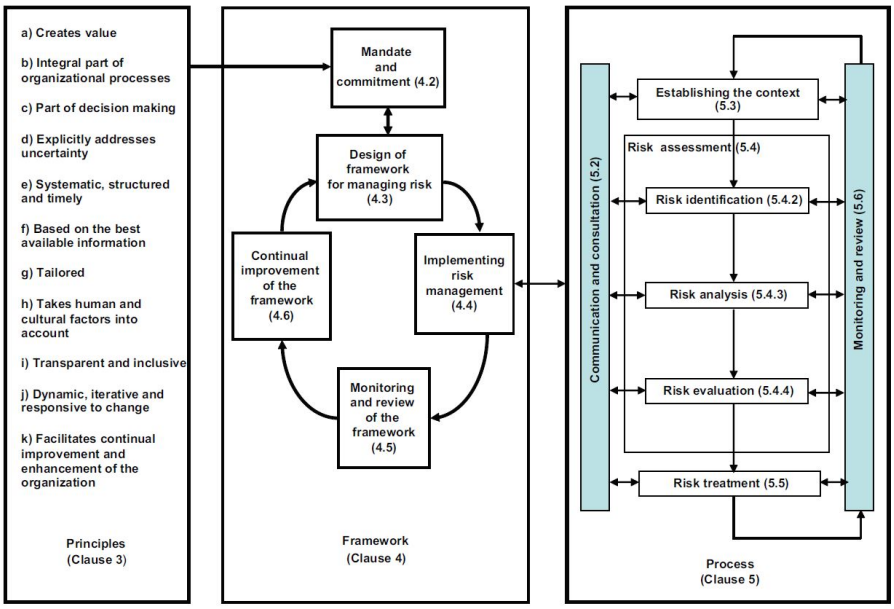

FIGURE 13. **Relationship between principles, framework and process as described in ISO 31000 - Risk Management[23]**

these steps are repeated with continuous communication and consultation with other steps. In the next setion we start applying this framework to our solution.

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 13. 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[23].

In our paper, the objective of the Risk Management is that the solution we propose meets the general security objectives including the confidentiality, integrity, availability, accountability, authentication, authorization and non-repudiation. The scope and criterion of managing the risk include how the risks will be classified and also the definition of the **risk appetite**, which means the level of risk that is acceptable or tolerable. Following section defines the these items.

5.2.1 Risk Evaluation Criteria

Risks are measured based on how likely it is that a vulnerability would be exploited after it has been exposed and how bad the consequence of this would be on the security objectives, more specifically, in terms of financial loss of the manufacturing company, for example in our case. In our analysis we have found that there could be three classes of likelihood and consequence. The definition

of these classes are described below.

Likelihood Classes According to ISO/Guide 73:2009[24], 'likelihood' is the 'chance of something happening', here 'something' could be an 'event' which means the 'occurrence or change of a particular set of circumstances'. Following this definition, in our security analysis, we customized its definition as to how easy it is to perform an attack exploiting a vulnerability. Our analysis shows three qualitative classes of significance for the likelihood of an 'event' happening and the definition is given in terms how long an attack takes to be implemented after a vulnerability has been exposed, described as follows.

- **High:** Fairly easy to materialize the attack. It is possible to implement such an attack *within 30 days* with brute force or after the vulnerability has been exposed.
- **Medium:** Quite difficult to materialize the attack. It is possible to implement such an attack *within 6 months* with brute force or after the vulnerability has been exposed.
- **Low:** Very difficult to materialize the attack. It takes *several years* to implement such an attack with brute force or after the vulnerability has been exposed.

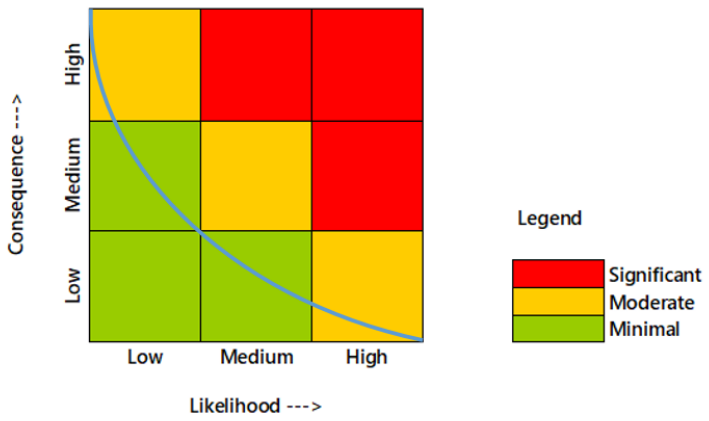

FIGURE 14. **Risk categorization matrix based on likelihood and consequence classes. The blue line is an example of the Risk Appetite curve for the manufacturer.**

Consequence Classes According to ISO/Guide 73:2009[24], 'consequence' is the 'outcome of an event affecting objectives'. Following this definition, in our security analysis, we customized its definition as to how severe the level of impact does the attack has in terms of the functionalities of the device and

the amount of financial loss and hamper of goodwill of the manufacturer. Our analysis shows three qualitative classes of significance for the likelihood of a risk and the definition is given as follows.

- **High:** High-consequence risks cause *catastrophic failures* in the machine's core functionalities making *a large number of the end users* lose control of their machines *at the same time*. Severe hamper in the good will of the manufacturing company raises it's *financial loss to a staggering amount*.
- **Medium:** Medium-consequence risks cause failures making *a few number of the end users* lose control of their machines. Some individual end users may be at great loss without having similar effect on the bigger end user base. The treatment may cost *significant financial cost* for the manufacturer.
- **Low:** Low-consequence risks cause *minor damage* to the devices' normal functionality *affecting very few end users* losing some functionality of their machines. Some individual users may incur some loss which can be *rectified with normal effort* from the manufacturing company.

Risk Categories Now that we have classified the likelihood and consequences, we can now define the risk categorization matrix based on those classes. A risk categorization matrix is provided in Figure 14 with an example of a risk appetite curve for the manufacturer. Risks below this curve are accepted by the manufacturer. In our analysis, we have categorized the risks in three categories described below.

- **Significant:** Risks mainly with higher classes of likelihood and consequence as shown in the risk categorization matrix. These risks must be treated immediately with the highest level of importance.
- **Moderate:** Risks mainly with medium classes of likelihood and consequence as shown in the risk categorization matrix. These risks needs treatment with secondary importance.
- **Minimal:** Risks mainly with low classes of likelihood and consequence as shown in the risk categorization matrix. These risks may be treated, however, most of them can be tolerated or accepted within **Risk Appetite** represented by the curve in Figure 14.

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 Available Security Features

Security has been one of the goals of the solution and it 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. During purchase the user must register his phone number or e-mail address with the manufacturer so that later when he tries to claim a machine, the server can implement 2-Factor Authentication - one is the phone number/e-mail address registered and the OTP sent be SMS or e-mail to that e-mail address/phone number.

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 optionally creates an account in the Manufacturer Server with a strong password before he tries to claim any washing machine. This will ensure that the user does not have to claim the claim machine every time he wants use it.

IV. The TCP connection of the washing machine with the portal is a secure 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.

V. The user establishes connection with the server using TLS over TCP with server certificate ensuring security of the connection.

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

5.3.2 Vulnerabilities and Threats

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:** An adversary gets hold of the phone/SIM or e-mail account of the end user and hence claims the machine and performs Denial-of-Service (DoS) attacks by removing the legitimate user from access control database. This could be because the phone/SIM was not protected or the e-mail account is not protected.

(b) **User account hacking:** An attacker cracks the account password resulting in compromise of the user account and the control of the machine because the password is too weak or the standard password management policy is not followed. In this case, the attacker can also run DoS attacks.

(c) **Client impersonation:** An adversary impersonates as client machine to the server because the client certificate is compromised. If this is successful, the attacker can damage the server or steal information from the server using the compromised certificate in a rogue washing machine.

(d) **Server compromise:** The manufacturer server is compromised and is used to exploit the open TCP Connection to do malicious activities because the security of the server is not strong enough.

(e) **Privacy breach:** A rogue user from the server side, for example a disgruntled employee, misuses the user's information and his habits resulting in a breach of client privacy. The communication between the machine and the user happens via the server which means the server has the user information e.g. e-mail address, phone number, address etc. and behavioral traits e.g. when the user normally is home etc. This information can be used by rogue personnels or sold to the appropriate parties by them.

(f) **Man-in-the-middle attack:** An adversary impersonates as the counterparts to both the machine and the server because the mutual authentication of the client, here the washing machine, and the server is circumvented.

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 addition the attacker can run brute-force attacks which the system is already secure against. In the next section, we analyze the risks associated with these threats.

5.4 Risk Analysis

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 consequence table of the threats identified in earlier.

5.5 Risk Evaluation and Treatment

From the initial risk analysis in the previous section, we find 6 risks and their categorization based on likelihood and consequence. In Figure 15 the initially assessed risks are presented in the risk matrix. Now in Section 5.2.1, we have defined that the risk below the risk appetite curve are accepted by the manufacturer. Hence risks (b) and (e) are within acceptable limit and need no treatment. However, they should be monitored and if possible, treated. Other risks need treatment.

There is no risk that is in the significant category. This risks need immediate treatment. However, four of the risks are in the moderate category - risk id (a), (c), (d) and (f). The treatment of these risks are described in Figure 3. The treatments described here reduces the likelihood of the risk. After they are treated, the risk move within the risk appetite curve of the manufacturer as shown in Figure 16. It is advisable to the manufacturers that they should analyze the risks in a more detailed manner and treat the consequences also in addition to the likelihoods.

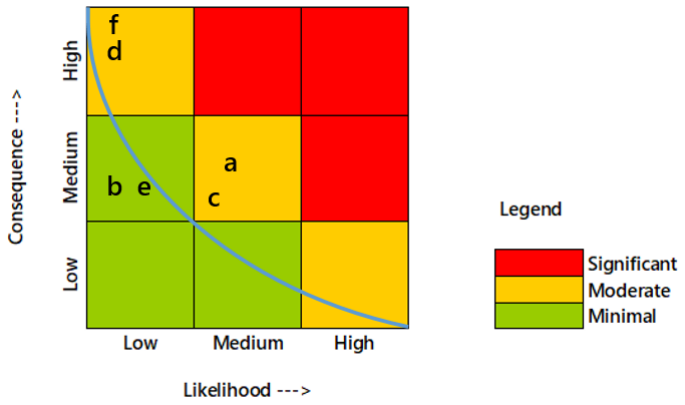

FIGURE 15. **Initial assessment of the risks shown in the risk matrix**

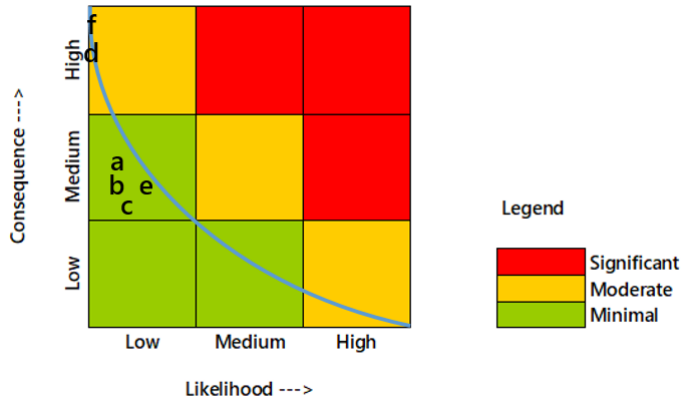

FIGURE 16. **Assessment of residual risks after the risks lying over the risk appetite curve are treated**

TABLE 3. **Risk analysis of the known threats**

Risk Id	Risk Name	Risk Statement	Likelihood	Consequence	Risk Rating	Treatment
(a)	Rogue claim	An adversary gets hold of the phone/SIM or e-mail account of the end user and hence claims the machine and performs DoS attacks by removing the legitimate user from access control database.	Medium	Medium	Moderate	User must secure his phone/SIM using password/PIN and maintain his e-mail account in order to avoid hacking.
(b)	User account hacking	An attacker cracks the account password resulting in compromise of the user account and the control of the machine because the password is too weak or the standard password management policy is not followed.	Low	Medium	Minimal	Enforce strong password management policy for user accounts.
(c)	Client impersonation	An adversary impersonates as client machine to the server because the client certificate is compromised.	Medium	Medium	Moderate	Enforce CertificateVerify from the client machine during TLS handshake. Revoke the old client certificates and issue new ones periodically.
(d)	Server compromise	The manufacturer server is compromised and is used to exploit the open TCP Connection to do malicious activites because the security of the server is not strong enough.	Low	High	Moderate	Enhance the security of the manufacturer server.
(e)	Privacy breach	A rogue user from the server side misuses the client's information and his habits resulting in a breach of client privacy.	Low	Medium	Minimal	Proper access control mechanism and industry code of conduct must be followed in the manufacturer organization.
(f)	Man-in-the-middle attack	An adversary impersonates as the counterparts to both the machine and the server because the mutual authentication of the client and the server is circumvented.	Low	High	Moderate	Client certificates must be verfied againt an updated CRL or using OCSP. Implement device magt. portocols like TR-069.

6 Evaluation

In this paper we have analyzed the technologies in terms of their applicability in the proposed solutions in different scenarios for implementation. The final task is to evaluate the solutions of different scenarios against the required evaluation criteria specified in section 2.2. Our evaluation will also take into account the state-of-art solutions available for the current topic in the industry. Table 5 summarizes the evaluation results on different criteria of requirements. The legends of the symbols used in the table are provided Table 4.

As described in detail in section 4.3, our analysis shows that there are three scenarios for implementation - InfoInternet with Wi-Fi, Protected Wi-Fi and Cellular Connectivity. We evaluate these three scenarios and in addition the today's best available implementation for every requirements in the next sections. The evaluation is the based on the best understanding of the solutions and not highly objective to the criteria mentioned.

6.1 Convenience

Today's smart washing machines needs many things in order to be more convenient. Many of their processes still require manual intervention. In our solution, manual interventions are minimized greatly. Some challenges still remains in automatic connectivity to protected Wi-Fi networks, at least for the first time connection. The passphrase needs to be typed in which is a manual work. Mechanisms used by some vendors to use the smartphone to circumvent this has security holes and an issue of inconvenience for th end user. The implementation scenarios can easily be implemented by the industry since the ecosystem is already available. One challenge for the Scenario 1 is that the InfoInternet or Open Wi-Fi is not widely available in the ecosystem yet making this scenario impractical still.

The level of automation is more favorable in our proposals that currently available solutions, especially in Scenario 1 because of the use of InfoInternet. The processes built in the solutions are quite flexible than today's available solutions. For example, it would be very easy to update the client certificate of the machine remotely. However, Scenario 2 provides more flexibility than others for example, if Wi-Fi is not available in place, a smartphone can easily be turned into a Wi-Fi hotspot and the washing machine can connect to the Internet through it. The last criteria we discuss on convenience is that in our solutions the washing machines are operable via the Internet from anywhere in the world which is not widely available in the industry yet.

6.2 Cost Efficiency

Cost is one of the main drivers for automation in the world. One the major drivers for automation in the processes in the industry is to reduce the human resource cost. However, in case of home appliances, the cost is a significant factor both for the manufacturers and the consumers. In our solution, we have not introduced any costly hardware or software which minimizes the cost which some

of the today's available washing machines failed to do. For example, many of the protocols used by the manufacturers are proprietary and undisclosed which makes the machines costly by nature. CPU and electronic memory usage also increases overall cost of the machine. In our solutions, since the level of automation is very high, CPU and memory usage naturally increases than most of the today's available solutions. However, Scenario 3 still has a benefit over the other scenarios since it uses cellular network which is designed to use less resources in the machine.

Lastly, we think customers will be less willing to purchase a solution that introduces recurring costs, for example, monthly costs paid to someone. This would be most likely for Scenario 3 since the consumer has to buy an extra subscription or service from the cellular operator to run his machine with cellular network. However, if an InfoInternet is available with cellular then this cost is removed. Wi-Fi may incur some recurring cost depending on the infrastructure used for Wi-Fi AP.

6.3 Security

Since in IoT, the devices always are connected to the Internet, the security is of utmost importance in the solutions based on IoT. In our solution the washing machines are always connected to the Internet in order to facilitate the integration and control of the machine from anywhere in the world. The security of the solution has extensively done in chapter 5. However, here we evaluate and compare the security feature of the three scenarios and the today's available solution. Firstly, our solution provide very high level of security and automation in the device authentication and user authentication which is not available in the industry as far as we have seen. Security features such as confidentiality and integrity protection are covered by proven highest standard protocols based on server and client certificates. This features are almost absent in today's solutions.

However, because the solutions we proposed are based on the trust of the manufacturer in the actual day-to-day operation of the machine, the risk of privacy breach, for example, giving out personal information of an end user, due to, for example, a disgruntled or rogue employee of the manufacturer, is there. However, this is very unlikely to happen and most likely not affect the operation seriously. In case of today's solutions, there is also a risk like this since the manufacturer has access to the usage history of the user. Another thing to consider is the service availability. The security mechanism in our proposed solutions are high enough and it is very unlikely for denial-of-service attack to succeed.

TABLE 4. **Symbol legends for the table of evaluation in table 5**

$\times$	Not applicable
$++$	More favorable
$+$	Favorable
$-$	Less favorable
$--$	Lesser favorable

TABLE 5. **Evaluation of proposed solutions in different scenarios against the today's available washing machines (symbol legends are given in table 4)**

	Evaluation Criteria for the Requirements	**Today**	**Scenario 1: InfoInternet with Wi-Fi**	**Scenario 2: Protected Wi-Fi**	**Scenario 3: Cellular**
Convenience	Level of manual jobb during integration	−−	++	+	++
	Automation in authentication	×	++	++	++
	Easily practicable in today's art	+	+	++	++
	Degree of automation	−	++	+	++
	Flexibility of the processes	−−	+	++	+
	Operate from anywhere over the Internet	−	++	++	++
Cost Efficiency	Costly hardware usage	+	++	++	+
	Extra recurring cost	+	++	+	−−
	CPU and memory usage	++	+	+	++
	Usage of undisclosed proprietary protocols	−	++	++	++
Security	Device authentication	×	++	++	++
	User authentication	×	++	++	++
	Confidentiality	×	++	++	++
	Integrity protection	×	++	++	++
	Risk of privacy breach	++	+	+	+
	Service availability	×	++	++	++
Scalability	Authentication mechanism scalability	×	++	++	++
	Device management and administration	−	++	++	++
	Applicability in newer challenging scenarios	−	−	++	++
	System scalability with number of devices and users	++	+	++	++
	Scalability with high number of users of a single machine	−	++	++	++

However, for today's solutions this does not apply since they are mostly based on local area network.

6.4 Scalability

The scalability of the solutions become a significant factor when the solution sees success and growth in the usage. As more and more customers are willing to purchase the machine, the service functionality and quality must not deteriorate and rather must be maintained at the similar high level. The features designed in the proposed solutions need to be scalable. We evaluate several important criteria for scalability here. The authentication mechanism involves quite a few infrastructure from the manufacturer side. The protocols and procedures involved are scalable with the customer growth. This does not apply for today's solutions since they are assumed not to be using device or user authentication on a similar level.

For the management of the device, sophisticated mechanisms based on TR-069 are used in our solution which is highly scalable. Today's solutions are not known to utilize device management on this level and hence supposed to face scalability issues. Another criteria is the solutions' capability of being applicable to newer and more challenging user scenarios. Scenario 2 and 3 are quite favorable on this criteria. However, current solutions and scenario 1 have limitations on this criteria. Lastly, the proposed solution is designed to be highly scalable if the number of users increase on a single machine. The user administration is controlled based on proven Access Control mechanisms available in the art. Today's solutions are also quite scalable on this, however they lack the access control mechanisms in most cases.

6.5 Our Judgment

Based on the discussions above, we think the proposed solutions provide a high level automation when it comes to integration and operation of the washing machine compared to the today's best available solutions in the industry. The choice of the solution would depend on the situation which prevails around the usage of the device. However, we think in general **Scenario 2: Protected Wi-Fi Connectivity** is the most practical solution fulfilling the requirements to the most. Even though this is not based on InfoInternet, it is well suited to most of the situations. The detailed arguments for this is, we think, quite evident in the evaluation table and the description above. We also think that other scenarios could also be best for situations best applicable to them.

7 Conclusion

The goal of this thesis was to propose a new way of integrating energy devices in a convenient, cost efficient, secure and scalable way based on the critical analysis of the state-of-the-art technologies and practicable user scenarios. To fulfill that target, we have introduced the method of engineering design and in order follow this method, we have dissected the problem into different layers and treated them separately. We have introduced different technologies which can be used to solve the problems in each layer. Some of these layers have been the capability of the energy devices for example washing machines, wireless technologies to be used for the communication with the energy devices, the mutual authentication of the devices with the server, the communication mechanism among the different integral components of the ecosystem, the user authentication mechanisms, device management and user administration procedures.

One of the core goals of this thesis was to introduce InfoInternet as the facilitator of this new integration process. The arguments for this are clear. InfoInternet is open for everyone and freely available to access basic information from the Internet. It is the preferable medium of communication for the premise of our thesis since it gives many flexibilities. However, since this is not available ubiquitously, the solution needs to be open for alternative communication mediums also. At this we open ourselves to the vast openness of the IoT wireless technologies. We discussed almost all the available wireless technologies relevant for the IoT solutions and evaluated them to find a few more suitable options for our solutions. In this way the solution is able to cover other practical scenarios also.

One of the main goals and challenges of this thesis was security of the solution. Security of the solution encompasses the mutual authentication mechanism of the device and the server since client-server model of communication was found to be the most appropriate way of communication for the current problem. The topics for security are the user authentication mechanisms and the confidentiality, integrity and availability of the communication among the server, device and the user. We have introduced different possibilities and chosen digital certificate based mutual authentication of the device and the server due to its reliability and convenience. For the user authentication we proposed to use a 2-Factor Authentication mechanism in the application layer on top of a TLS based secure transport layer communication. We discussed about the optional use of a proof of possession mechanism using a physical button in the machine to avoid some rouge activities. Later part of the analysis discussed about the device management mechanisms for example for the management of the software updates, remote troubleshooting and certificate management. We proposed to use industry standard TR-069 for this for highly scalable and industry-wide use.

Before evaluation of the solutions, this thesis also analyzes the security aspects and risks associated with it extensively and provides treatments for the significant risks. Well-practiced risk analysis frameworks are used to perform the security analysis. This kind of analysis would help the manufacturers to find the security holes in the solution when they start to implement similar solutions in real life. This also gives the research community the basis for critical analysis

which can drive the further development of the solutions.

The proposals coming out of this thesis are based on different scenarios for implementation. We picked up three most relevant scenarios and evaluated them against today's best available similar solutions. This evaluation was performed based on the criteria of convenience, cost efficiency, security and scalability. Our analysis shows that in general the most practical solution would be to implement the solution using protected Wi-Fi connectivity. This scenario is evaluated to fulfill the requirements to the most. In this solution, the washing machine uses protected Wi-Fi as wireless medium, connects to the Internet, performs a certificate-based mutual authentication with the server and make itself available for claim by the legitimate user. The user connects to the server, does a 2-Factor Authentication with the server to prove his identity to claim the washing machine. Both the communication legs are secured using cryptographic keys generated after certificate-based authentication mechanisms like TLS or IPsec and communicate over reliable protocols like TCP. This solution is analyzed to be the most optimum solution in terms of all requirements.

However, other implementation scenarios are also proposed if other situations become more practical. For example, if Wi-Fi based InfoInternet becomes widely available, then another scenario will become more appropriate or if Wi-Fi not being available in an area becomes a considerable concern, cellular network scenario can be implemented instead. Hence, we believe that this thesis provides a well-analyzed guidance for the manufacturers to invest their energy to build a solution like the ones proposed.

When it comes to future works on this, there are several things which can be covered in future works. For example, the machine-to.machine communications in different higher level user scenarios encompassing practical everyday situations is not covered in this thesis. Other subjects to work on could be the ways to build useful if-this-then-that applications on top of the platform provided in this thesis and to remove the dependency on the device-specific smartphone apps in order to create a larger IoT ecosystem for smart homes where users don't have to install different applications for different appliances used in the same house.

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] N. Dhanjani, *Chapter 1. Lights Out—Hacking Wireless Lightbulbs to Cause Sustained Blackouts*, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, O'Reilly Media, Inc., Aug 13, 2015, ISBN:978-1-491-90233-2

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

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

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

[7] 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

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

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

[10] 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

[11] 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.

[12] IEEE 802 LAN/MAN Standards Committee. http://www.ieee802.org/

[13] Third Generation Partnership Project (3GPP). http://www.3gpp.org/

[14] 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

[15] 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

[16] M. Weyn, *Overview of Low Power Wide Area Networks*, IoT Belgium, September 17, 2015, https://www.slideshare.net/MaartenWeyn1/overview-of-low-power-wide-area-networks

[17] Postscapes, *IoT Standards and Protocols*, August 20, 2018, https://www.postscapes.com/internet-of-things-protocols/

[18] 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.

[19] 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.

[20] 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

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

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

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

[24] ISO, *ISO/Guide 73:2009(en) Risk management — Vocabulary*, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

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

[26] 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

[27] V. Karagiannis et. al., *A Survey on Application Layer Protocols for the Internet of Things*, Transaction on IoT and Cloud Computing, 2015, Pages 1454-1464, ISSN: 2331-4753 (Print), 2331-4761 (Online)

[28] V. Gazis et al., *A survey of technologies for the internet of things*, International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, 2015, pp. 1090-1095. doi:10.1109/IWCMC.2015.7289234

[29] M. R. Palattella et al., *Standardized Protocol Stack for the Internet of (Important) Things*, IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389-1406, Third Quarter 2013. doi:10.1109/SURV.2012.111412.00158

[30] P. Srisuresh, M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, RFC 2663, August 1999. http://www.ietf.org/rfc/rfc2663.txt

[31] S. Loreto, P. Saint-Andre, S. Salsano, and G. Wilkins, *Known Issues and Best Practices for the Use of Long Polling and Streaming in Bidirectional HTTP*, RFC 6202, April 2011. http://www.ietf.org/rfc/rfc6202.txt

[32] R. Fielding, Ed., and J. Reschke, Ed., *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*, RFC 7230, June 2014. http://www.ietf.org/rfc/rfc7230.txt

[33] International Organization of Standards (ISO), *ISO/IEC 20922:2016, Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1*, June 2016. https://www.iso.org/standard/69466.html

[34] Wikipedia, *Challenge-Response Authentication*, https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication

[35] W. Stallings, *Network Security Essentials: Applications and Standards (6th Edition)*, Pearson Education, Inc, 2016, ISBN-13:978-0134527338

[36] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, August 2008. http://www.ietf.org/rfc/rfc5246.txt

[37] M. L. Das, N. Samdaria, *On the security of SSL/TLS-enabled applications*, Applied Computing and Informatics, Volume 10, Issues 1–2, 2014, Pages 68-81, ISSN 2210-8327, https://doi.org/10.1016/j.aci.2014.02.001

[38] XMPP, https://xmpp.org/about/technology-overview.html

[39] TR-069 CPE WAN Management Protocol (CWMP Version 1.4), Issue 1, Amendment 6, March 2018, https://www.broadband-forum.org/technical/download/TR-069_Amendment-6.pdf