Privacy in Smart Homes

Using Privacy Impact Assessment to Inspect Privacy Issues in a Smart Home

Mahmoud Azimeh & Håvard Friborg

SUPERVISORS

Vladimir Oleshchuk & Harsha Sandaruwan Gardiyawasam Pussewalage

University of Agder, 2022

Faculty of Engineering and Science

Department of Engineering and Sciences

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2). Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

This thesis is written as the final part of a two-year Master of Cyber Security program from the Faculty of Engineering and Science, University of Agder, Grimstad. This report is the delivery of IKT523-G Master's Thesis, Cyber Security.

We wish to express our gratitude to our advisors, Professor Vladimir Oleshchuk and Associate Professor Harsha Sandaruwan Gardiyawasam Pussewalage, for their guidance through this last section of our education.

We also want to send a "Thank You" to our families for their unwavering support.

Abstract

IoT has an ever-increasing amount of development as more and more different devices connect to the Internet and become IoT devices. For the regular private user, the smart home may be the most enticing domain of IoT as it can be used to ease their lives. Smart home and smart home devices are one of the subfields of the Internet of Things. They allow the inhabitants to control various home devices remotely from anywhere within the house or anywhere in the world at any particular time. Smart homes have several benefits. They are improving the quality of individuals' lives, as individuals can control their various smart devices at any time. In addition, a smart home allows individuals to have greater control of their energy use. Other pros of smart homes include complete control over devices, increased convenience, and insurance benefits. However, regardless of the many benefits of smart homes, they are also associated with various challenges. Security and privacy are significant challenges related to the smart home environment.

This thesis will discuss the privacy impact of smart homes and smart devices. Four different devices have been included, and each device will be analyzed to conclude what private sensitive information they collect. Moreover, a privacy impact assessment (PIA) tool will be used to conclude whether our manual analysis of the devices was correct or not. Lastly, we will propose some solutions that we consider will increase the protection of users' privacy.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Smart home and smart home devices are a subfield of the Internet of Things (IoT), which provides the inhabitants the ability to control kitchen appliances, home security systems, Heating, Ventilation, etc., remotely from anywhere in the house or anywhere in the world at any time. An ecosystem is being formed known as a smart home ecosystem when all these smart home devices are connected together [50]. The benefit of this smart home ecosystem is that it increases the security, safety, health, fitness, and overall quality of life of the users.

The idea of IoT was first introduced at the Massachusetts Institute of Technology by Kevin Ashton while he was working on the Auto-ID [27]. The concept of IoT includes connecting different devices, vehicles, home appliances, and buildings with the internet. The goal of connecting these devices to the internet is to augment, sense, identify and process the data. All these smart devices communicate with each other, make a small network or chain of devices, and exchange data. After getting data from all devices in the home, the central device sends the data to a cloud server over the internet[50].

Unfortunately, the concept's widespread acceptance has resulted in huge security risks, jeopardizing the privacy and security of all IoT components and segments. Aside from the need to provide the finest and most dependable services, designers have encountered considerable hurdles, security being at the top of the list. The security element of IoT has not been effectively addressed, necessitating an in-depth investigation of all security and privacy concerns in IoT[28].

This project will discuss the privacy impact of smart homes, smart devices, and smart appliances. First, we will discuss the origin of the smart home in detail and what roles residents play in smart home systems. Furthermore, we will also discuss the privacy structure of the smart home system. Next, we will discuss the smart home architecture in detail and discuss the privacy structure of smart appliances such as smart fridges, smart thermostats, smart meters, and smart hubs.

1.1 Motivation

More and more people are introducing smart appliances into their lives and making their homes into smart homes. However, in an ecosystem where so much personal information is gathered, it is essential that the list of information gathered and generated is known to the user and continually striving for further steps to improve privacy. We hope this report will help spotlight the privacy of smart home users and potential avenues for future use.

1.2 Case Description

This thesis aims to inspect the privacy level of smart homes and find possible avenues to increase the privacy levels. Furthermore, we will use processes and tools to find the necessary personal information needed for a smart house to function. Second, we will find innovations in technologies that can be integrated into the smart home system to improve users' privacy.

We decided upon three questions that would be our research questions:

1. What types of personal information are generated and exchanged in the environment?
2. How can we do a privacy impact assessment on a smart home environment?
3. How we can provide better privacy guarantees for end-users in a smart home environment?

1.3 Scope and Limitations

The decision was made to focus specifically on privacy in smart homes. This means that security issues were considered relevant only if they would affect the user's privacy.

Business aspects of the smart homes were considered out of scope as that is outside of our expertise and would need more assumptions that could lead the assignment astray.

As we conducted a PIA and DPIA, there were questions related to the legalities of the smart home. In these cases, only GDPR was considered as the authors are stationed in Norway, where GDPR is the governing law.

We set some limitations on how we would conduct the assignment from the beginning.

There would be no payments for any software, articles, or other aids or tools. Therefore, we were limited to aids that were free or had a free trial. Articles were accessed using our position as students at UiA.

We decided to make our own smart home architecture. This included choosing a set amount of smart appliances in the smart home. These appliances then had their functionalities defined by us. This led to the limitation of not being able to use a functioning smart home and not using smart appliances that are available to buy.

1.4 Research Methodology

After setting a research goal, we set a path towards the answer. The goals are to identify personal information collected in the smart home system, perform a Privacy Impact Assessment and find methods that can increase users' privacy. Since we will analyze the privacy impact of smart homes with existing methodologies, the research will be considered a case study.

We will start by researching smart homes and smart appliances, finding definitions and specifications, and choosing what we find relevant. Then a smart house architecture will be created with a set amount of smart appliances. We use the smart home architecture to perform a Privacy Impact Assessment to find Personal Information and its states in the system.

After the Personal Information is found, we will research possible methods to increase users' privacy in smart homes. The possible methods will be presented with their solutions and downsides. Furthermore, they will be discussed how they could work together.

1.5 Thesis Structure

The report is divided into seven chapters.

Chapter 2 describes the theory about smart houses and smart appliances. We collected definitions and combined them with those that best fit this assignment.

Chapter 3 contains the smart house architecture created by us with the chosen smart appliances. The smart house architecture also includes the Data Flow Diagram.

Chapter 4 is the Privacy Impact Assessment and DPIA.

Chapter 5 discusses potential technologies being developed or theorized that could help increase privacy in a smart home.

Chapter 6 discusses the results found from the PIA and methods for increasing privacy. Future work and challenges faced are also included.

Chapter 7 ends the report with the conclusion.

Chapter 2

Theory on Smart Homes and Privacy

This chapter discusses the definitions of *smart home* and *privacy.* We take several different definitions and combine the parts that we find relevant for this report. The definition of a smart home is especially diverse. Additionally, a brief theory and background will be included to provide readers with a better understanding of the concepts.

2.1 Smart Home

Like many topics in tech, Smart Home has no standard definition used by everyone. Therefore we have gathered several definitions we think are relevant and work when looking at privacy in smart homes. The list is in no specific order.

Table 2.1: Smart Home definitions.

Smart home definitions	
Definition	Source
In 2003 the UK Department of Trade and Industry (DTI) came up with the following definition for a smart home: "A dwelling incorporating a communications network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed."	"What is a smart home by" smarthomeenergy.co.uk[55]
A smart home is a residence equipped with smart technologies aimed at providing tailored services for users. Smart technologies make it possible to monitor, control and support residents, which can enhance the quality life and promote independent living. To facilitate the implementation and adoption of smart home technology it is important to examine the user's perspective and the current state of smart homes.	"A Systematic Review of the Smart Home Literature: A user perspective" by Davit Marikyan, Savvas Papagiannidis and Eleftherios Alamanos[38]
A residence equipped with computing and information technology that anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond.	"Smart Homes: Past, Present and Future" by Frances K. Aldrich[4]

A smart home refers to a convenient home setup where appliances and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device. Devices in a smart home are interconnected through the internet, allowing the user to control functions such as security access to the home, temperature, lighting, and a home theater remotely. Smart home appliances come with self-learning skills so they can learn the homeowner's schedules and make adjustments as needed. Smart homes enabled with lighting control allow homeowners to reduce electricity use and benefit from energy-related cost savings. Some home automation systems alert the homeowner if any motion is detected in the home when they're away, while others can call the authorities—police or the fire department—in case of imminent situations.	"What Is a Smart Home?" by Adam Hayes[2]
"Smart home" denotes the use of technical systems, automated processes and connected, remote-controlled devices in apartments and houses. The main objective of the functions is to improve the quality of life and convenience in the home. Other goals are greater security and more efficient use of energy thanks to connected, remote-controllable devices	"Smart Home: Everything you need to know" on infineon.com [31]

Smart-home environments have evolved to the point where everyday objects and devices at home can be networked to give the inhabitants new means of controlling them. The smart home adjusts its functions to the inhabitants' needs in accordance with the information it collects from the inhabitants, the computational system, and the context.	"Evolution towards smart home environments: Empirical evaluation of three user interfaces" by Kaisa Väänänen and Tiiu Koskela [60]
Smart Homes, also known as automated homes, intelligent buildings, integrated home systems or domotics, are a recent design development. Smart homes incorporate common devices that control features of the home. Originally, smart home technology was used to control environmental systems such as lighting and heating, but recently the use of smart technology has developed so that almost any electrical component within the house can be included in the system. Moreover, smart home technology does not simply turn devices on and off, it can monitor the internal environment and the activities that are being undertaken whilst the house is occupied. The result of these modifications to the technology is that a smart home can now monitor the activities of the occupant of a home, independently operate devices in set predefined patterns or independently, as the user requires.	"The Smart Home Concept : our immediate future" by Ricquebourg, Vincent [48]

The themes that come up in most of the definitions are

- Increased life quality (Comfort, entertainment, convenience, security, independence and more)
- Remote access to control the devices and information.
- Adjust automatically based on information gathered and context.
- Connected to the internet
- Devices communicates between each other.
- Managing all connected devices from one place.

Our own definition would be:
A Smart Home is a residence equipped with devices made to increase the quality of life of its residents. The devices are connected to the internet and can be controlled by users through voice, smartphones, computers, or the data it collects to adjust its functions according to the needs of the residents.

2.1.1 Smart Home's Origin

The X10 protocol was developed in 1975 in Scotland [61]. The development of the X10 protocol paved the way for modern home automation technology. It sends radio frequency (RF) which allows users to control their home appliances using their existing electrical wiring [56]. However, due to the radio-band noise of the electrical wiring, the signals sent through the X10 protocol were not always entirely reliable. In some cases, signals would fail to cross circuits that were connected to different polarities [54].

In 2005 a new technology was introduced that combined the wireless signals of the X10 protocol with the electric signals. Z-wave and Zigbee, and other protocols have appeared to mitigate the radio-band noise problem [54].

Since then, smart home technology has played a significant role in our lives. Today, various types of smart home devices are available in the market. Some are created by major technology brands like Google, Amazon, and Samsung. Examples of smart home devices are:

- **Smart locks**: differ in how they are smart. Some may use passwords, RFID keys, biometric data, or even facial recognition to unlock the doors. If connected to a smart hub or a central system, this information is sent. The data is often sent using Bluetooth. [49] Other data that may be stored in the system are names, user permissions, and timestamps. Together, this data can be used to set a profile of when a user arrives and leaves and what rooms they may have access to.
- **Smart TVs**: can collect viewing watching habits like TV shows watched as well as advertisements[33]. Smart TVs may also allow a user to browse the Internet, which brings all the sending of data that follows.[3] Some smart TVs may have a voice-activated control integrated as well. Se Voice-activated control for more details.
- **Smart security cameras**: can be used to protect a users home, the camera themselves film what they can see, but they also often have sensors that can detect any motion and the security system can send automatic messages to the user about there being motion detected when not expected any[37]. So a smart security system would have a constant stream of video along with alerts on movements in the guarded area.
- **Light bulbs**: can be connected to the user's mobile phone or the smart hub. The smart bulbs cannot record users' data directly. The smart lights bulbs could store data about how users use the lights. If the smart bulbs are connected via the smart hub, and threat actors grant access to the hub by hacking it, then they will be able to collect some information about how users use their lights [19].
- **Voice activated controls**: depends on users' voice in order to complete their tasks like placing calls, reading newspapers, playing music, and checking

the weather. The voice-activated control, or more precisely, voice assistant, is always listening, and its microphone is always on since the users' voice activates them. However, despite the devices' ability to record and transmit information, they are still very new and prone to security issues. Moreover, the companies use humans in order to review the recorded commands, which leads to privacy violations [11].

Additionally, the companies does not only collect and analyze recorded voice in the smart home. The voice assistants are able to collect other personal information from other IoT devices as long as the user grant access [11].

2.1.2 Smart Home Resident Roles

A study conducted by Huang and Mennicken [40] aims to analyze the various effects of smart home technologies on the residents and seeks to understand how smart home technologies are integrated. It also explores the factors that influence the design and implementation of smart homes. The study revealed that the main motivations behind home automation were related to the different roles of the homeowners and the technological capabilities of the devices. In addition, the study identifies individuals people who have a solid technical background and have a degree in a technical field as home technology drivers. They are described as individuals who can plan and install the home automation system and are responsible for operationalization once it is in place. At the same time, individuals with no technical backgrounds assumed the primary responsibility for their home technology. Those individuals are described as motivated by their desire to have the technology installed and maintained. As a result, they typically took the lead in making the repairs and adjustments needed.

2.2 Privacy

Privacy has many definitions as well, however the definitions vary less than for developing technologies like smart homes.

We like the definitions used by privacyinternational.org:
“Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information. ” [46]

As well as the definition used by the European Union in their GDPR laws:
“Data privacy means empowering your users to make their own decisions about who can process their data and for what purpose.” [24]

We believe that they contain the essence of what privacy is and needs. Privacy is when confidential information is protected against unauthorized access and the user is the one who chooses whom to give access to what information about them. These parts are important in a smart home as there may be an incredible amount of information gathered about the users. A user of a smart home should be able to choose what information the smart house may gather on said user. The user should also be able to choose who may obtain access to that information and what that information is used for.

2.2.1 Privacy Impact Assessment

Privacy impact assessment (PIA) is a process that was established to help organizations identify and manage the privacy risks that occur from new projects. This process can also help them develop strategies and procedures to minimize the impact of new projects and procedures. Additionally, it can benefit various stakeholder groups, such as the customers and the organization itself. In the US and Europe, policies have been established to standardize the process; namely, PIA [53].

The objective of a PIA is to review the various processes and procedures of an organization that are used to collect or manage the personal data of its customers. The review is carried out to identify areas of concern and how these practices might compromise or affect the privacy of the individuals the organization holds and collects their data. The goal of a PIA is to ensure that organization's policies and procedures comply with the applicable laws and regulations. It also aims to identify and manage the risks associated with the use and collection of personal data [53].

A privacy impact report is usually conducted to identify the various components of a proposed system that would collect and manage the personal information of its customers. It also aims to establish how the system can be managed. It can also go beyond an assessment of a system and consider the impact of the proposal on the individuals who are affected by it [53].

2.2.2 Privacy Threats In Smart Homes

A threat can be defined as an event or situation resulting in an unwanted outcome for a specific resource or entity. In the IoT, privacy threats are typically triggered by the various phases of the data lifecycle [6].

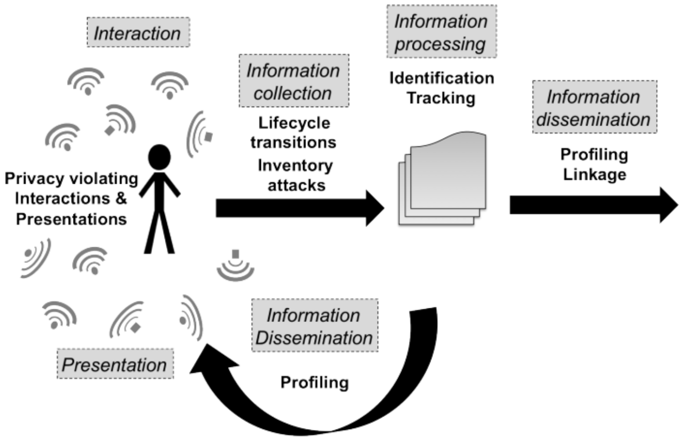


Figure 2.1: Threats in the IoT [6]

Due to the increasing number of features and technologies being used in the Internet of Things, various privacy threats are being identified. This section aims to provide a comprehensive overview of these threats. Figure 2.1 shows that the privacy threat phases are arranged into five different steps according to where they are most likely to appear [6].

1. **Identification:** The term identification refers to the threat of linking a person's name and address with data about them. This can be done by using various data sources or attaching a specific name or address to a particular context. This can also enable or aggravate other threats such as profiling and tracking [6].

2. **Localization and Tracking:** The threat of localization and tracking is the ability to determine and record a person's location through time and space. This can be done by using various data sources such as GPS, cell phone location, and internet traffic. Some of the most common privacy violations identified related to the threat of the IoT include the unauthorized access to a person's private information, such as the location of individuals and personal information about their illness [6].

   Aside from this, other features such as localization and tracking are also important for implementing an IoT system. These are some examples that show that users can consider it a privacy violation when they do not have control over their location information and that their data has been used in an inappropriate manner [6].

3. **Profiling:** The concept of profiling refers to gathering information about individuals to identify their interests. This is usually done in e-commerce platforms to improve customer service and personalization. In internal applications, it can also analyze and improve customer experience. There are various types of privacy violations that can be caused by profiling. Some of these include price discrimination, automated decisions, and the collection and selling of personal information [6].

4. **Privacy-violating interaction and presentation:** This type of threat is

usually referred to as shoulder-surfing. It involves intentionally disclosing private information to an unauthorized individual. IoT applications, e.g., healthcare and retail, transportation, and smart retail, are expected to require heavy interaction with their users. This is because the devices used in these systems will be able to collect and use information about their users. In such systems, users can control their environment through smart devices [6].

Although these systems' interactions and presentation mechanisms are expected to be public, they can still be monitored by people in the surrounding area. This type of threat can arise when their users' private information is exchanged. For instance, a person might ask for directions to a specific health clinic in a smart city. However, since the system might display the way to the location on a public display, it should not be answered since it will be visible to anyone who passes by [6].

5. **Lifecycle transitions and inventory attacks:** The private information of users is often threatened by the actions of smart devices when changes in control spheres are made. This issue has been highlighted by the discovery of compromising videos and photos on the used cameras, smartphones, or other electronic devices that stores photos and videos. Therefore, the actions of smart devices during the lifecycle transition are mainly responsible for the privacy violations that occur due to the information collected and stored.

   Aside from being used by people, smart devices also interact with other entities and services, such as systems and applications. This data is often stored in product history logs. For instance, in the case of medical devices, this information is used to monitor the health of their users. The collection of the data usage could reveal a lot about users' lifestyle [6].

   On the other hand, an inventory attack is an unauthorized access to a person's personal information. It involves collecting data about a person's activities and characteristics. The rise of the All-IP and end-to-end vision has made smart devices query-able. This allows legitimate entities such as the system owner to query it, but non-authorized individuals can also take advantage of this. For instance, an inventory attack could allow unauthorized individuals to collect data about a specific place.

Various privacy violations related to inventory attacks have been reported. First, burglars can use them to target private homes and factories. Similar to how they use social media to target or stalk potential victims [6].

6. **Linkage:** This threat is to link various data sources together, revealing truthful or misleading information that the user did not want to share and reveal this information with the other sources. Privacy violations can also occur when the privacy protection is bypassed and when systems combine data sources without proper procedures. This can lead to unauthorized access, and dissemination of private information [6].

   The increasing number of connected devices and the complexity of their data sources will cause the threat of linkage to grow in the future. One of the main reasons this happens is that various companies and organizations will eventually link their systems to form a new kind of distributed system. Although horizontal integration is generally more secure, it can also provide a way to enhance privacy by allowing more local data flow [6].

Chapter 3

Smart House Architecture

This chapter will discuss the architectural setup of our smart house case. The architectural structure includes what smart devices are included, the functions that make them smart, and how they communicate with the user and each other. The functions and communication of the smart devices are shown using a Data Flow Diagram.

3.1 Home Architecture

We decided to use a limited number of devices and focus on how they would work together and how privacy would affect them.

These devices are:

- Smart fridge
- Smart thermostat
- Smart meter

These are controlled by a smart hub that communicates with them all and can access the Internet. The smart hub is the fourth and last smart device in the architectural setup.

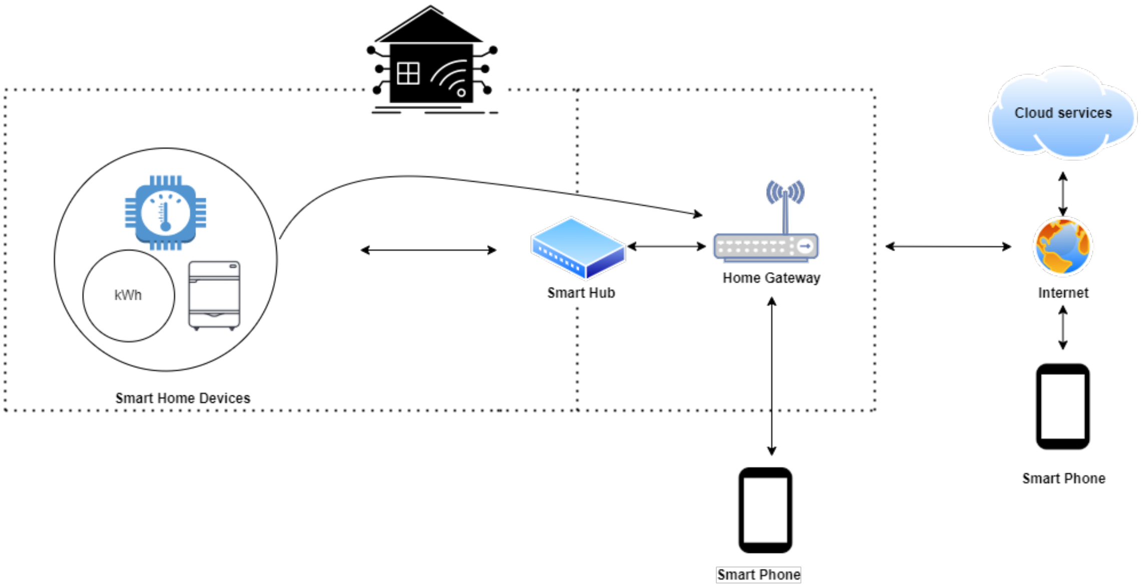


Figure 3.1: SmartHome

Inspiration for the setup was taken from "Security considerations for a secure and trustworthy smart home system in the IoT environment [26]", and "Security and privacy issues for an IoT based smart home[25]".

3.2 What Makes It Smart

This section will describe what makes each of these devices smart and what smart functionalities we assume them to have for this paper.

3.2.1 Smart Fridge

A smart fridge can store a shopping lists list of items in stock with expiration dates. Have to-do lists or even pictures[21].

A smart fridge is a fridge that is smart with the storage and preparation of food and can also have other smart features.

We have chosen to include only food-related features. Using these [21, 36, 51, 22] for inspiration the features we would assume our smart fridge to have would be:

- List of food items in the fridge. This can be done by the user adding items to a list as items are put inside the fridge and photo recognition by the fridge.
- Logs of when items have been used (and how much). A weight sensor in the fridge will log how much of an item has been used, and it, with photo recognition, can log what items are being taken out and put back in.
- Automatically make shopping lists after the use of items Items that are low in stock or out of stock can be automatically added to the shopping list or just added to a recommendation.
- Predict temperatures needed based on user habits.
- Meal planner with calendar and receipts. The fridge can offer receipts, and the user will ad the receipt to a day in the calendar.
- Energy control controls energy usage or delays other functions to decrease energy usage at daily peaks. The fridge can have access to power delivery services data when peeking at power consumption, and the price is
- Camera inside the fridge. Users can access the camera inside the fridge to look at all items inside from their phones.

3.2.2 Smart Thermostat

A smart thermostat can turn heating and cooling equipment on and off to reach the desired temperature in each room. The smart thermostat can help users save on energy costs and lower the environmental impact the user have[39].

Based on several references[13, 14, 15], these are some functionalities that make the thermostat smart;

- Remote control of temperature: A user should be able to set the desired temperatures from their phone.
- Room by room temperature: Each room should be able to have a different temperature.
- Room sensors: The thermostat should show the current temperature inside and other measurements like humidity.
- User sensors: The thermostats should be able to tell if someone is in the room and turn down the temperature regulation if no one is there.
- Routine learning: The thermostat should learn from using the desired routine and temperatures the users want throughout the week.
- Routine making: The users should be able to alter or create their routines for the temperatures at home.
- Away mode: If the user is not at home, the thermostat should go into the eco mode to save on power. This can be done by using sensors and checking if the user's phone is in the same house as the thermostat.
- Time till the desired temperature: The thermostat should estimate when the desired temperature will be reached.
- Logging of usage: The thermostat should log the usage of heating or cooling equipment and be able to show the users the use over time.

3.2.3 Smart Meter

A smart meter is an electronic device installed in a smart home or facility for measuring and reporting energy consumption remotely. Also, a smart meter transmits energy consumption data to energy suppliers to facilitate energy use monitoring and billing [57]. A smart meter provides several functionalities that make it smart. Firstly, a smart meter measures the amount of electricity used in a smart home. It then transmits this data directly to the energy provider at least once a month and also displays usage in the portable in-house display in real-time. As a result, similar to other smart devices and applications, a smart meter permits homeowners to track and monitor their energy consumption patterns in real-time [63]. In addition, a smart meter often leverages a smart data network to transmit automatic readings continuously, allowing energy companies and homeowners to monitor and bill energy consumption.

In addition, smart meters contain a telecommunications interface to support remote communication between the energy providers' central systems and the smart meter installed in a smart home. The built-in telecommunications interface allows distant reading and communications. Furthermore, the telecommunications interface permits additional smart functions, such as the remote operation of the smart meter's internal switch, remote modification of the meter's configurations and parameters, and remote sending of new tariffs. The smart meter's telecommunications interface and other technological developments enable it to accomplish these and other smart functions.

It is also worth noting that a smart meter permits smart homeowners to subscribe to their preferred cost-effective tariffs and energy register. In particular, a smart meter can store energy consumption measures and readings on a per hour basis, which facilitates near real-time monitoring [30]. Thus, this smart function makes it possible for energy consumers to bill their energy consumption for each period but at different tariffs. As such, smart homeowners can choose a tariff that enables them to reduce energy bills based on their energy consumption profiles. Besides, the smart functions lead to not only reduced spending on energy but also position smart meters as useful tools for nurturing a responsible energy consumption culture [30].

Another essential function of a smart meter is the collection of multiple records of various energy supply events. Specifically, other than collecting and storing energy consumption readings, a smart meter also collects real-time data regarding the status of an energy grid [30]. Smart homeowners can use this information to identify various events, such as energy supply interruptions, incorrect connections, and inefficient voltages. This smart function benefits smart homeowners since it minimizes the time required to detect and remediate faults and enhances the quality of energy supply significantly [30].

Additionally, there are more essential functionalities of a smart meter [34] ;

- **Power management:** Having a smart meter can help the system maintain its operation when the primary source of the energy supply is lost.
- **Synchronization:** This process involves transferring data collected by a smart meter to a central hub or a collection system. It is also very important to ensure that the transmission of data is reliable.

3.2.4 Smart Hub

A smart home hub is typically a hardware device that works seamlessly with a home automation network. It can be used for monitoring and controlling the communication between various IoT devices that use different protocols such as Bluetooth and Zigbee [8]. Additionally, having a smart home hub is beneficial if you're looking to integrate various devices into one system. It allows them to interact with each other using the same platform [47] . Moreover, a smart hub can collect and translates different communication protocols from various IoT devices in a smart home [8] .

3.3 Data Flow Diagram

Data Flow Diagrams (DFDs) have been included in our thesis. The purpose is to map out the data flow of the various conducted appliances. Four DFDs have been made, where each diagram maps out how each device communicates and the data flow when they perform their functionalities.

After making the DFDs, we decided on what data flow we consider privacy sensitive and having potential privacy issues. We marked the lines that follow the problematic data in red. In addition, the red arrows identify the specific different appliances' data flows exposed to various privacy threats. Shown on the DFDs, the problematic functions and data flows are the ones that demand communication between the user and the smart appliance. The functions that are done only inside of the smart appliance (such as 4.0 Temperature prediction in the smart fridge DFD A.1) are not considered problematic even though they use and store a lot of sensitive data.

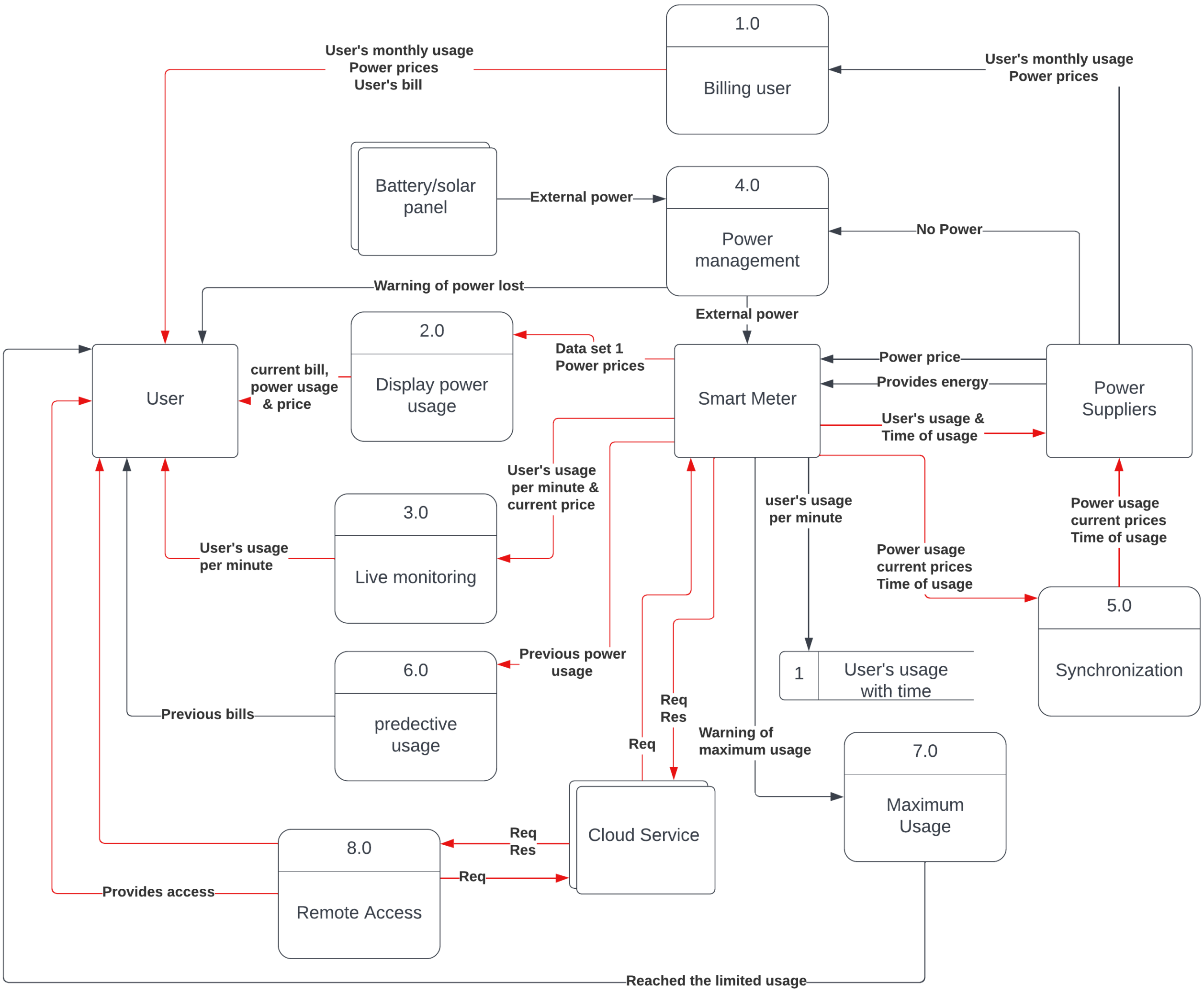


Figure 3.2: Smart Meter DFD

Figure 3.2 shows the created DFD for the Smart Meter, all other DFDs are found in the Appendix at A. All the squares with rounded corners are the functions of the smart appliance. The normal squares are the entities involved in the data flow, and the rectangle without the right line are databases. Making the DFDs was essential to ensure that the architecture was correctly done and important for the Privacy impact Analysis that was done after.

Chapter 4

Privacy Impact Assessment

A privacy impact assessment (PIA) is used to detect and analyze privacy risks throughout a system's life cycle. Privacy impact assessment reveals the Personally Identifiable Information (PII) gathered and how it will be handled, kept safe, and shared.

Government agencies such as the EU require PIAs to be conducted before processing PII[9]. In the United States of America, all federal agencies that develop technologies used for collecting and maintaining PII are required to conduct a PIA [18], and Australian Government agencies are required to perform a PIA for any projects considered high privacy risk[10]. PIAs are an excellent way to compile a list of the PII types collected and show how it is moved around for what purposes and entities. PIAs should also show how found privacy risks are mitigated.

In this PIA, the "Planning for Success: Privacy Impact Assessment Guide"[32] by the Information, and Privacy Commissioner of Ontario was used as a base, along with creating tables for all PII information collected in each of the smart appliances systems. However, not everything from the guide was relevant to the PIA needed for this assignment. Each smart appliance was analyzed individually as they all have their system and are connected to the Internet. They are shown to be connected through the Smart hub.

All functions of the smart devices are predefined in the house architecture and shown in the DFD diagrams.

The PIA process we used follows four key steps as listed below [32];

- **Preliminary Analysis:** Examine the system to determine if it involves collecting, using, retaining, disclosing, security, or disposal of personal information.
- **System Analysis:** Collect specific information about the system and who are the players? What is the type of manner in which personal data is collected, used, shared, or secured?
- **Privacy Analysis:** Using information from previous steps, identify potential risks and impacts on privacy. Then, consider ways to reduce or eliminate risks and assess the proposed privacy and security solutions.
- **PIA Report:** Document the findings and proposed privacy solutions. Then, share the report with stakeholders for approval to implement recommended solutions.

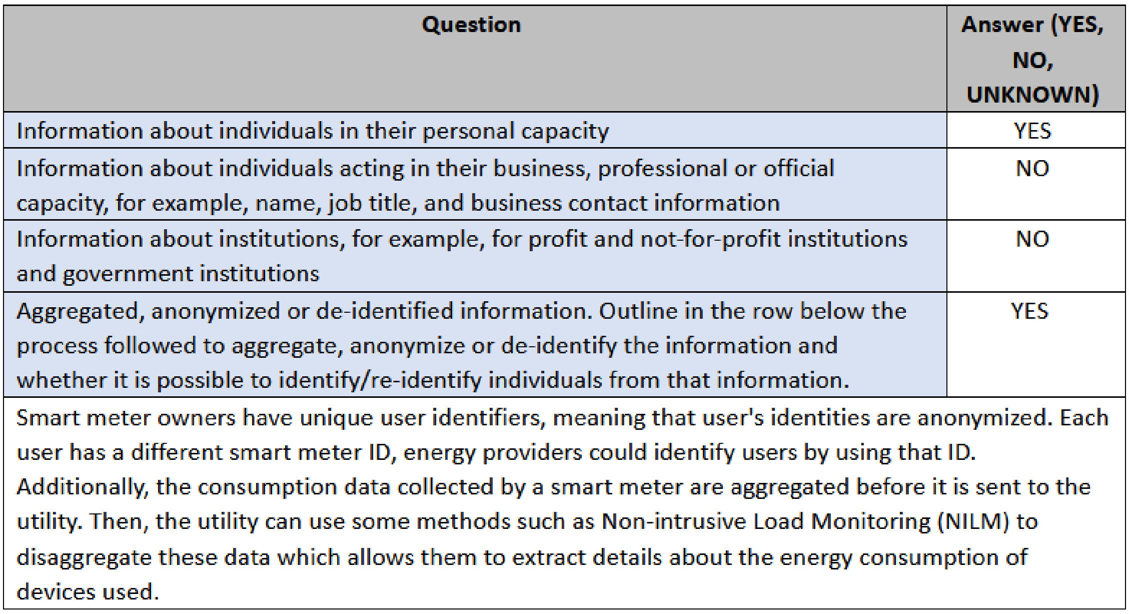
We have chosen to show the PIA of the Smart Meter and an explanation of how it was done. The rest of the PIAs are in the Appendix B.

4.1 Preliminary Analysis

The first step of a PIA is to ensure that the PIA is necessary. This is done by investigating whether PII is collected, used, retained, disclosed, or disposed of and identifying the type of PII. These tables are taken from the "Planning for success" guide.

The first question is on what types of information are collected.

Figure 4.1: Identify the kinds of information involved in the project (check all that apply).

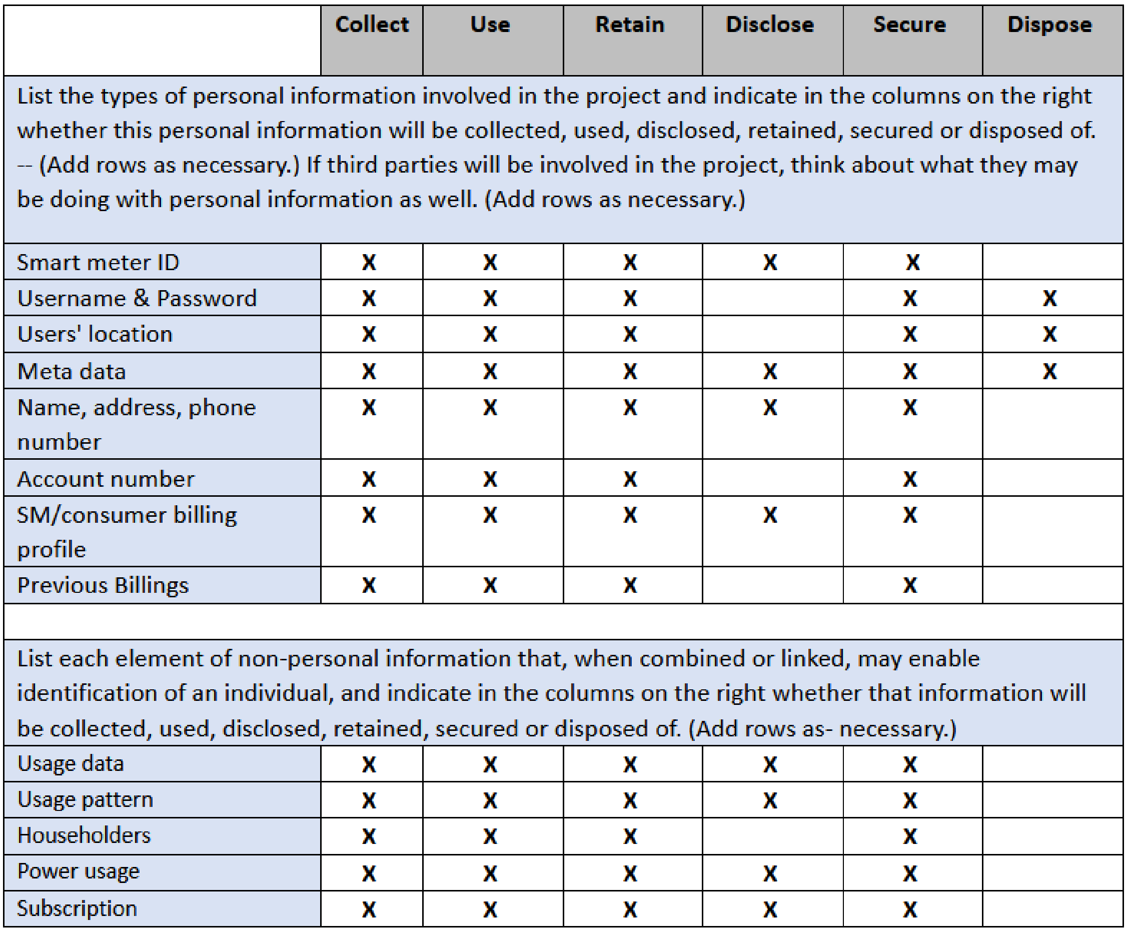


Question	Answer (YES, NO, UNKNOWN)
Information about individuals in their personal capacity	YES
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	NO
Information about institutions, for example, for profit and not-for-profit institutions and government institutions	NO
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	YES
Smart meter owners have unique user identifiers, meaning that user's identities are anonymized. Each user has a different smart meter ID, energy providers could identify users by using that ID. Additionally, the consumption data collected by a smart meter are aggregated before it is sent to the utility. Then, the utility can use some methods such as Non-intrusive Load Monitoring (NILM) to disaggregate these data which allows them to extract details about the energy consumption of devices used.	

For this question, the smart appliances were primarily alike. They are made for personal usage, and we will not focus on any business usage or aspects. The devices also do not contain any information about profit, non-profit, or government institutions. The different smart appliances differ in the aggregation/ de-identify methods used and the reason for usage.

The second question focuses on the usage of the data.

Figure 4.2: Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).



	Collect	Use	Retain	Disclose	Secure	Dispose
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. -- (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Smart meter ID	X	X	X	X	X	
Username & Password	X	X	X		X	X
Users' location	X	X	X		X	X
Meta data	X	X	X	X	X	X
Name, address, phone number	X	X	X	X	X	
Account number	X	X	X		X	
SM/consumer billing profile	X	X	X	X	X	
Previous Billings	X	X	X		X	
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as- necessary.)						
Usage data	X	X	X	X	X	
Usage pattern	X	X	X	X	X	
Householders	X	X	X		X	
Power usage	X	X	X	X	X	
Subscription	X	X	X	X	X	

The list of personal information involved in the smart applications differs somewhat, but they all have user login information, account, and appliance number. They also have indirect personal information through appliance settings and usage patterns of the devices. They also differ in what information is shared. For example, the smart fridge can share a shopping list and authentication to a shopping and delivery service. All appliances can communicate through the smart hub as well. For example, they may share a change of power state to show that they entered “eco mode” or similar.

The self-made tables in B.2 and below describe the same information types more with sensitivity level, origin, and what entities may access it.

The third question asks for all whom information is collected about.

To whom does the personal information relate?

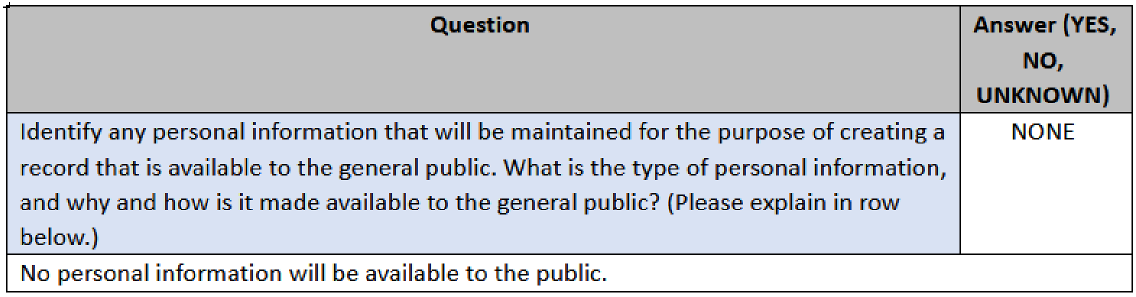
List all the individuals whose personal information will be involved in the project, that is, the data subjects.

> The user(s) / owner of the smart meter. Users are considered anyone living in a house with a smart meter installed. Only the owner will be registered with PII, such as name, address, billing information, etc.

This is the same for all smart home appliances. The user is the only one who has their information collected. However, the user is considered a singular entity; this is not always correct. For example, a smart house can have several inhabitants and visitors who interact with the smart fridge or are registered by the thermostat's motion detectors. The appliance registries their usage, and all interactions would be used to create usage patterns. In a sense, the usage pattern is about the household and not the user. However, one cannot consider the information collected as PII of other people in the house. One cannot determine who is recorded in a room or using electricity.

This question involves what information is public. All the smart appliances have the same answer here; none of the information collected will be available to the public. All are private information for private use by the user and possibly the company connected to the smart appliance.

Figure 4.3: Public Records and Excluded Personal Information



Question	Answer (YES, NO, UNKNOWN)
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	NONE
No personal information will be available to the public.	

As shown on the tables, all the smart home appliances collect and use some form of PII. Because of these reasons, the answer for if the PIA should be continued was set to a yes.

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.

> YES
> The PIA process will continue as personal information is collected and used. A PIA is a good way for the Master Thesis Report to examine how privacy can be impacted and protected in a smart home.

All of the PIAs done implied that we should continue with the PIA. Later when using a tool to perform a DPIA we got the same result.

4.2 System Analysis

4.2.1 Scope of PIA (Smart meter version)

> This PIA review is for the smart meter considered in the smart home architecture created for our case used in the master thesis. The scope of the PIA includes the Smart meter and its communication with other parties. The other parties are the user, power suppliers, and communication with the smart hub. Business aspects are considered out of scope as this master report focuses more on the technical aspects. Moreover, the only legal aspects considered are the GDPR as we are stationed in Europe.

This PIA has chosen to remove most business aspects, such as contracts with other corporations, as this would add more complexities without helping find privacy issues with the technologies.

The scope is set similarly for all the appliances. However, the communication with other parties differs, with the Smart Hub having all the different devices and the Smart Meter having more communication for electricity payments.

4.2.2 Project Authority

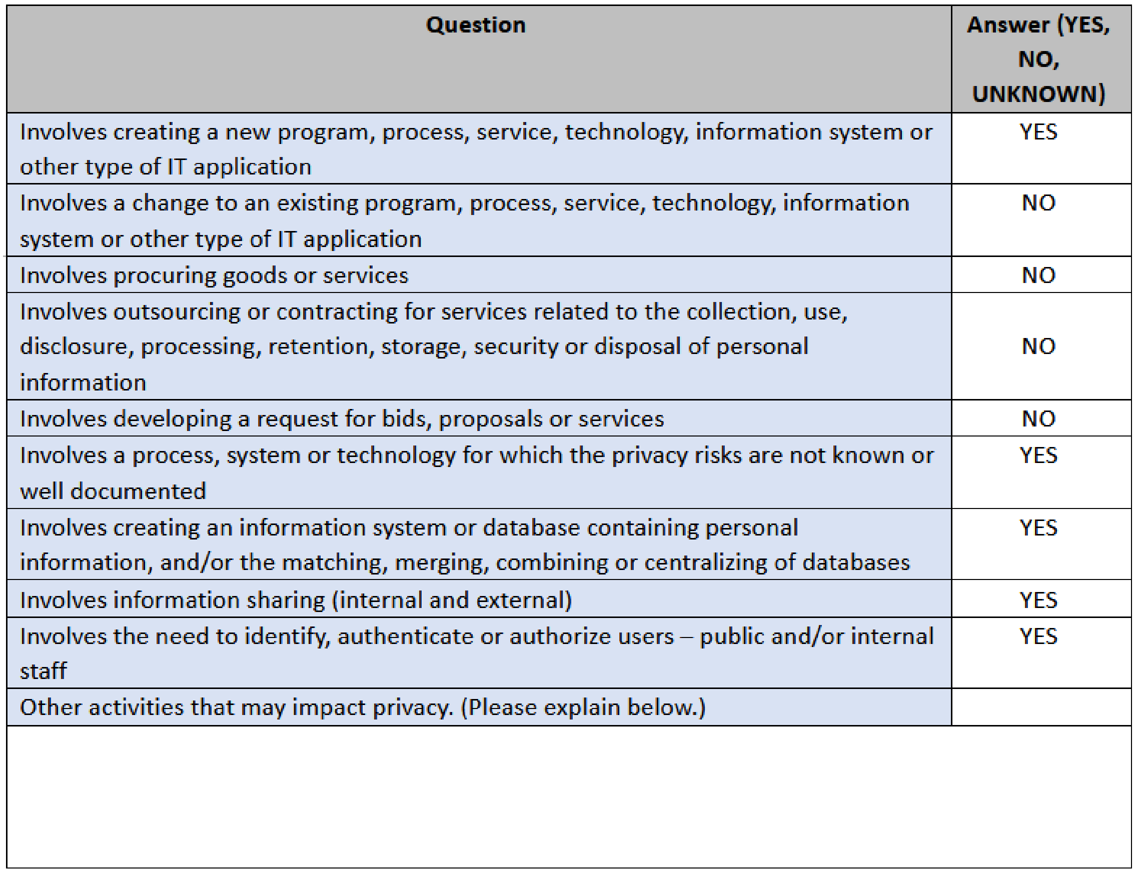
Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

> All services that use, store or move personal data are under the regulation of GDPR.

We, the writers, are stationed in Europe, where GDPR is the governing law considering PII.

4.2.3 Project Characteristics

Figure 4.4: Identify key characteristics of the project (check all that apply).



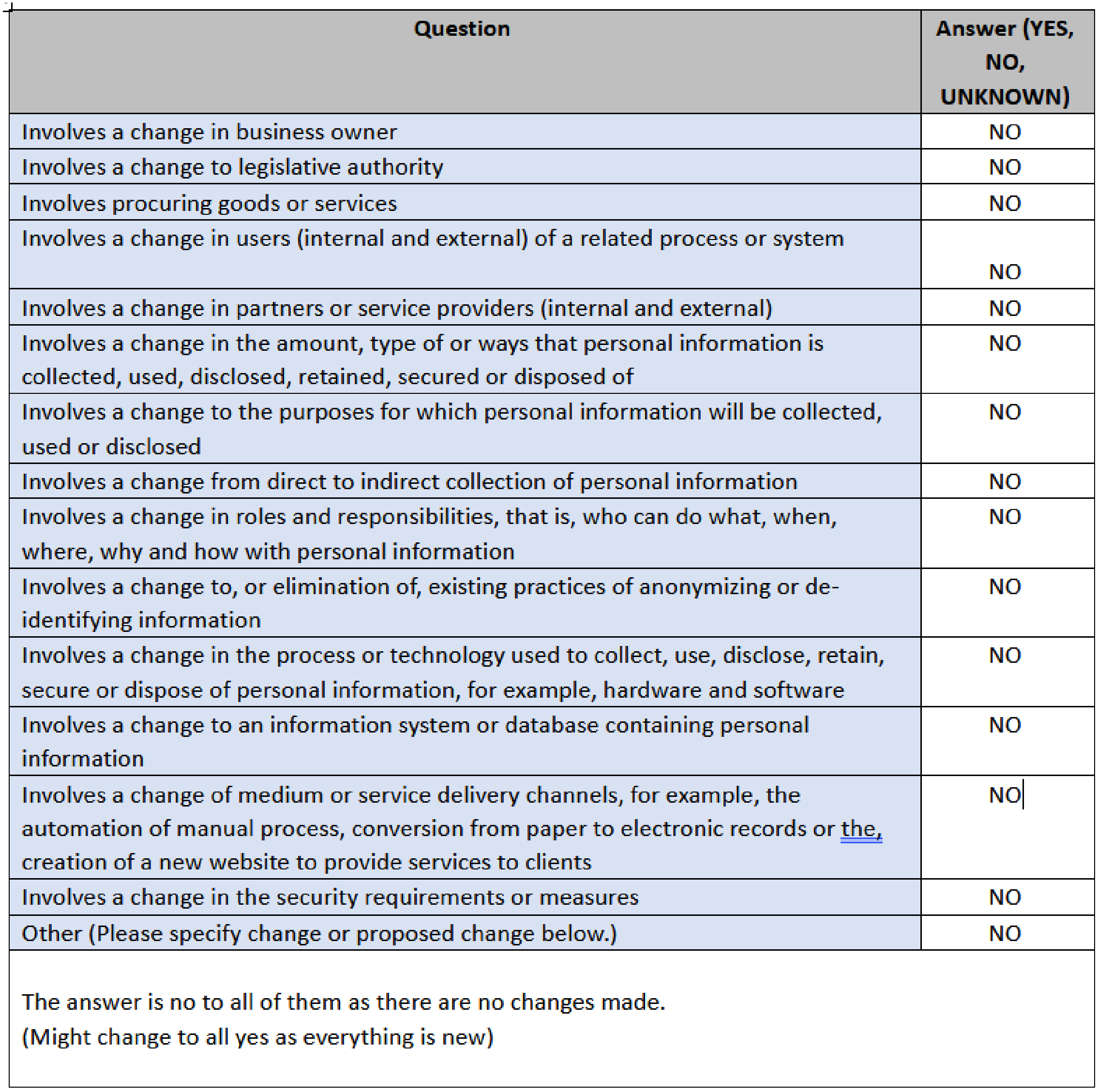
Question	Answer (YES, NO, UNKNOWN)
Involves creating a new program, process, service, technology, information system or other type of IT application	YES
Involves a change to an existing program, process, service, technology, information system or other type of IT application	NO
Involves procuring goods or services	NO
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information	NO
Involves developing a request for bids, proposals or services	NO
Involves a process, system or technology for which the privacy risks are not known or well documented	YES
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	YES
Involves information sharing (internal and external)	YES
Involves the need to identify, authenticate or authorize users – public and/or internal staff	YES
Other activities that may impact privacy. (Please explain below.)	

If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The service is set up by us for a case study and has no previous PIA assessments, so all programs, processes, and services can be considered new.
2. The privacy issues with smart homes and, by extension, a smart meter are not well documented/explored, and smart home devices are ever-increasing in complexity.
3. A user interaction database is stored on the device itself and user data in the clouds needed to service the user.
4. Information is shared between the smart meter and the user and between the smart meter and the smart hub (change of state or order to change state).
5. Users will have to use login credentials to connect to the smart meter from outside the same network and access cloud services.

The key characteristics of the project were considered based on how we thought it would look. A lot of the project was planned using the DFD diagram, but some aspects were not considered before the PIA was considered, and then some aspects were reconsidered. There was a big focus on privacy, and having the architecture of the smart house focused on not inviting third parties unless they can bring another service to the user.

Figure 4.5: Identify any changes that will result from the project (check all that apply).



Question	Answer (YES, NO, UNKNOWN)
Involves a change in business owner	NO
Involves a change to legislative authority	NO
Involves procuring goods or services	NO
Involves a change in users (internal and external) of a related process or system	NO
Involves a change in partners or service providers (internal and external)	NO
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	NO
Involves a change to the purposes for which personal information will be collected, used or disclosed	NO
Involves a change from direct to indirect collection of personal information	NO
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information	NO
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information	NO
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software	NO
Involves a change to an information system or database containing personal information	NO
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients	NO
Involves a change in the security requirements or measures	NO
Other (Please specify change or proposed change below.)	NO
The answer is no to all of them as there are no changes made. (Might change to all yes as everything is new)	

The reason all the boxes were set as “NO” is that this is the creation of a new system and no changes are made as there was nothing to change. privacy impact assessment is required to happen when creating new technologies and when major changes are made, that is why we chose to set all of these as no.

If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

NA

Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

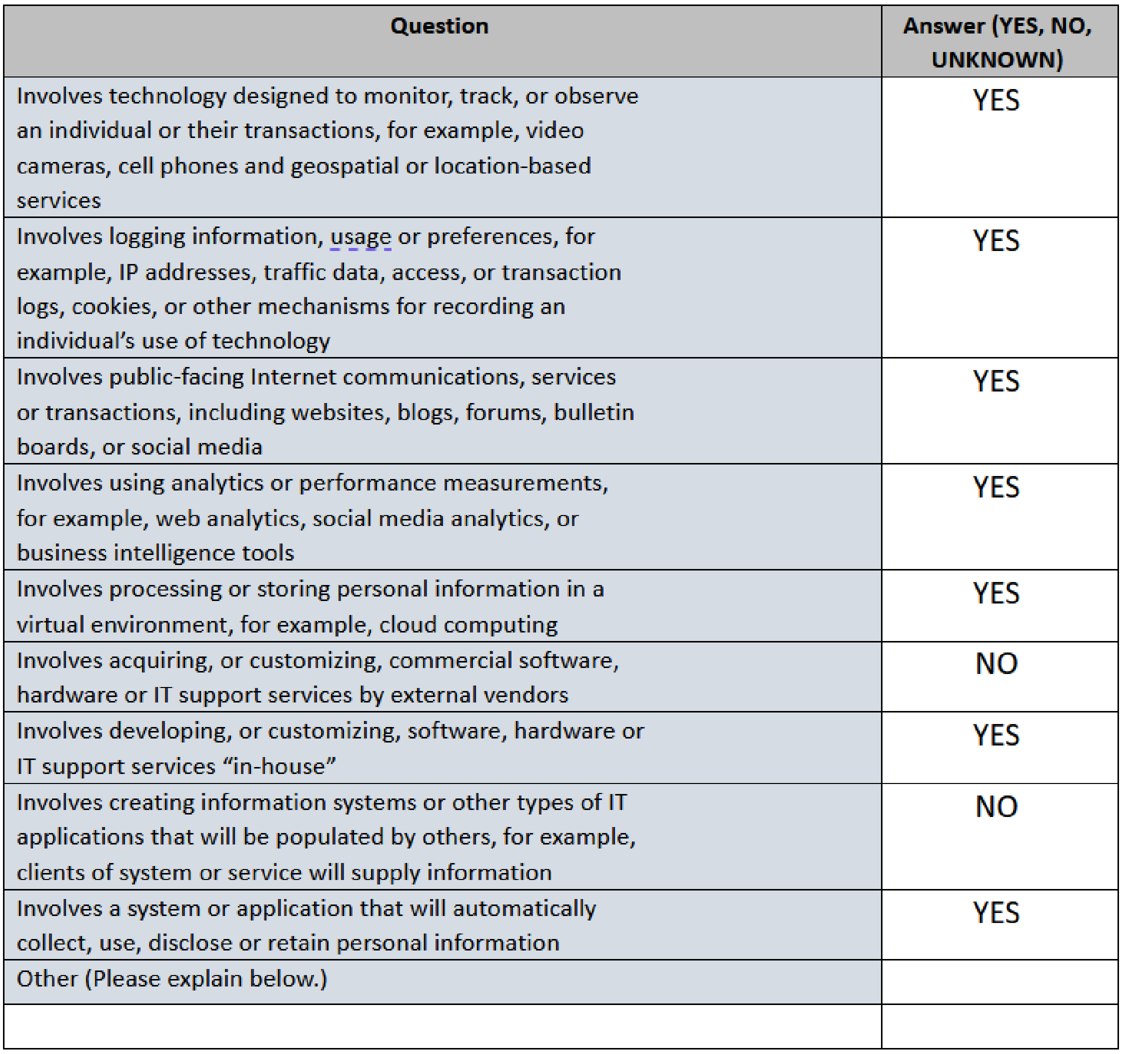
NA

As stated, we do not focus on business processes as it complicates without

4.2.4 Technology

These questions consider the technologies used in the project.

Figure 4.6: Identify technology-related characteristics of the project (check all that apply).



Question	Answer (YES, NO, UNKNOWN)
Involves technology designed to monitor, track, or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services	YES
Involves logging information, usage or preferences, for example, IP addresses, traffic data, access, or transaction logs, cookies, or other mechanisms for recording an individual's use of technology	YES
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	YES
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools	YES
Involves processing or storing personal information in a virtual environment, for example, cloud computing	YES
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors	NO
Involves developing, or customizing, software, hardware or IT support services "in-house"	YES
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information	NO
Involves a system or application that will automatically collect, use, disclose or retain personal information	YES
Other (Please explain below.)	

If you answered yes to any of the above, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

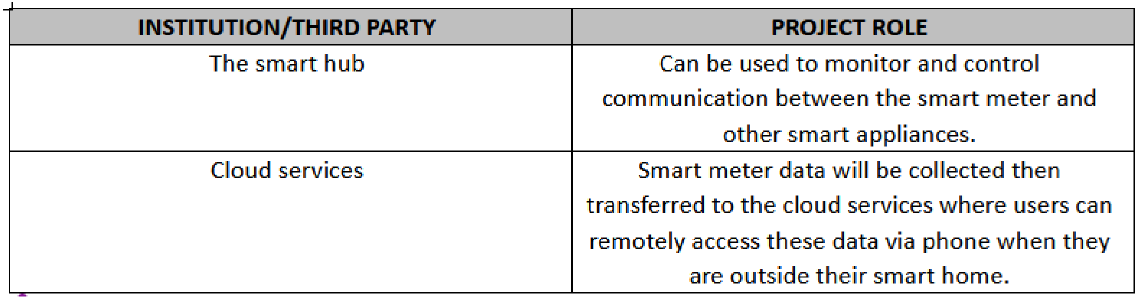
1. The smart meter has been developed with some technology that provides power suppliers with the ability to know users'/smart meter locations. In addition, the smart meter will measure overall users' power usage and then generate billing based on that.
2. Smart meter users have logging information to log in to the web portal to monitor their power usage outside of their homes.
3. The smart meter does involve public-facing internet communication and services, where users' power consumption transfers from the smart meter to the power suppliers.
4. The smart meter involves using analytics and performance measurements. First, it measures users' power consumption usage. Additionally, the smart meter can analyze power used each hour, and by using analytics, it can detect any data tampering.
5. The smart meter data will be stored in a cloud-based service, where users can access data via their phones.
6. The smart meter and its software are created and owned by the same company.
7. The smart meter automatically collects user power usage, uses the collected data and transfers it to the power suppliers, and retains it.

We went through each smart appliance and figured out what technologies they included. Except for the smart hub, all appliances contained technologies for monitoring or tracking an individual. However, the technologies used for that differ. All of the other boxes have the same answer for all of the boxes; however, the reasons differ.

4.2.5 Roles and Responsibilities

This part focuses on the roles and responsibilities and what entities contain them.

Figure 4.7: List other institutions or other third parties involved in developing or implementing the project and describe their role.



INSTITUTION/THIRD PARTY	PROJECT ROLE
The smart hub	Can be used to monitor and control communication between the smart meter and other smart appliances.
Cloud services	Smart meter data will be collected then transferred to the cloud services where users can remotely access these data via phone when they are outside their smart home.

List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information on behalf of your institution

None The Smart Hub does collect, use/process, retain, store, disclose and dispose of data; however, this is not considered as "on behalf of your institution(the smart meter supplier)" as this is a secondary and optional function that the owner decides on using.

We decided that a smart hub connected would count as a third party, but it gives new functionalities and does not collect or process the smart meter's data. And the cloud connection is considered part of the smart meter service and not delivered by a third party.

Identify any location outside of the EU where personal information may be retained or stored, and the third parties involved.

No personal information will be stored or retained outside the EU.

All data will be stored in the EU for ease of the project and compliance with the GDPR.

List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

> No other parties will have access to or use personal information.

In this context, we set the rules so that no other parties can access the PI.

Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

> NA

As we are not considering any other third parties, this is irrelevant.

4.2.6 Relevant Information

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed Project Analysis Questionnaire.

> NA

As mentioned we do not put focus on the business aspects.

4.2.7 Personal Information Flows

Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis

Questionnaire.

> See DFD diagram 3.2 and extra tables included in section B.4

The Data Flow Diagrams show how the data moves. Moreover, the tables underneath show how the information is collected and used.

4.3 Personal Information Table

We created tables of all the personal information that was generated or exchanged for each of the smart appliances. All of the tables are placed here B.1 in the appendix. Each smart appliance has several tables for where the PI is generated or exchanged. The tables contain the Parameter or type of PI along with its description and sensitivity, origin and who uses the PI. As we have done with the PIA we will only show the Smart Meters tables here.

PIA of smart meter

User account			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Login	User identifier **(Not sensitive)**	Created by user	User Billing server Web-portal App server
Password	User password **(High sensitive)**	Created by user	User User Billing server Web-portal App server
Name, address, phone number	account holder's details (name, address, phone number) **(High sensitive)** can be combined with payment methods	SM owner	Billing server App server
Account number	Unique account number for SM owner **(Low sensitive)**	App server	SM owner App server Web-portal Billing server

PIA of smart meter

Daily Usage			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Usage pattern	Traceable power usage patterns and householder behaviors **(High sensitive)**	Power suppliers	SM owner
Householders	Gives ability to the suppliers to know when users are most active **(High sensitive)**	SM owner	SM owner
Power usage	provides used power Current price current total price of power used **(Moderate sensitivity)**	SM owner	householders, SM owner

PIA of smart meter

User subscription			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
SM type and serial number	SM information **(Low Sensitivity)**	Manufacturer	App server
Subscription	Subscription type, Subscription demands **(Low Sensitivity)**	SM owner	App server
Subscriber's Name	User's Full name **(High Sensitivity)**	SM owner	Billing server
Address	User's Country, City, State, Street **(Moderate Sensitivity)**	SM owner	Billing and App servers
User's phone number	Phone number of SM owner **(Moderate Sensitivity)**	SM owner	Billing and App servers

PIA of smart meter

Billing Details			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
SM ID	SM identification, identifies users **(Low sensitive)**	Provided by suppliers	SM owner
SM/consumer billing profile	Payment methods **(High sensitive)**	SM owner	SM owner
Previous Billings	List of previous bills **(High sensitive)**	SM owner Power providers	SM owner Power providers

PIA of smart meter

Attachment to Web-portal			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	User account number when created **(Moderate Sensitivity)**	Account server via SM owner	App server Web-portal
SM Serial number	Unique identifier for the SM **(Moderate Sensitivity)**	SM manufacturer	SM owner App server Web-portal

4.4 Smart Meter Privacy

The data from a Smart meter can either be privacy-sensitive or non-sensitive. Usage pattern data are, for instance, classified as privacy-sensitive, whereas the general information about the smart meter itself is classified as non-privacy sensitive [7]. The smart meter does not send the actual power usage even though it is connected to the utility. Still, it might send information about how smart appliances have been used and which time the householders have utilized all different devices.

Additionally, the utility could also be fetched this information if it is not adequately secured. For instance, if we assume that there is someone in the middle and intercept this data from the consumption values, then they will be able to see which equipment is running inside the household at different time intervals. Therefore, utilities must secure their customers' data to prevent data leakage issues.

In figure 4.8, we can see an actual example of a privacy violation when a utility collects energy consumption data from a smart meter in a customer's house [64]. The data shown in the figure shows customers' activities that can be collected and combined with other relevant information that allows the utility to trace the energy usage patterns and identify customers' behaviors. Furthermore, as we can see in the figure, the data collected identify when customers are active and inactive. Therefore, it is always essential to think about customers' privacy protection and how it should be preserved when SMs are deployed [64].

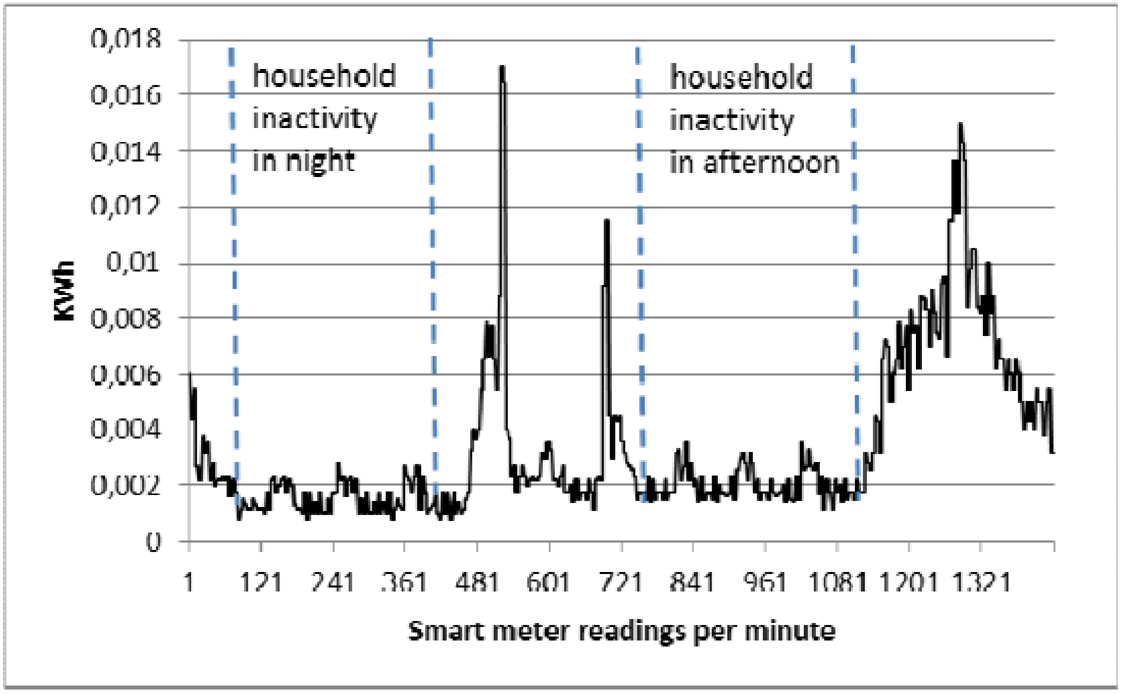


Figure 4.8: SM reading per minute [64]

4.4.1 SM Data Inference

Non-Intrusive Load Monitoring (NILM) is used to gather more data about users. NILM makes it possible to derive information such as users' behavior and their locations, the appliances they have at home, and the total electricity they use [7]. Moreover, NILM can divide the energy data into various categories: appliances, lighting, cooking, heating, and hot water. Based on these categories, the utility company uses disaggregation techniques to extract details about the energy consumption of each device of an individual household. If we assume that someone gains access to this data, then they will be able to figure out what appliances are being used and how often [7].

4.5 Privacy and Usability

Privacy and usability do not concur with one another. There is always a difference. Privacy refers to the scenario where an individual's information and life are not exposed when they do not want it exposed. Identical to the systems, it is terrible for the information that was meant to be private to be exposed to unauthorized people. Therefore, privacy is the act of being accountable for one's information [29]. Usability is the process of operating a device, or a technology [59]. There is a conflict between usability and privacy, and most people base their concerns more on usability.

Besides, if data will be secured in a PIA analysis on smart meters in smart homes is critical in ensuring data privacy. Smart meters are usually connected to the home's electrical grid and collect data on electricity usage. Such data can improve energy efficiency and help utilities manage demand [16].

However, if this data is not correctly secured, it could be accessed by unauthorized individuals who could use it for nefarious purposes. Therefore, any PIA conducted on smart meters must include an assessment of the security measures to protect the data collected by these devices. Only by assuming that data will be secured can one ensure that it will be. The other assumption is that the system properly anticipates the privacy impacts of introducing smart metering, remote communication, and control capabilities to domestic consumers. Then, the provider manages and designs the solution to provide for adequate controls over personal information, including new controls governance.

4.6 PIA Tools

To ensure that the manual PIA was correct, we decided to use a PIA tool to compare our manual PIA with the outcome from a tool. If the outcome from the tools differs mainly from the work we have done, it can indicate something wrong. The tools could also show where work would have to be done in business and legal aspects, which we have considered out of scope. The tool was only used on the smart fridge. If the results from the PIA done using a tool were the same as what we got from the manual PIA, then the manual PIA was done correctly, and the result was correct.

4.6.1 Tool Selection

Several online services that offer PIAs (or DPIAs) were considered before we decided to use CyberComply by Vigilant Software. They were used as they provided a free trial on their tools for DPIA, risk assessments, and more. We also chose CyberComply as it included a privacy risk assessment in the DPIA with controls from sets such as Essential Cybersecurity Controls, ISO 27001, NIST 800-53, SOC 2 TSC, and more.

4.6.2 CyberComply

The CyberComply DPIA was done by answering a questionnaire divided into six parts. The first two describe the project and identify the need for the DPIA. Then there are questions on the necessity and proportionality of the processing of the PI. The last two parts are the privacy risk assessment and review of the DPIA.

We set the amount of data subjects as 0-10 because we considered the subjects to be one household compared to the entire user base (hover many households) of the appliance.

CyberComply faults

When the PIA was done with everything except the privacy risk assessments, the risk assessment we were trying to use was faulty and would not save any risk scenarios. Therefore, the generated DPIA report does not include any of the privacy risk assessments with accompanying controls.

4.6.3 Comparisons

The results are shown through the generated report posted in the appendix, see C. The DPIA was shown as necessary by the first two question parts. Again, this is consistent with the manual PIA that we did.

Several of the questions were similar enough that the answer was the same. However, there were more questions included that showed our lack of expertise, such as question 4 in the Context of Processing part **"To what extent are individuals likely to expect the processing?"** It also shows our lack of planning in the codes of practices.

The CyberComply DPIA included more questions in connection to GDPR. The questions were answered as well as possible with the limitation of the writers not being lawyers and the project being made for the master project, so some aspects are not considered out as they are considered out of scope.

The DPIA report shows where future work would have to be done for a real product. It also shows that on the aspects set as inside the scope of the master thesis, the manually done PIAs are on the right path correct.

The DPIA would have been a big help in the privacy risk assessment. However, during the work on the project, it was not fixed in a timely enough manner to be used. A less effective risk assessment was done using CyberComplys' risk assessment tool. The generated report from that is in the appendix D.

4.6.4 Privacy Risk Assessment

As mentioned 4.6.2 the DPIA tool from CyberComply did not work when trying to create a Privacy Risk Assessment for the DPIA.

However, as it seemed like an excellent way to create a list of vulnerabilities and subsequent controls, we tried to use the normal risk assessment tools CyberComply had based on specific assets. This risk assessment does not focus on privacy as the one in the DPIA would. However, as the latter did not work, the second-best was chosen.

The choice was made to still focus on privacy as this is the focus of the master thesis. Consequently, any vulnerability that was not considered to affect privacy specifically would not be included.

The risk assessment tool was based on assets, whereas the privacy risk assessment was scenario-based. This made it harder to connect it to the DPIA.

The risk analysis contained extensive lists of possible threats, vulnerabilities, and controls. The risk analysis was done by using the tool to go through the list of threats and adding the ones we considered relevant for privacy issues. Then we added the vulnerabilities that could be connected to the threat. Lastly, the controls to mitigate the vulnerabilities were added. The controls were from ISO 27001, 27018, 27032, SOC 2 TSC, NIST 800-53, CSA CCM v3, Cyber Essentials, and ECC 2018 publications. The tool also included the function to add risk level by using a matrix table (see figure 4.9) with the outcome and likelihood combined to give the risk score. The table could be made before and after controls were introduced to show the effect of the controls. However, this was not done as we combined all the threats, vulnerabilities, and controls.

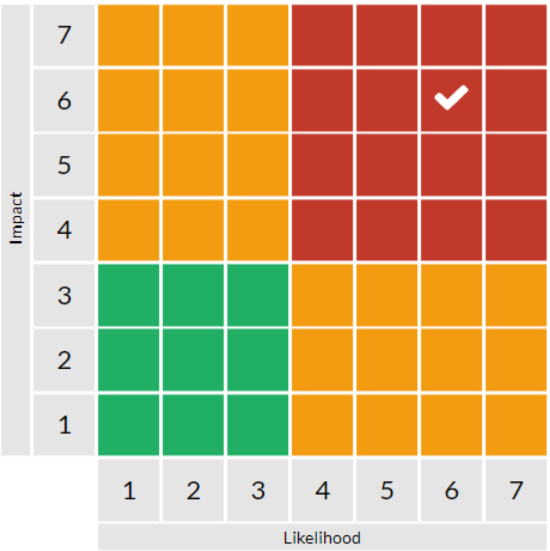


Figure 4.9: Likleihood and Outcome combines to Risk (not accurate for this representation)

4.7 PIA and DPIA Reflections

The personal information sent in transit for each smart appliance is quite similar. Therefore, the threats and vulnerabilities could be mostly the same between devices when doing the risk analysis.

Chapter 5

Privacy Improvement Methods

This chapter will discuss newer technologies being developed or are waiting for their implementation to be normalized. The technologies will be explained; what are they, what problems they solve, or weaknesses they mitigate. Then the feasibility of the technology will be discussed in the view of smart homes.

5.1 Authentication Protocol

Related to our case, many researchers have proposed various authentication protocols that can be used to secure the communication between users and smart devices in smart home environments. Santoso et al. [52] proposed a secure authentication protocol with the help of **Elliptic Curve Cryptography** (ECC). Unfortunately, some authors [5, 20] claimed that the proposed protocol by Santoso et al. [52] fails to provide users anonymity and non-traceability. Additionally, they meant that the protocol is vulnerable to smart card and privileged-insider attacks. Dey et al. [17] proposed a protocol based on a session key for the smart home by using public-key cryptography.

Additionally, they claimed that their proposed protocol was immune to various attacks, such as message replay, message-forgery, device compromise, and man-in-the-middle (MITM). However, several researchers [23, 43] claimed that the proposed protocol by Dey et al. [17] was not flawless as it was meant to be. They claimed that the protocol proposed does not provide confidentiality and anonymity, fails to ensure message freshness, and at last, it is not immune against known-key attacks [23, 43].

Although most proposed protocols are based on asymmetric key cryptography, this is considered ideal for low-capacity devices. However, they are still not acceptable for the smart devices due those protocols are too computationally expensive [45].

Xiang et al. [62] proposed a protocol for the smart home environment, where they claim that their protocol ensures mutual authentication and data integrity. However, another study claims that the protocol provided by Xiang and Zheng [62] does not provide secure mutual authentication and is vulnerable to session key disclosure attacks, impersonation, and stolen smart device [42].

Moreover, the study suggests a solution to improve security flaws of the protocol where they propose a secure and lightweight authentication protocol for IoT-based smart homes. The improved protocol consists of four various phases [42];

1. **Initialization:** In this phase, a Registering Authority generates a master key K_{RA} and both smart device and gateway will have a unique identity, ID_{SD}, and ID_G. Additionally, the smart device will have a secret key K_{SD}. This process must be done before the gateway and smart device is deployed in the smart home.

2. **Registration:** This phase consists of details registering the smart devices and users. Smart devices have to be registered by the registering authority (RA) to provide services to users.

   For Smart device registration, the first step is that smart device generates a random number r_{SD} and computes a pseudo-identity PID_{SD}, which is the hash of the smart device ID concatenated with the randomly generated number PID_{SD} = h($ID_{SD}||r_{SD}$). Then the smart device sends the PID_{SD} along with r_{SD} to the registering authority. On the RA side, RA generates a random number as well r_{RA}; then it computes the key shared between the gateway and the smart device K_{GSD} = h(PID_{SD} || K_{RA} || r_{RA}), which is the hash function of the pseudo-identity of the smart device, the key of RA, and the random number generated of RA. Then, RA stores PID_{SD}, K_{GSD}, and r_{SD} in the home gateway's database and sends K_{GSD} to SD. Lastly, after receiving the message from Ra, SD computes B_1 = r_{SD} $\oplus h$(ID$_{SD}$ || K_{SD}) and B_2 = K_{GSD} $\oplus h$(r$_{SD}$ || K_{SD}), then SD stores the computed values along with pseudo-identity of SD in the memory. This process is illustrated in figure 5.1.

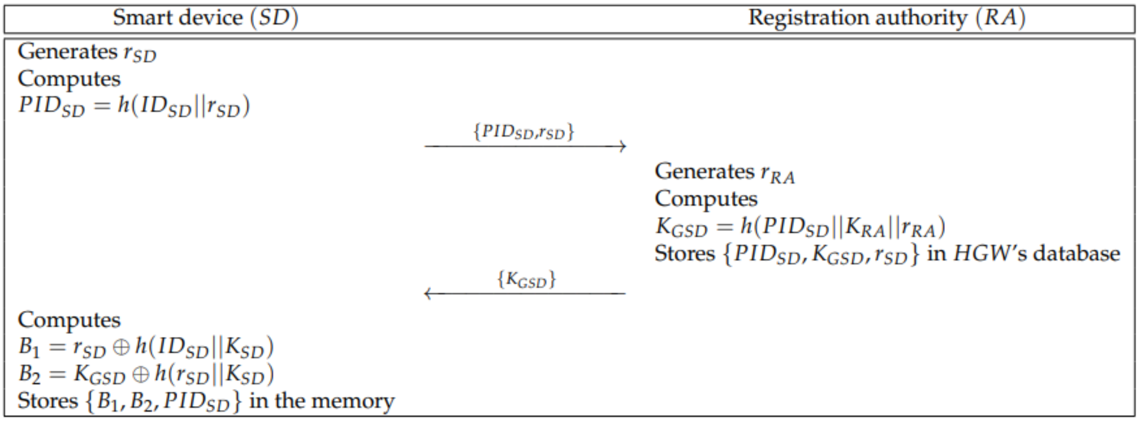
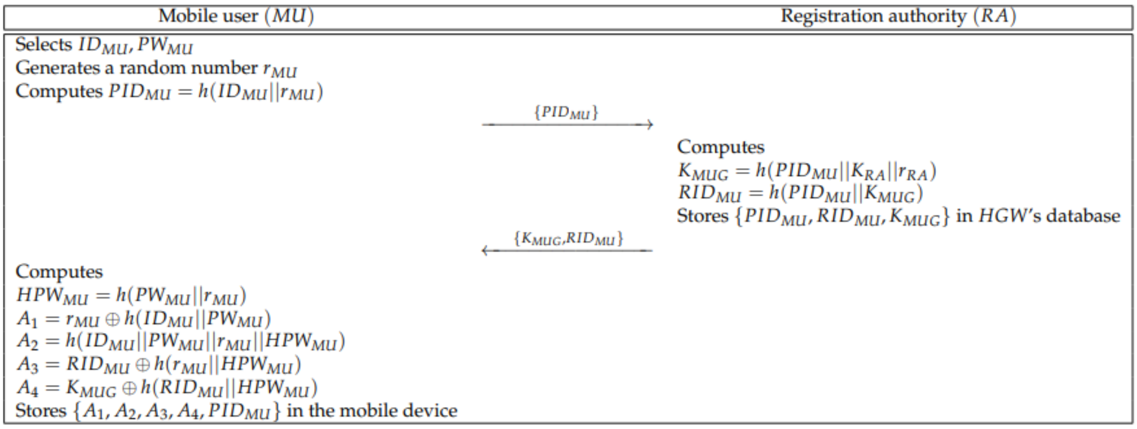

Smart device (SD)
Registration authority (RA)
Generates r_{SD}
Computes
$PID_{SD} = h(ID_{SD}||r_{SD})$
$\{PID_{SD}, r_{SD}\}$
Generates r_{RA}
Computes
$K_{GSD} = h(PID_{SD}||K_{RA}||r_{RA})$
Stores $\{PID_{SD}, K_{GSD}, r_{SD}\}$ in HGW's database
$\{K_{GSD}\}$
Computes
$B_1 = r_{SD} \oplus h(ID_{SD}||K_{SD})$
$B_2 = K_{GSD} \oplus h(r_{SD}||K_{SD})$
Stores $\{B_1, B_2, PID_{SD}\}$ in the memory

Figure 5.1: Smart Device Registration [42]

The second part is Mobil user (MU) registration at RA. In the beginning MU selects its identity (ID_{MU}) and password (PW_{MU}), then it generates a r_{MU} and computes PID_{MU}. Moreover, MU sends its pseudo-identity to RA. At the RA side, RA computes a key K_{MUG} that is shared between the mobile user and the gateway and RID_{MU}. Then, RA stores the received message from MU which is PID_{MU} along with the computed values K_{MUG} and RID_{MU} in the gateway's database. Further, RA sends the computed values K_{MUG} and RID_{MU} to MU. After received the message from RA, MU computes HPW_{MU}, A_1, A_2, A_3, A_4. Then, it stores A_1, A_2, A_3, A_4 along with its computed pseudo-identity PID_{MU} in the mobile device. This protocol is illustrated below in figure 5.2.


Mobile user (MU)

Registration authority (RA)

Selects ID_{MU}, PW_{MU}
Generates a random number r_{MU}
Computes $PID_{MU} = h(ID_{MU}||r_{MU})$

$\xrightarrow{\{PID_{MU}\}}$

Computes
$K_{MUG} = h(PID_{MU}||K_{RA}||r_{RA})$
$RID_{MU} = h(PID_{MU}||K_{MUG})$
Stores $\{PID_{MU}, RID_{MU}, K_{MUG}\}$ in HGW's database

$\xleftarrow{\{K_{MUG}, RID_{MU}\}}$

Computes
$HPW_{MU} = h(PW_{MU}||r_{MU})$
$A_1 = r_{MU} \oplus h(ID_{MU}||PW_{MU})$
$A_2 = h(ID_{MU}||PW_{MU}||r_{MU}||HPW_{MU})$
$A_3 = RID_{MU} \oplus h(r_{MU}||HPW_{MU})$
$A_4 = K_{MUG} \oplus h(RID_{MU}||HPW_{MU})$
Stores $\{A_1, A_2, A_3, A_4, PID_{MU}\}$ in the mobile device

Figure 5.2: Mobil User Registration [42]

3. **Authentication And Key Agreement:** In this phase, an authentication key establishment will be executed to authenticate the gateway, smart device, and the user and establish a session key between the smart device and user.

   The initial step in this phase is that MU inputs its identity (ID_MU) and password (PW_{MU}). Then, MU computes a random number (r_{MU}), HPW_{MU}, A_2^*. Next, MU verifies if A_2^* is equal to A_2, if the verification is satisfied MU generates a random nonce (RN_{MU}) and computes RID_{MU}, K_{MUG}, M_1, C_1, and V_{MU}. Then, MU sends (PID_{MU}, M_1, C_1, and V_{MU}) to the HGW.

   When the HGW receive the message from MU, the HGW retrieves RID_MU and K_{MUG} corresponding to PID_{MU}. Then, it computes (RN_{MU}^* || PID_{SD}^*) and V_{MU}^*. Furthermore, it checks if V_{MU}^* is equal V_{MU}. If equal the HGW retrieves K_{GSD} and r_{SD} corresponding to PID_{SD} and generates RN_G. Moreover, the HGW computes M_2, M_3, h(ID_{MU} || RN_{MU}), C_2, and V_{MUG}. Lastly, it sends PID_{MU}, M_3, C_2 and V_{MUG} to SD.

   Upon receiving the message, SD computes r_{SD}, K_{GSD}, M_2^*, V_{MUG}^*. Then, it checks if $V_{MUG}^* = V_{MUG}$ and the statement is valid, SD generates RN_SD. Next, SD computes (h(ID_MU || RN_MU || h (ID_G || RN_G)), a session key SK, M_4, and V_{SD}. Finally, SD sends M_4, V_{SD} to the HGW.

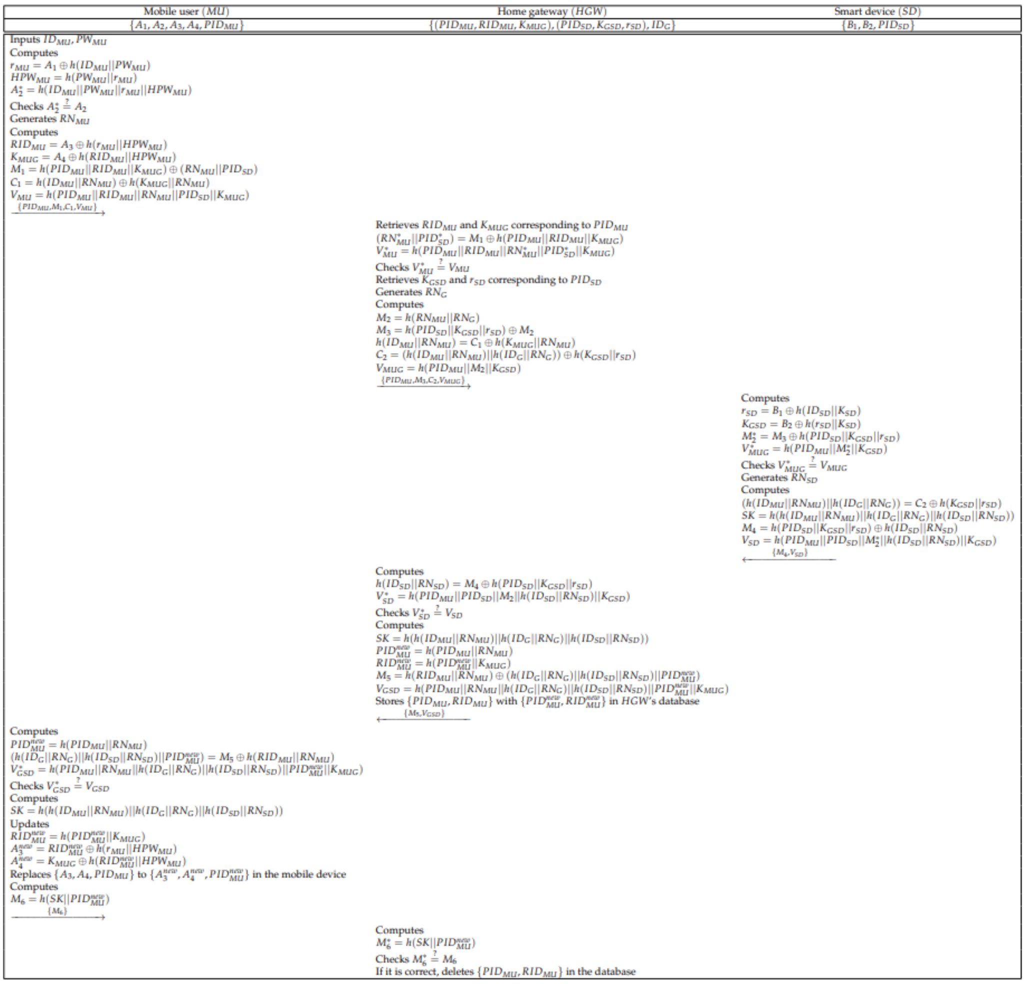
   When the HGW receive the message from SD, it computes h (ID_{SD} || RN_{SD}), V_SD^*. Then, HGW checks if $V_SD^* = V_{SD}$. Then it computes SK, $PID_M^{new}U$, $RID_M^{new}U$, M_5, V_{GSD}. Then it stores PID_{MU}, RID_{MU} with $PID_M^{new}U$, $RID_M^{new}U$

in HGW's database. Finally, it sends M_5,V_{GSD} to MU.

Upon reciving the message, MU computes $PID_{M}^{new}{}_{U}$, (h(ID_G || RN_G || h (ID_{SD} || RN_{SD} || $PID_{M}^{new}{}_{U}$), and V_{GSD}^{*}. Then, its checks if $V_{GSD}^{*} = V_{GSD}$. After that, MU computes SK and updates $RID_{M}^{new}{}_{U}$, A_3^{new}, A_4^{new}. Then, it replaces A_3, A_4, PID_{MU} to A_3^{new}, A_4^{new}, $PID_{M}^{new}{}_{U}$ in MD. Moreover, it computes M_6 and sends it to HGW.

Upon receiving the message, HGW computes M_6^{*} and checks if $M_6^{*} = M_6$. If the statement is correct, it deletes the stored PID_{MU}, RID_{MU} in the database.

This protocol is illustrated in figure 5.3.



Mobile user (MU)	Home gateway (HGW)	Smart device (SD)
$\{A_1, A_2, A_3, A_4, PID_{MU}\}$	$\{(PID_{MU}, RID_{MU}, K_{MUG}), (PID_{SD}, K_{GSD}, r_{SD}), ID_G\}$	$\{B_1, B_2, PID_{SD}\}$

Inputs ID_{MU}, PW_{MU}
Computes
$r_{MU} = A_1 \oplus h(ID_{MU}||PW_{MU})$
$HPW_{MU} = h(PW_{MU}||r_{MU})$
$A_2^{*} = h(ID_{MU}||PW_{MU}||r_{MU}||HPW_{MU})$
Checks $A_2^{*} \overset{?}{=} A_2$
Generates RN_{MU}
Computes
$RID_{MU} = A_3 \oplus h(r_{MU}||HPW_{MU})$
$K_{MUG} = A_4 \oplus h(RID_{MU}||HPW_{MU})$
$M_1 = h(PID_{MU}||RID_{MU}||K_{MUG}) \oplus (RN_{MU}||PID_{SD})$
$C_1 = h(ID_{MU}||RN_{MU}) \oplus h(K_{MUG}||RN_{MU})$
$V_{MU} = h(PID_{MU}||RID_{MU}||RN_{MU}||PID_{SD}||K_{MUG})$
$\xrightarrow{\{PID_{MU}, M_1, C_1, V_{MU}\}}$

Retrieves RID_{MU} and K_{MUG} corresponding to PID_{MU}
$(RN_{MU}^{*}||PID_{SD}^{*}) = M_1 \oplus h(PID_{MU}||RID_{MU}||K_{MUG})$
$V_{MU}^{*} = h(PID_{MU}||RID_{MU}||RN_{MU}^{*}||PID_{SD}^{*}||K_{MUG})$
Checks $V_{MU}^{*} \overset{?}{=} V_{MU}$
Retrieves K_{GSD} and r_{SD} corresponding to PID_{SD}
Generates RN_G
Computes
$M_2 = h(RN_{MU}||RN_G)$
$M_3 = h(PID_{SD}||K_{GSD}||r_{SD}) \oplus M_2$
$h(ID_{MU}||RN_{MU}) = C_1 \oplus h(K_{MUG}||RN_{MU})$
$C_2 = (h(ID_{MU}||RN_{MU})||h(ID_G||RN_G)) \oplus h(K_{GSD}||r_{SD})$
$V_{MUG} = h(PID_{MU}||M_2||K_{GSD})$
$\xrightarrow{\{PID_{MU}, M_3, C_2, V_{MUG}\}}$

Computes
$r_{SD} = B_1 \oplus h(ID_{SD}||K_{SD})$
$K_{GSD} = B_2 \oplus h(r_{SD}||K_{SD})$
$M_2^{*} = M_3 \oplus h(PID_{SD}||K_{GSD}||r_{SD})$
$V_{MUG}^{*} = h(PID_{MU}||M_2^{*}||K_{GSD})$
Checks $V_{MUG}^{*} \overset{?}{=} V_{MUG}$
Generates RN_{SD}
Computes
$(h(ID_{MU}||RN_{MU})||h(ID_G||RN_G)) = C_2 \oplus h(K_{GSD}||r_{SD})$
$SK = h(h(ID_{MU}||RN_{MU})||h(ID_G||RN_G)||h(ID_{SD}||RN_{SD}))$
$M_4 = h(PID_{SD}||K_{GSD}||r_{SD}) \oplus h(ID_{SD}||RN_{SD})$
$V_{SD} = h(PID_{MU}||PID_{SD}||M_2^{*}||h(ID_{SD}||RN_{SD})||K_{GSD})$
$\xleftarrow{\{M_4, V_{SD}\}}$

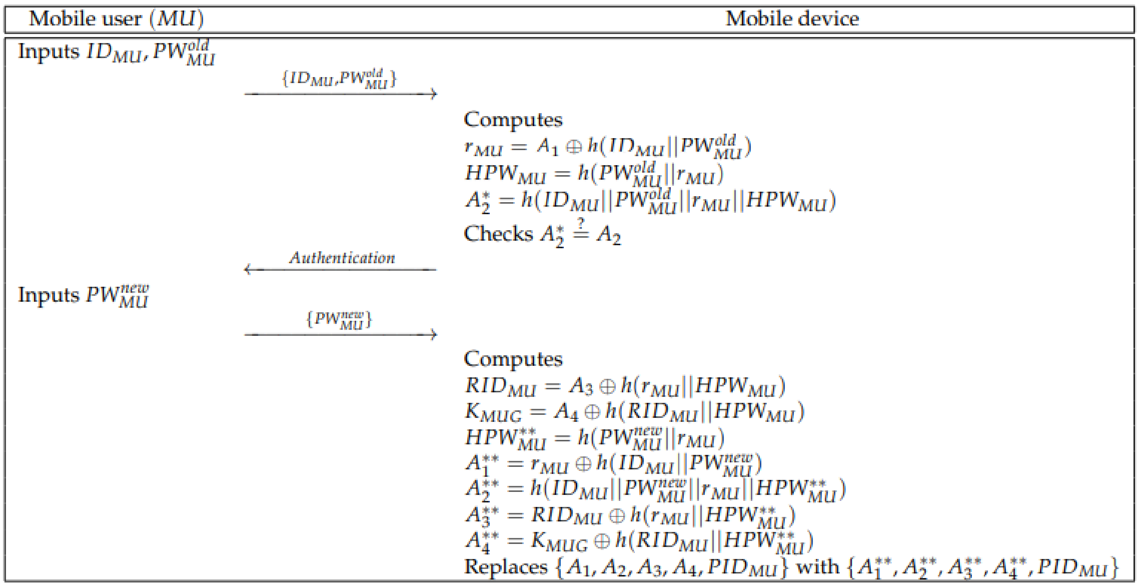
Computes
$h(ID_{SD}||RN_{SD}) = M_4 \oplus h(PID_{SD}||K_{GSD}||r_{SD})$
$V_{SD}^{*} = h(PID_{MU}||PID_{SD}||M_2||h(ID_{SD}||RN_{SD})||K_{GSD})$
Checks $V_{SD}^{*} \overset{?}{=} V_{SD}$
Computes
$SK = h(h(ID_{MU}||RN_{MU})||h(ID_G||RN_G)||h(ID_{SD}||RN_{SD}))$
$PID_{MU}^{new} = h(PID_{MU}||RN_{MU})$
$RID_{MU}^{new} = h(PID_{MU}^{new}||K_{MUG})$
$M_5 = h(RID_{MU}||RN_{MU}) \oplus (h(ID_G||RN_G)||h(ID_{SD}||RN_{SD})||PID_{MU}^{new})$
$V_{GSD} = h(PID_{MU}||RN_{MU}||h(ID_G||RN_G)||h(ID_{SD}||RN_{SD})||PID_{MU}^{new}||K_{MUG})$
Stores $\{PID_{MU}, RID_{MU}\}$ with $\{PID_{MU}^{new}, RID_{MU}^{new}\}$ in HGW's database
$\xleftarrow{\{M_5, V_{GSD}\}}$

Computes
$PID_{MU}^{new} = h(PID_{MU}||RN_{MU})$
$(h(ID_G||RN_G)||h(ID_{SD}||RN_{SD})||PID_{MU}^{new}) = M_5 \oplus h(RID_{MU}||RN_{MU})$
$V_{GSD}^{*} = h(PID_{MU}||RN_{MU}||h(ID_G||RN_G)||h(ID_{SD}||RN_{SD})||PID_{MU}^{new}||K_{MUG})$
Checks $V_{GSD}^{*} \overset{?}{=} V_{GSD}$
Computes
$SK = h(h(ID_{MU}||RN_{MU})||h(ID_G||RN_G)||h(ID_{SD}||RN_{SD}))$
Updates
$RID_{MU}^{new} = h(PID_{MU}^{new}||K_{MUG})$
$A_3^{new} = RID_{MU}^{new} \oplus h(r_{MU}||HPW_{MU})$
$A_4^{new} = K_{MUG} \oplus h(RID_{MU}^{new}||HPW_{MU})$
Replaces $\{A_3, A_4, PID_{MU}\}$ to $\{A_3^{new}, A_4^{new}, PID_{MU}^{new}\}$ in the mobile device
Computes
$M_6 = h(SK||PID_{MU}^{new})$
$\xrightarrow{\{M_6\}}$

Computes
$M_6^{*} = h(SK||PID_{MU}^{new})$
Checks $M_6^{*} \overset{?}{=} M_6$
If it is correct, deletes $\{PID_{MU}, RID_{MU}\}$ in the database

Figure 5.3: Authentication and key agreement phase [42]

4. **password update:** In this phase, users can update their passwords individually. Users have to send their ID and the old password through a secure channel to mobile devices. Then the mobile device will compute a random number for the user and will do some computation to verify whether the information received is correct or not. If the information provided is accurate, the mobile device will send an authentication message to the user. Then, the user will be able to update their password, and the mobile device will then replace old passwords with the new ones entered. This phase is illustrated in figure 5.4



Mobile user (MU)

Mobile device

Inputs ID_{MU}, PW_{MU}^{old}

$\xrightarrow{\{ID_{MU}, PW_{MU}^{old}\}}$

Computes
$r_{MU} = A_1 \oplus h(ID_{MU}||PW_{MU}^{old})$
$HPW_{MU} = h(PW_{MU}^{old}||r_{MU})$
$A_2^* = h(ID_{MU}||PW_{MU}^{old}||r_{MU}||HPW_{MU})$
Checks $A_2^* \overset{?}{=} A_2$

$\xleftarrow{Authentication}$

Inputs PW_{MU}^{new}

$\xrightarrow{\{PW_{MU}^{new}\}}$

Computes
$RID_{MU} = A_3 \oplus h(r_{MU}||HPW_{MU})$
$K_{MUG} = A_4 \oplus h(RID_{MU}||HPW_{MU})$
$HPW_{MU}^{**} = h(PW_{MU}^{new}||r_{MU})$
$A_1^{**} = r_{MU} \oplus h(ID_{MU}||PW_{MU}^{new})$
$A_2^{**} = h(ID_{MU}||PW_{MU}^{new}||r_{MU}||HPW_{MU}^{**})$
$A_3^{**} = RID_{MU} \oplus h(r_{MU}||HPW_{MU}^{**})$
$A_4^{**} = K_{MUG} \oplus h(RID_{MU}||HPW_{MU}^{**})$
Replaces $\{A_1, A_2, A_3, A_4, PID_{MU}\}$ with $\{A_1^{**}, A_2^{**}, A_3^{**}, A_4^{**}, PID_{MU}\}$

Figure 5.4: Password update phase [42]

5.2 Homomorphic Encryption

Homomorphic Encryption is an encryption technique where the data can be computed while in its encrypted state. This allows a user to encrypt their data, send it and have a third party compute the data without having the ability to read it, thereby upholding the confidentiality of the data. The user can then be sent the resulting data (still encrypted) and decrypt it to be able to read the results[41]. The results from the encrypted data are the same as if the computations were done in plaintext[44].

Homomorphic Encryption can be divided into three main groups depending on what operations can be performed on the encrypted data.

- Partially Homomorphic Encryption (PHE) PHE can only be used for algorithms that only use addition or multiplications, but the amount of times the calculation can be used is unlimited[1].
- Somewhat Homomorphic Encryption (SWHE) SWHE can be used when both addition and multiplication are needed. However, the number of times the calculations can be done is limited because the cipher text increases with each homomorphic operation[1].
- Fully Homomorphic Encryption (FHE) FHE can both be used for addition and multiplication and support an arbitrary number of calculations[1]. FHE comes with the problem of having a higher operations cost than the two other groups.

Homomorphic Encryption increases privacy compared to normal Advanced Encryption Standard (AES) encryption as AES encryption could only be used for data transition but not during operations.

In the article, "Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges[44]" a comparison is made for different Encryptions based on: Size, Privacy, Possible operations, Complexity, and Execution time.

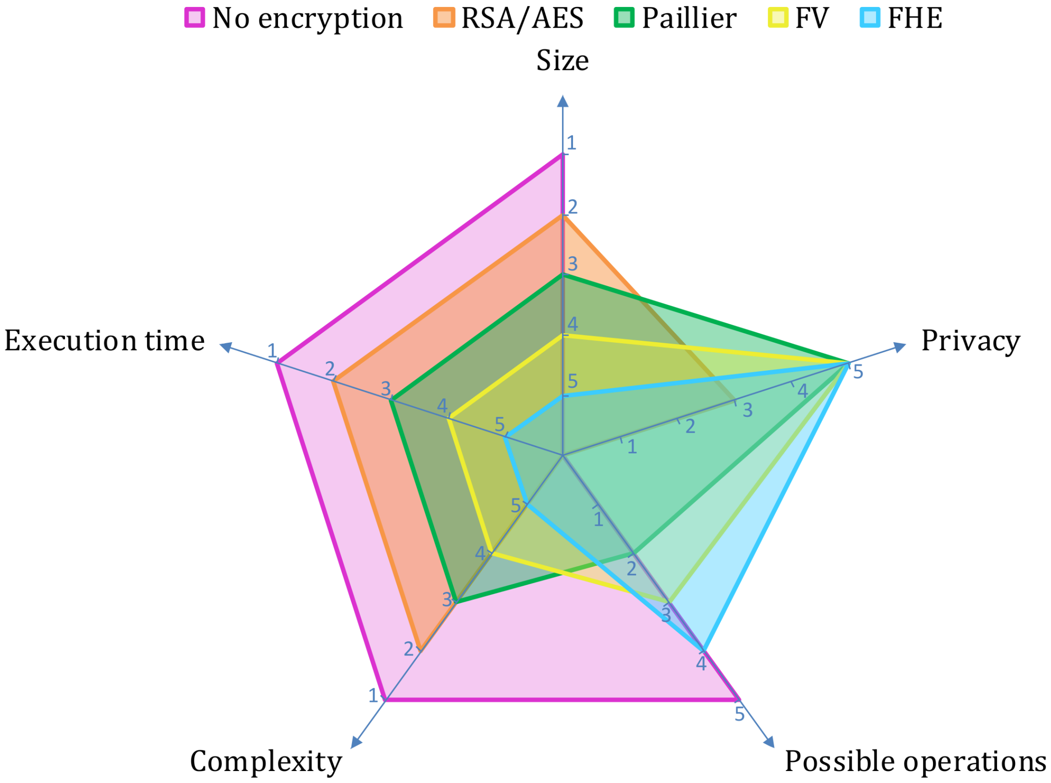


Figure 5.5: Comparison of different encryption techniques [44]

Fan and Vercauteren (FV) is a SHE algorithm, and Paillier is equivalent to PHE.

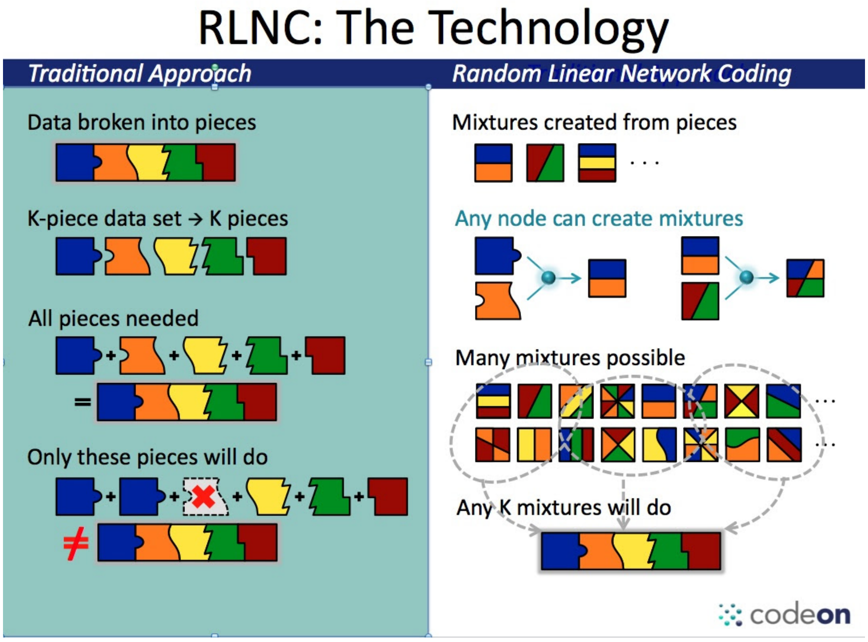
As shown, all the different Homomorphic Encryptions have the same level of privacy. The difference between the HEs comes in all the other metrics. HE can give a higher level of privacy than AES and goes from 0 to several possible operations. The execution time is an area where the Homomorphic Encryptions fall short with the high computational cost compared to all the other methods, with the Fully Homomorphic Encryption being the most costly. HEs also struggle with the ciphertext size, as shown in the figure 5.5.

Homomorphic Encryption in a smart home can be used to send personal data to a third party and have them perform computations on the encrypted data. This could be done for several reasons; the third party has more computational power, and the third party may combine several pieces of data from different devices. For example, the third party may be your phone, a computer, or a cloud service.

5.3 Random Linear Network Coding

Homomorphic Encryption extends the cipher texts, thereby increasing the messages having to be sent. However, network Coding (herby abbreviated to NC) works on cutting down on the network traffic. This section will focus more specifically on the NC scheme, Random Linear Network Coding (RLNC)[44].

In a classical store-and-forward route, the message is broken down into smaller blocks before being sent. RLNC differs in that it does not send the broken blocks of the message after. Instead, RLNC takes the broken blocks and blends them using an algorithm into coded packets. Then, several groups of mixed packets can be used to recombine the original data. Using the standard method, the packets would all have to come in the correct order, and if n packet is missing, n packet is the one that must be received through new sendings. However, if RLNC lost a packet, it would have more packets that could be sent again and still recover the original data. This makes RLNC impervious to the coupon collector problem[44]. As RLNC can use a different packet than the lost one, it can have a small number of extra packets sent when sending the data the first time. This would lead the message not to be sent from the start again as it would have to with the traditional approach. The strain on the bandwidth would be lowered, and latency will decrease.



RLNC: The Technology

Traditional Approach

Data broken into pieces

K-piece data set → K pieces

All pieces needed

Only these pieces will do

Random Linear Network Coding

Mixtures created from pieces

Any node can create mixtures

Many mixtures possible

Any K mixtures will do

Figure 5.6: Explanation of RLNC from[12]

Figure 5.6 shows the data is broken up into pieces and mixed. And how they can be combined back into the original data using several different combinations.

RLNC (and by extension NC) has one significant security flaw, which is vulnerable to pollution attacks[58]. However, this can be solved by using homomorphic encryption. Another problem with RLNC is that as it needs to mix the pieces, it requires extra computational power before it can send the message.

5.4 Securing the Gateway in Smart Home Using Blockchain

The gateway used to control and monitor the SH is a network that enables multiple devices to communicate with one another. This could expose the data collected by these devices to unauthorized individuals. This could cause users' privacy to be violated, and it could cause device malfunctions. In addition, without security standards, the various services that are available to users through the SH will not be able to be seamlessly integrated. This is why the various security measures that are required for the gateway must be implemented [35].

Confidentiality, integrity, and authentication are some security requirements for gateways in a SH [35].

- **Confidentiality:** SH networks collect and retain various data, including sensitive information about users. Access to this data should be restricted to only authorized individuals. To ensure that this information is secure, blockchain technology can be conducted.
- **Integrity:** No falsification must occur during data transfer when data is transmitted and received between each configuration. The hash function decreases the probability of this data being falsified and enables the monitoring and verification of precisely what information is collected.
- **Authentication:** Authentication in SH network configurations prevents an outside attacker from doing harmful actions inside a conventional network. Blockchain can be used to verify that the network is a legitimate member and may take advantage of the ability to check it at a specific moment to enable the proper configuration of the SH network.

The use of blockchain technology in SH gateways is critical to ensuring the integrity and security of data being sent between devices. As a centralized network, the SH network may be adapted to a distributed network by utilizing blockchain at the cloud layer [35]. A SH gateway based on blockchain comprises three layers: the device layer, the gateway layer, and the cloud layer. The device layer includes sensors and devices that monitor and collect data in the network environment. The device layer's data is stored in the gateway layer, providing it to users as needed. The gateway's ID and the data processed by each gateway are registered in the blockchain at the cloud layer's third layer. Users may access information at any time and from any location, thanks to the sharing of blocks [35]. The figure 5.7 illustrates how it is supposed to be.

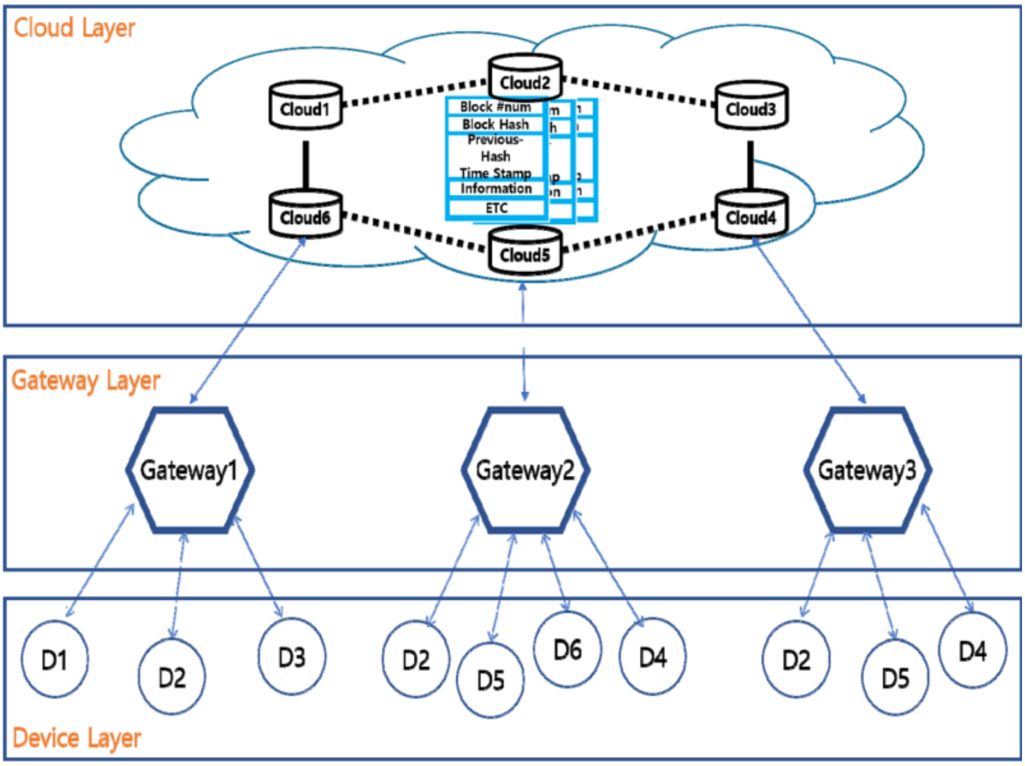


Figure 5.7: A smart home gateway based on Blockchain [35]

Figure 5.8 depicts the suggested architecture's flowchart proposed in [35], which enables data from devices at the end to be gathered, registered in the blockchain, and suitably displayed to users. To gather and transmit data to the user, the acquired data goes through hash value processing, and formatting creates blocks and verifies them regularly to ensure integrity even if data falsification happens. Continuous data analysis and quality maintenance are required to provide relevant information.

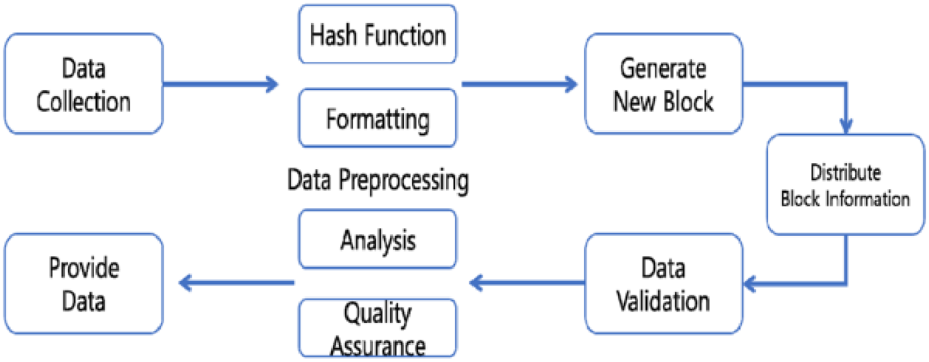
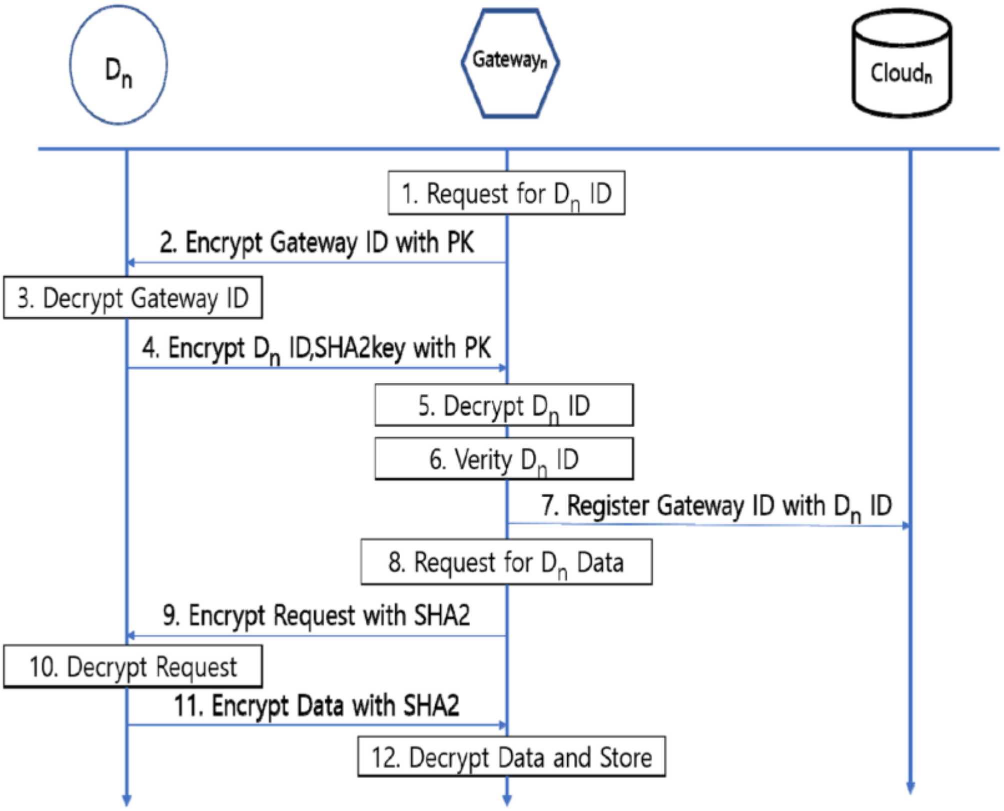


Figure 5.8: Flow of blockchain for smart home gateway [35]

5.4.1 Data Collecting And Identifying Gateway Devices

SM IoT devices are linked to a single gateway, where each connected device grants its unique ID. As a result, the devices and gateways can perform encryption and decryption operations using public-key infrastructure (PKI) and Secure Hash Algorithm 2 (SHA-2) [35]. The proposed processes for device and gateway registrations protocol are illustrated in the figure 5.9 below.



D_n
Gateway_n
Cloud_n
1. Request for D_n ID
2. Encrypt Gateway ID with PK
3. Decrypt Gateway ID
4. Encrypt D_n ID,SHA2key with PK
5. Decrypt D_n ID
6. Verity D_n ID
7. Register Gateway ID with D_n ID
8. Request for D_n Data
9. Encrypt Request with SHA2
10. Decrypt Request
11. Encrypt Data with SHA2
12. Decrypt Data and Store

Figure 5.9: Device Identification and data collection [35]

1. In the first message, the Gateway sends an ID request for the connected devices.
2. Then, the gateway encrypts its ID with the help of the pre-shared key between the gateway and the device D_n and sends it to D_n.
3. In the third message, D_n decrypts the received message from the gateway, which contains the gateway's ID and requests.

4. In the following message, the device D_n computes its ID and encrypts it along with the SHA-2 key. Then, the message is sent to the gateway.

5. In the fifth and sixth message, the gateway decrypts the message received from the device D_n then verifies the device ID.

6. In the following message, the gateway sends and stores the verified ID of D_n in the cloud. Additionally, the gateway and the cloud communicate periodically to update registered devices' IDs.

7. In the eighth and ninth message, the gateway sends a data request to device D_n. The requested data are data that have been collected from the devices. Then, the gateway encrypts its request with the hash algorithm SHA-2 and sends it to D_n.

8. Next, in the tenth and eleventh message, the device D_n decrypts the message received from the gateway. Then, the device D_n replays to the request with its data encrypted with SHA-2 and sends it to the gateway.

9. In the final message, the gateway decrypts the message received from device D_n, which contains the data collected from the device. Then, the gateway stores the decrypted data from D_n.

5.4.2 Blockchain Based Gateway Data Management

A blockchain-based network ensures the integrity of the transmitted and stored data. The data generated by the network's end nodes can be stored using the SHA-3 algorithm. This method is based on the necessary information generated by the end nodes. Cloud-based blockchain then compares those blocks in real-time and verifies data by checking if there is a tampered block in the chain [35]. The processes of monitoring and registering gateway data that are sent and received through a blockchain can be illustrated in figure 5.10.

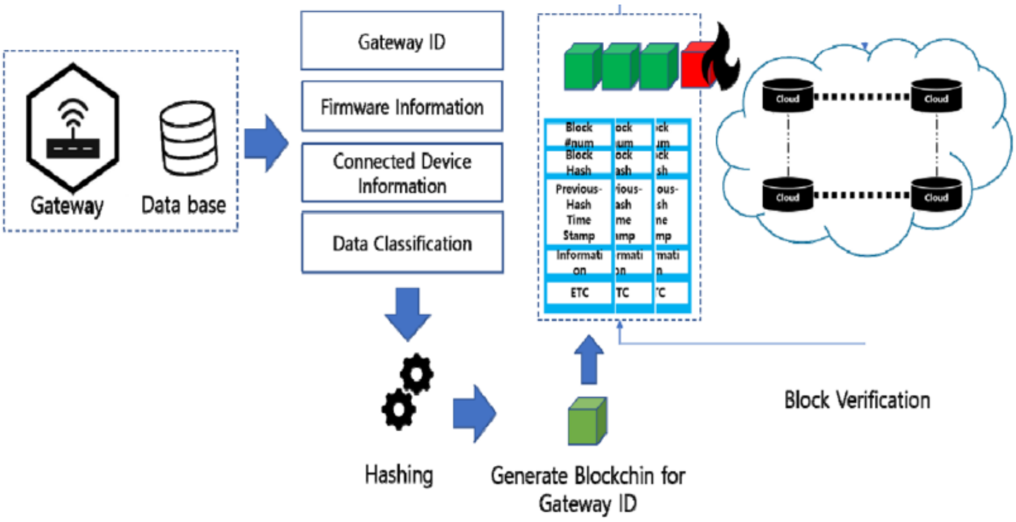


Figure 5.10: Gateway data management using blockchain [35]

5.4.3 Preprocessing Data Inside The GW

The data collected from various IoT devices in the SM is sent to the GW, then processed based on users' needs. Figure 5.11 illustrates the data transfer process from smart devices to the gateway, where the process is divided into three various categories; **Collection, Preprocessing, and Hashing** [35].

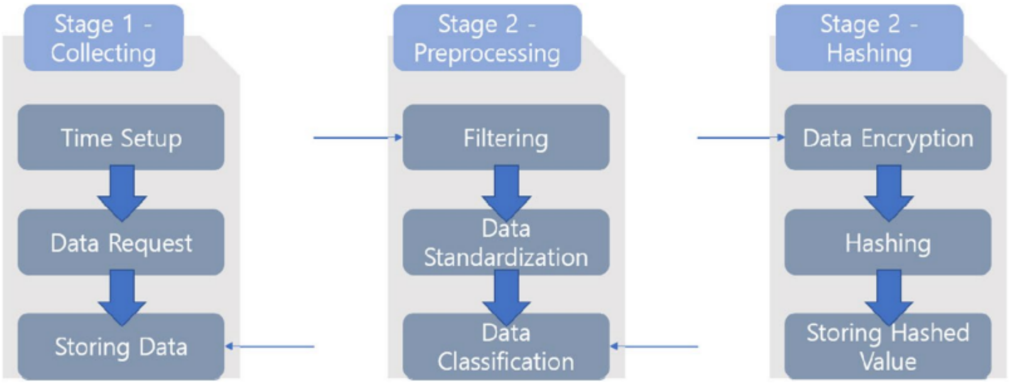


Figure 5.11: Preprocessing GW's data [35]

- **Collecting:** The device's data is sent and received by the router for a particular time. Whenever new information is required, it is requested from the device. This data is then stored at the GW in the device's storage.

- **Preprocessing:** The data sent from the device is pre-processed inside the GW. Then, for optimal storage space, it stores and filters the data required by the router. This process is carried out using the classification and standardization procedures.

- **Hashing:** Encryption can be used to protect users' private information collected in the SM. The SHA-256 algorithm can be used depending on the user's password, and the hash function can be used to save the device's common data.

Chapter 6

Discussions

This chapter will discuss the results found through the PIA/DPIA and methods for increasing Privacy. Challenges faced during the work on the thesis and possible future work are also discussed.

6.1 Results

Architecture and DFDs

When we made the smart home architecture, we deliberately made it not interact with any third party or cloud service to compute the data. This was done as we wanted a privacy-focused smart home. Another reason was that it would be more viable to keep business and legal aspects out of scope. However, not including third parties and cloud services, the way we did may not necessarily represent all smart homes.

6.1.1 Information Gathered

As shown in the PIA tables B.1 the PIA, several types of information are gathered, some types were the same across all of the smart devices, and each of the devices also had its specific types of information collected. Therefore, we created a table that combined the common information types among the smart appliances in our smart home.

Common information types from B.1

Common information types	
Information type	Sensitivity level
Account number	Moderate
Device Serial number	Moderate
Account login email	Low
Account login password	High
Name, address, phone number	High
Usage pattern	High
Device Settings	Moderate

As shown in figure 6.1, smart appliances collect and generate several highly sensitive personal information types. In addition, the individual smart appliances also generated high sensitive PI, such as voice recordings in the smart fridge.

6.1.2 Privacy Impact Assessment

We have shown a way to perform a privacy impact assessment. First, we designed a smart home architecture for our case. This included listing the devices' functions and creating a data flow diagram to show how the data would have to flow for the functions to work. The DFD helped immensely investigate what personal information is gathered in the smart home. If a PIA is to be done on a smart house already in active use, the steps would differ somewhat but remain the same. The architecture should be noted down with the DFD. Finding what information is gathered would also be easier as the user could perform data subject requests on the parties collecting information (usually the manufacturer). This would lead to a more accurate PIA.

6.1.3 Privacy For End-User

Homomorphic Encryption

Homomorphic Encryption can be used to move some of the work assignments to other devices. This could be having a smart appliance giving a home server a task, or we could use cloud computations. It would not matter where we send the data to be computed as the information is encrypted. It is important to remember that sending information at set time slots each day could give away a user pattern; this again could be alleviated by sending work to be done at set times even when not using the device. Another way is functions that are not time-critical being done at random intervals. Such as changing the settings of a smart device based on the usage pattern the device has logged.

Not all functions of smart home appliances need to be done in real-time. An example would be a change of settings caused by user routines. These functions are examples of where the computational cost would not hinder the function. Homomorphic Encryption should be used in functions where it is preferable to transfer the operations of personal data without the operating party having access to the data in plaintext. Furthermore, the function should not be time-sensitive.

Homomorphic Encryption with RLNC

Homomorphic Encryption comes with some downsides, such as having longer cipher texts that can clog the home network and increase latency for sending. This is why we also recommend using RLNC. In addition, RLNC can send some extra blocks in the first sending to avoid having to repeat messages if a middle block is lost. This would help decrease the network traffic and latency of sending packages. Finally, homomorphic encryption also works to protect RLNC from pollution attacks.

Authentication Protocol

The authentication protocol can ensure that the communication between the smart devices and users is secure in a smart home environment. Authentication means verifying whether a claimed identity is true or not. The reason for choosing authentication protocol is to ensure that mutual authentication and data integrity is preserved and unauthorized individuals do not gain access and tamper with the data transmitted in the smart home. Since this protocol is based on the session key, the adversary might want to get the exchanged messages between, for instance, the user and the smart devices. However, the adversary will be passive since they can only record the exchanged messages and do not possess the shared session key between the parties. The characteristic of the session key is that in each session, both parties who want to communicate must generate a new key and forget it after it has been used. In addition, the session keys have a typically shorter lifetime; it might be two minutes. However, if the adversary somehow gets the session key, only two minutes' worth of data can be decrypted. Therefore, we believe that this protocol provides **Perfect Forward Secrecy** (PFS).

Securing The Gateway Using Blockchain

The gateway in the smart home is the connection between the devices. The centralized characteristic of the gateway in the smart home makes it vulnerable. The reason for choosing blockchain to secure the gateway in the smart home is that it provides a decentralized solution that does not rely on a centralized intermediary. Moreover, the blockchain solution was chosen to ensure the integrity of transmitted or stored data. It compares the blocks in the chain in real-time and verifies data by checking if there is a tampered block in the chain. Although the proposed solution minimizes the threats regarding integrity, authentication, and confidentiality in the smart home, it has some limitations due to the computational complexity.

6.2 Challenges

The thesis was initially supposed to be on privacy in telehealth. The original plan was to look at smart devices used by patients at home, such as cardiac monitoring and sleep apnea breathing machines. We interviewed people who worked in the technical parts of hospitals, sykehuspartner (responsible for facilitating communication between devices and hospitals), and one developer of cardiac monitoring monitors. Unfortunately, the project had to change course when we could not gather information from other developers, doctors, or medical personnel who directly worked with the devices. The choice was made to move away from telehealth and into smart homes as smart homes contained significantly more public research relevant to privacy. We learned much from the telehealth research and interviews, and we were able to use and take ideas from into the smart home.

Another challenge we met was during the usage of the CyberComply DPIA tool. The tool was supposed to be used for completing a Privacy Risk Assessment as part of the DPIA. Unfortunately, this part did not work. A significant amount of time was spent finding any fault; however, the fault lay with the CyberComply. So this aspect of the DPIA was unable to be done. A second tool (risk analysis) from CyberComply was used to set a simple privacy risk analysis. The tool we meant to use would be supposed to make threat scenarios; however, we had all the threats, vulnerabilities, and subsequent controls.

6.3 Future Work

Some future work that could be done to improve on the smart house privacy

- Protocols: Several articles indicated that Homomorphic encryption and Blockchain could be used together to increase the privacy-preserving in a smart home. Due to the time, we could not include that part in our research.

- Use available smart appliances: A more accurate life architecture would be made if the smart appliances were replaced with available smart devices from the store. This would most likely lead to differences in the personal information gathered. The data flow would also most likely differ. However, we believe that our suggested methods for increasing privacy would still be applicable.
- Create a working environment using the suggested methods for increasing privacy: A smart home environment could be created to test the methods more practically. This environment could be just a simulation or a physical setup with available or specially made smart appliances. Such an environment would further prove the usefulness of the suggested methods.
- Find needed increase of computational power. All of the methods we provided increased the computational cost of the smart appliances. Therefore work could be done to ensure that the devices can handle the work they are set to do.
- Include business aspects and legal aspects: as discussed in 1.3, business and legal aspects of the smart home and PIA were considered out of scope. Therefore, these aspects should be assessed by someone with more expertise in business and legal affairs.

Chapter 7

Conclusion

In our case description, we have chosen three research questions. The first research question is:

- **What types of personal information are generated and exchanged in the environment?**

We first illustrated a smart home architecture with four various connected devices to answer this question. Then, data Flow Diagrams (DFDs) were made to demonstrate the flow of personal information and show what information is considered exposed to privacy threats. The PI types were PI from account creation (mixed sensitivity) and user patterns generated from smart appliances (highly sensitivity).

The second research questions is;

- **How can we do a privacy impact assessment on a smart home environment?**

We have used three different methods when doing a PIA. The work on the PIA is based on the architecture and DFD diagrams we designed. The first method analyzed the selected devices and created tables containing the information types generated with their origin, sensitivity levels, and who uses them. The second one was to use a template with questionnaires where the answers were based on the devices. The third method was using a PIA tool, namely Cybercomply. In this method, more questionnaires were answered, and most of the questions were the same as those we already answered in the second one. Moreover, we chose the PIA tool to compare our self-made PIAs to ensure our work was correct.

The third research question is;

- **How can we provide better privacy guarantees for end-users in a smart home environment?**

We have researched different technologies and presented the ones found relevant to this case. We have discussed developing methods and their solutions with pros and cons. Finally, we have shown how the solutions could increase privacy for end-users in smart homes at a computationally expensive cost. The technologies we presented were homomorphic encryption, RLNC, authentication protocols, and securing the gateway using Blockchain.

The main takeaway from this project is that IoT entirely changes how people live. It does this by interconnecting the device in a home, making it a smart home. The interlinked home can make the owner's life easier and highly enjoyable. Nevertheless, it comes with its challenges. For example, much sensitive personal information is generated, gathered, sent, and computed for smart devices to perform their functions. This needs more awareness, and we hope that through this report, we have helped show the sensitive information gathered and how to develop the smart home ecosystem further to protect the end-users privacy.

Appendix A

Data Flow Diagrams

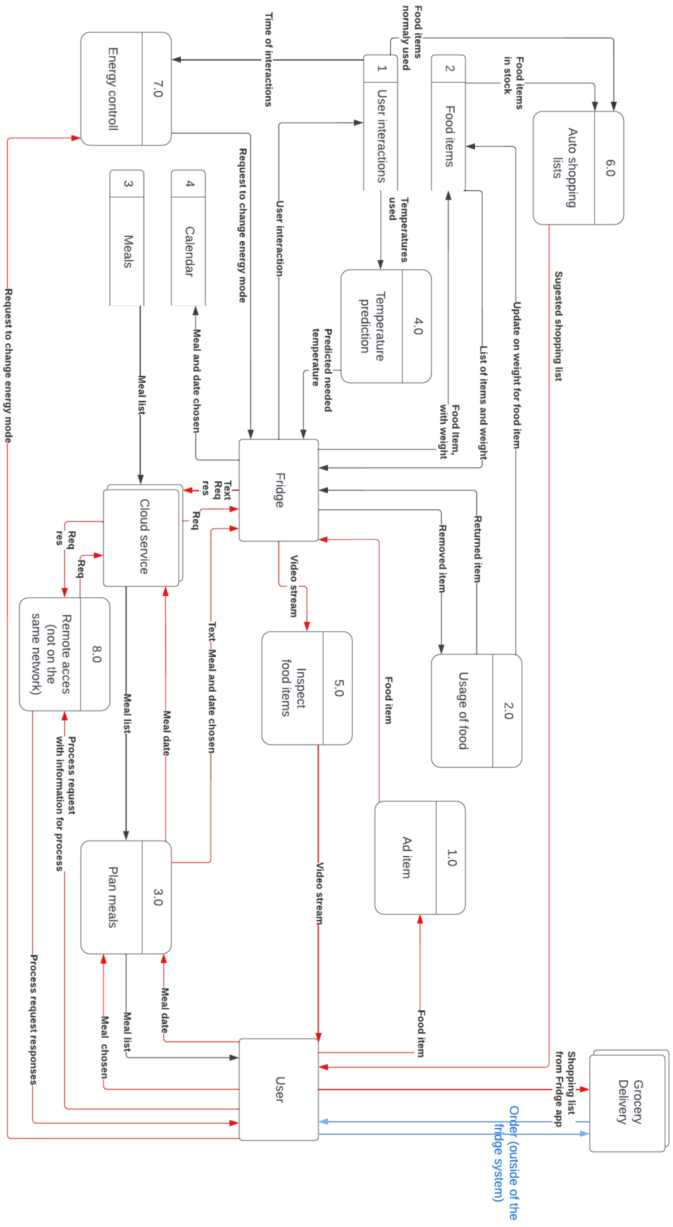


Figure A.1: Fridge DFD

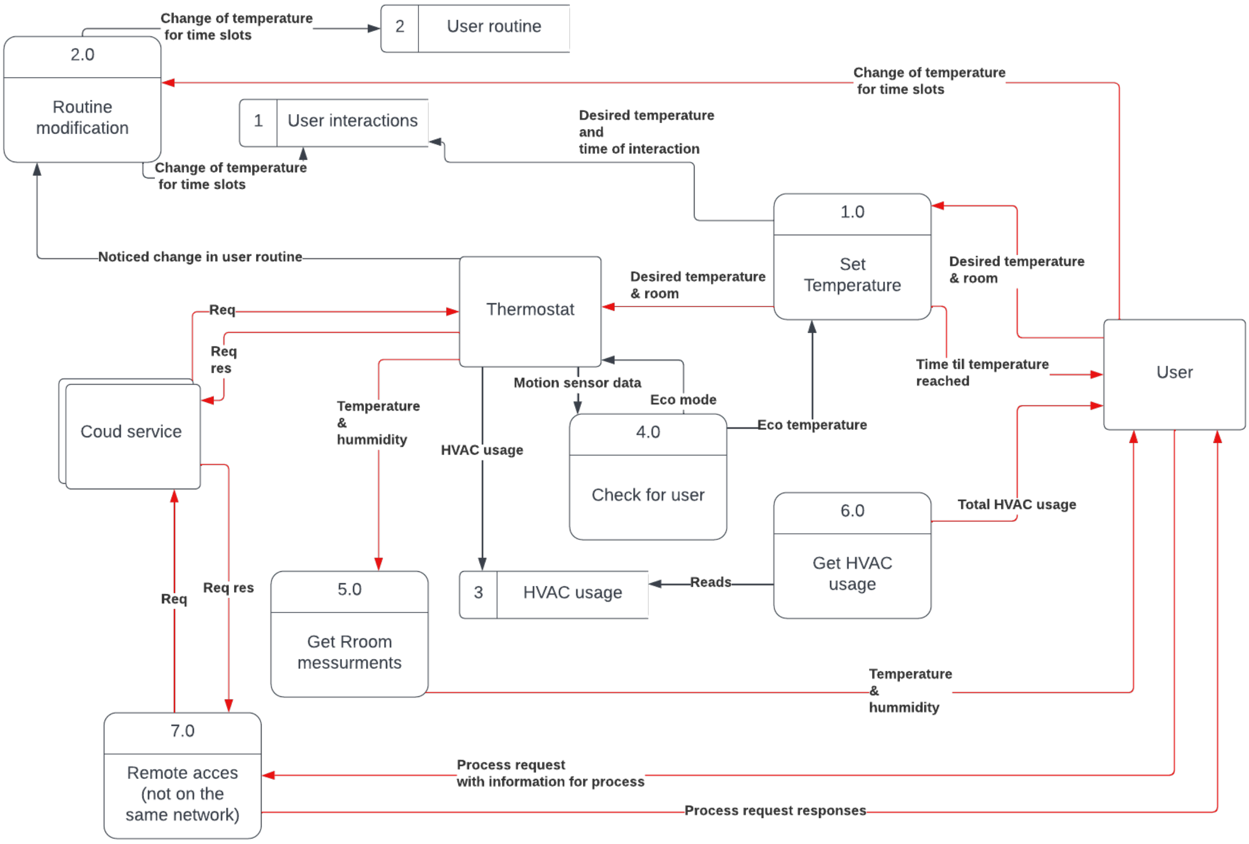


Figure A.2: Thermostat DFD

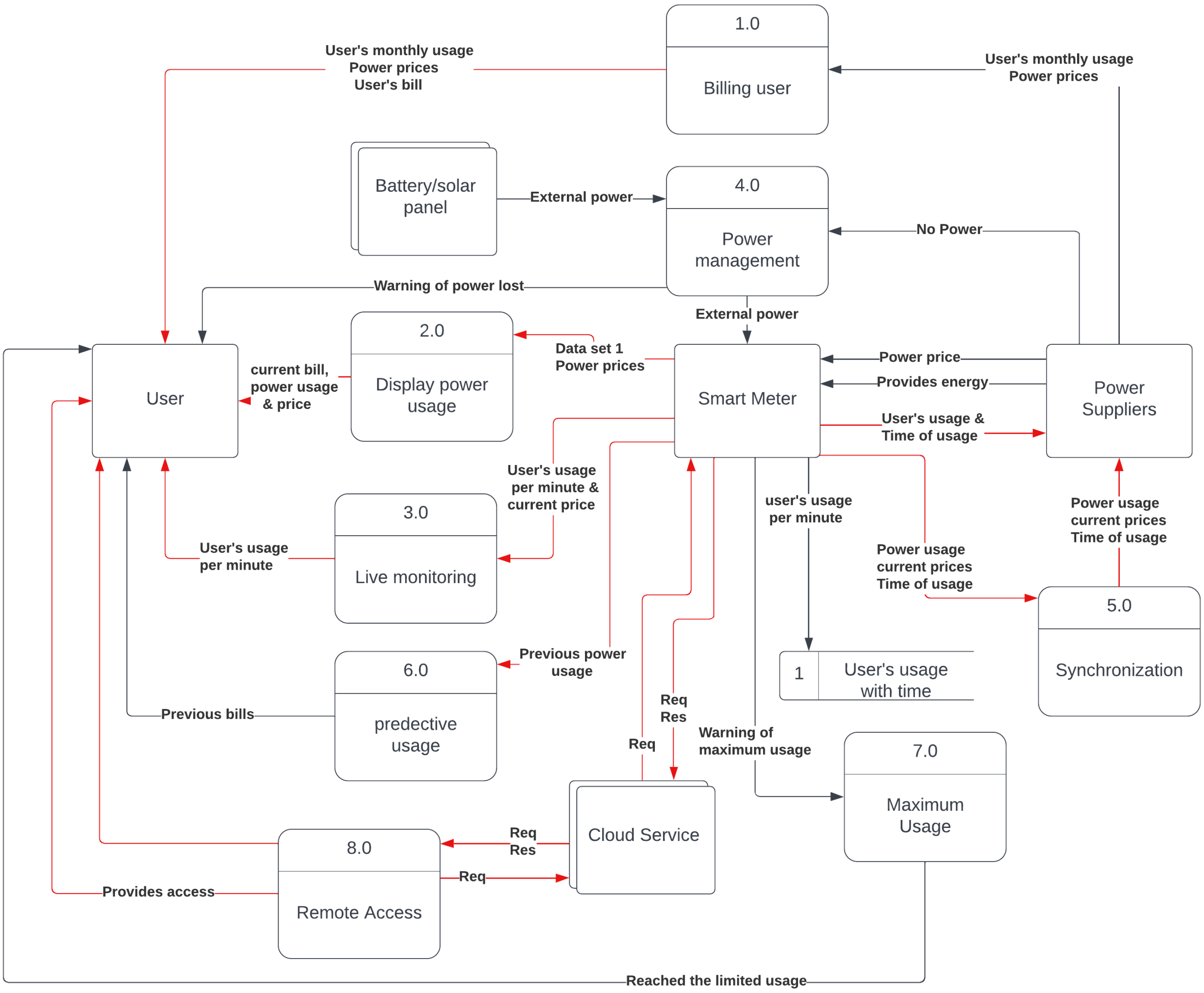


Figure A.3: Smart Meter DFD

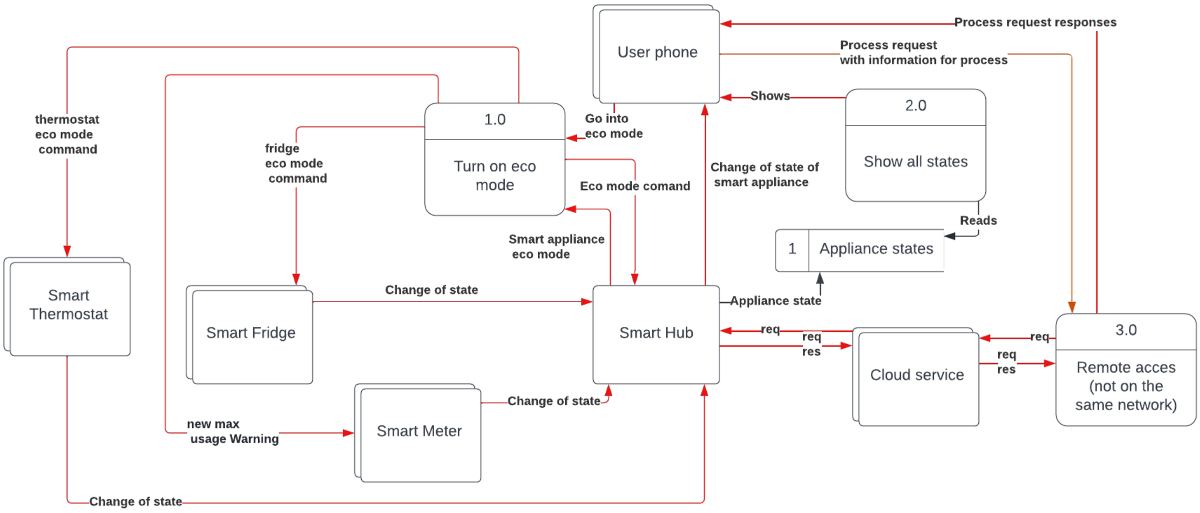


Figure A.4: Smart Hub DFD

Appendix B

Manual PIAs

B.1 PIA Tables

B.2 Smart Fridge

PIA of smart Fridge

User Account			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	Unique account number **(Low Sensitivity)**	Created by the account server when an account is registered.	User, Smartphone app, Fridge
Fridge Serial number	Unique identifier for the fridge **(Low sensitivity)**	Manufacturer	Fridge owner, Application server, Smartphone app
Account login	User identifier email **(Low sensitivity)**	Created by user	Fridge Smartphone app Shopping app User

Name, address, phone number	Owners (Name, address, phone number) **(High sensitivity)**	Fridge Owner	Smartphone app Shopping app

PIA of smart fridge

Daily Usage			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Voice recording	Voice recorded of user saying food items added to fridge. **(High sensitive)**	User Phone app	Smartphone app Fridge
Transcribed App microphone data	Voice to text data from user talking to phone. **(High sensitive)**	User talk to phone, transcription engine	Fridge Smartphone app
Usage pattern	User pattern from usage of the fridge and app **(High sensitivity)**	User, Smartphone app, Fridge	User, Smartphone app, Fridge
Fridge settings	Day to day settings to the fridge made by the user using the smartphone app. (Moderate sensitivity)	Fridge owner	User, Smartphone app, Fridge
Food list	List of food items in the fridge. **(Moderate sensitivity)**	Fridge owner Smartphone app	User, Smartphone app, Fridge
Food usage logs	Logs on when and how much of a food item was used **(High sensitivity)**	Fridge, User	User, Smartphone app, Fridge
Meal plan	Meal plan includes meal, date and ingrediences needed. **(High sensitivity)**	Fridge, User	User, Smartphone app, Fridge

PIA of smart fridge

Fridge connection			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	Unique account number **(Moderate Sensitivity)**	Account setup	Fridge Smartphone app
Fridge Serial number	Unique identifier for the fridge **(Moderate Sensitivity)**	Fridge manufacturer	Fridge Smartphone app

B.3 Smart Thermostat

PIA of smart Thermostat

User Account			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	Unique account number **(Low Sensitivity)**	Created by the account server when an account is registered.	User, Smartphone app, Thermostat
Thermostat Serial number	Unique identifier for the Thermostat **(Low sensitivity)**	Manufacturer	Thermostat owner, Application server, Smartphone app
Account login	User identifier email **(Low sensitivity)**	Created by user	Thermostat Smartphone app User
Password	User Password **(High sensitive)**	Created by user	Thermostat Smartphone app User
Name, phone number	Owners (Name, phone number) **(Moderate sensitivity)**	User	Smartphone app Thermostat

PIA of smart Thermostat

Thermostat daily usage			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Temperature settings	Temperature settings for each room and time. **(High sensitive)**	User, Thermostat	Thermostat Smartphone app User
Thermostat settings	Day to day settings set by the user or by Thermostat self-learning **(Moderate sensitivity)**	User, Thermometers self-learning	Thermostat Smartphone app User
Sensor data	Sensor data on users in rooms. **(High sensitivity)**	User Thermostat	Thermostat Smartphone app User
Thermostat sensor data	Temperature and humidity sensor data in different rooms. **(Moderate sensitivity)**	Thermometer	Thermostat Smartphone app User
Usage patterns	User pattern from usage of the Thermostat and app **(High sensitivity)**	User, Thermometer	Thermostat Smartphone app User

PIA of smart thermostat

Thermostat connection			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	Unique account number **(Moderate Sensitivity)**	Account setup	Thermostat Smartphone app
Thermostat Serial number	Unique identifier for the Thermostat **(Moderate Sensitivity)**	Thermostat manufacturer	Thermostat Smartphone app

B.4 Smart Meter

PIA of smart meter

User account			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Login	User identifier **(Not sensitive)**	Created by user	User Billing server Web-portal App server
Password	User password **(High sensitive)**	Created by user	User User Billing server Web-portal App server
Name, address, phone number	account holder's details (name, address, phone number) **(High sensitive)** can be combined with payment methods	SM owner	Billing server App server
Account number	Unique account number for SM owner **(Low sensitive)**	App server	SM owner App server Web-portal Billing server

PIA of smart meter

Daily Usage			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Usage pattern	Traceable power usage patterns and householder behaviors **(High sensitive)**	Power suppliers	SM owner
Householders	Gives ability to the suppliers to know when users are most active **(High sensitive)**	SM owner	SM owner
Power usage	provides used power Current price current total price of power used **(Moderate sensitivity)**	SM owner	householders, SM owner

PIA of smart meter

User subscription			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
SM type and serial number	SM information **(Low Sensitivity)**	Manufacturer	App server
Subscription	Subscription type, Subscription demands **(Low Sensitivity)**	SM owner	App server
Subscriber's Name	User's Full name **(High Sensitivity)**	SM owner	Billing server
Address	User's Country, City, State, Street **(Moderate Sensitivity)**	SM owner	Billing and App servers
User's phone number	Phone number of SM owner **(Moderate Sensitivity)**	SM owner	Billing and App servers

Table B.10: PIA of smart meter

Billing Details			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
SM ID	SM identification, identifies users **(Low sensitive)**	Provided by suppliers	SM owner
SM/consumer billing profile	Payment methods **(High sensitive)**	SM owner	SM owner
Previous Billings	List of previous bills **(High sensitive)**	SM owner Power providers	SM owner Power providers

PIA of smart meter

Attachment to Web-portal			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	User account number when created **(Moderate Sensitivity)**	Account server via SM owner	App server Web-portal
SM Serial number	Unique identifier for the SM **(Moderate Sensitivity)**	SM manufacturer	SM owner App server Web-portal

B.5 Smart Hub

PIA of smart hub

Account Creation			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Login	Users identifier **(Low Sensitivity)**	Created by user	User App server Phone App
Password	User Password **(High Sensitivity)**	Created by user	User App server Phone App
Account number	Unique account number **(Moderate Sensitivity)**	Manufacturer App server	smart hub owner App server smartphone app
Secret question	unique answer to the secret question in order to recover account's password **(High Sensitivity)**	created by user	App server account owner

PIA of smart hub

Attachment to smartphone app			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Account number	User account number when created **(Moderate Sensitivity)**	Account server via hub owner	App server Smartphone app Web-portal
Smart hub serial number	Unique identifier for the hub **(Moderate Sensitivity)**	Manufacturer	Hub owner App server smartphone app Web-portal
Smart hub settings and configurations	settings and configs made on the hub by using smartphone app or web-portal **(Moderate Sensitivity)**	smart hub owner	App server Smart hub

PIA of smart hub

Daily usage			
Parameter	**Description/sensitivity**	**Origin**	**Consumer**
Usage pattern	accessible usage patterns and behaviors of smart appliances connected to the hub **(High Sensitivity)**	App Server	Smart hub owner
Smart appliances data	collected data from connected smart devices to the smart hub **(High Sensitivity)**	App server smart hub smart devices	App server smart hub's owner
Smart appliances states	Changing mode operation of connected devices to the smart hub **(High Sensitivity)**	App server	App server smart hub owner via smartphone

B.6 Fridge PIA

PIA of smart home case for master Smart Fridge

Questionary A: PRELIMINARY ANALYSIS QUESTIONNAIRE

0 PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity, that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

1. COLLECTION, USE AND DISCLOSURE

1.1 Identify the kinds of information involved in the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Information about individuals in their personal capacity	YES
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	NO
Information about institutions, for example, for profit and not-for-profit institutions and government institutions	NO
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	YES

1.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	Collect	Use	Retain	Disclose	Secure	Dispose

List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Name	X	X	X	X		
Username & Password	X	X	X		X	X
Account number	X	X	X		X	
Fridge Serial number	X	X	X		X	
Name, address, phone number	X	X	X	X	X	
Voice recording	X	X	X		X	X
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as- necessary.)						
Transcribed App microphone data	X	X	X		X	X
Usage pattern	X	X	X		X	
Fridge settings	X	X	X	X	X	X
Food list	X	X	X		X	
Food usage logs	X	X	X		X	
Meal plan	X	X	X	X	X	X

1.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

The user / owner of the smart fridge.

2.1 Public Records and Excluded Personal Information

Question	**Answer (YES, NO, UNKNOWN)**
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	NONE
No personal information will be available to the public.	

3.1

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.
YES The PIA process will be continued as there is personal information collected and used and a PIA is a good way for the Master Thesis Report to examine how privacy can be impacted and protected in a smart home.

QUESTIONARY B: PROJECT ANALYSIS QUESTIONNAIRE

1 Scope of PIA

This PIA review is for the smart fridge that is considered in the smart home architecture created for our case used in the master thesis. The scope of the PIA includes the Smart Fridge and it’s communication with other parties. The other parties are the user, food shopping services as well as communication with the smart hub. (Next is not decided) Business aspects are considered out of scope as this master report focuses more on the technical aspects. And the only legal aspects considered are the GDPR as we are stationed in Europe.

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

All services that uses, stores or moves personal data is under the regulation of GDPR.

Question	Answer (YES, NO, UNKNOWN)

Involves creating a new program, process, service, technology, information system or other type of IT application	YES
Involves a change to an existing program, process, service, technology, information system or other type of IT application	NO
Involves procuring goods or services	
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information	NO
Involves developing a request for bids, proposals or services	NO
Involves a process, system or technology for which the privacy risks are not known or well documented	YES
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	YES
Involves information sharing (internal and external)	YES
Involves the need to identify, authenticate or authorize users – public and/or internal staff	YES
Other activities that may impact privacy. (Please explain below.)	

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The service is set up by us for a case study and have no previous PIA assessments so all program, process, services can be considered new.
2. The privacy issues with a smart home and by extension a smart fridge are not well enough documented / explored and smart home devices are ever increasing in complexity as well.
3. A database of user interaction is stored on the device itself as well as user data in the clouds needed to service the user.
4. Information is shared between the smart fridge and the user as well as between the smart fridge and the smart hub(change of state or order to change state).
5. Users will have to use login credentials to connect to the fridge from outside of the same network and to access cloud services.

3.3 Identify any changes that will result from the project (check all that apply).

Question	**Answer (YES, NO, UNKNOWN)**

Involves a change in business owner	NO
Involves a change to legislative authority	NO
Involves procuring goods or services	NO
Involves a change in users (internal and external) of a related process or system	NO
Involves a change in partners or service providers (internal and external)	NO
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	NO
Involves a change to the purposes for which personal information will be collected, used or disclosed	NO
Involves a change from direct to indirect collection of personal information	NO
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information	NO
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information	NO
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software	NO
Involves a change to an information system or database containing personal information	NO
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients	NO
Involves a change in the security requirements or measures	NO
Other (Please specify change or proposed change below.)	NO
The answer is no to all of them as there are no changes made. (Might change to all yes as everything is new)	

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

NA

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services	YES
Involves logging information, usage or preferences, for example, IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology	YES
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	YES
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools	YES
Involves processing or storing of personal information in a virtual environment, for example, cloud computing	YES
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors	NO
Involves developing, or customizing, software, hardware or IT support services "in-house"	YES
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information	NO
Involves a system or application that will automatically collect, use, disclose or retain personal information	YES
Other (Please explain below.)	

4.2 **If you answered yes to any of the above**, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

- The smart fridge contains a camera to allow user to monitor the items within the fridge.
- The smart fridge does record users' usage,

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role

INSTITUTION/THIRD PARTY	PROJECT ROLE
Food shopping store	Can accept shopping lists, process them, and deliver food.
The smart hub	Can be used to monitor and control communication between the smart fridge and other smart appliances.

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information on behalf of your institution

INSTITUTION/THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE
NONE (must defend in report)		

5.3 Identify any location outside of the EU where personal information may be retained or stored, and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY
None		

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	Relation RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5

Identify how other institutions or third parties will be bound to follow relevant

privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts				
Memoranda of Understanding				
Agreements (service level and trade)				
Other (Please explain below.)				

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and

activity relevant to the project. Consider the factors identified in the guide. Attach all

related documentation to your completed Project Analysis Questionnaire.

N/A

7. PERSONAL INFORMATION FLOWS

7.1 Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis Questionnaire

B.7 Thermostat PIA

PIA of smart home case for master Smart Thermostat

Questionary A: PRELIMINARY ANALYSIS QUESTIONNAIRE

0 PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity, that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

1. COLLECTION, USE AND DISCLOSURE

1.1 Identify the kinds of information involved in the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Information about individuals in their personal capacity	YES
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	NO
Information about institutions, for example, for profit and not-for-profit institutions and government institutions	NO
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	YES

**1.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	Collect	Use	Retain	Disclose	Secure	Dispose

List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Name	X	X	X	X		
Username & Password	X	X	X		X	X
Account number	X	X	X		X	
Name, Phone number,	X	X	X		X	
Thermostat Serial number	X	X	X			
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as- necessary.)						
Usage data	X	X	X	X	X	X
Temperature settings	X	X	X	X	X	
Thermostat settings	X	X	X			
Sensor data	X	X	X		X	
Thermostat sensor data	X	X	X	X	X	
User patterns	X	X	X		X	

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

The user / owner of the smart thermostat

2.1 Public Records and Excluded Personal Information

Question	Answer (YES,- NO, UNKNOWN)
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	NONE
No personal information will be available to the public.	

3.1

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.
YES The PIA process will be continued as there is personal information collected and used and a PIA is a good way for the Master Thesis Report to examine how privacy can be impacted and protected in a smart home.

QUESTIONARY B: PROJECT ANALYSIS QUESTIONNAIRE

1 Scope of PIA

This PIA review is for the smart thermostat that is considered in the smart home architecture created for our case used in the master thesis. The scope of the PIA includes the smart thermostat and its communication with other parties. The other parties are the user, cloud service as well as communication with the smart hub. (Next is not decided) Business aspects are considered out of scope as this master report focuses more on the technical aspects. And the only legal aspects considered are the GDPR as we are stationed in Europe.

Define the scope of the PIA review and analysis, that is, what aspects of the project

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

All services that use, store or move personal data is under the regulation of GDPR.

3. PROJECT CHARACTERISTICS

3.1 Identify key characteristics of the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves creating a new program, process, service, technology, information system or other type of IT application	YES
Involves a change to an existing program, process, service, technology, information system or other type of IT application	NO
Involves procuring goods or services	NO
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information	NO
Involves developing a request for bids, proposals or services	NO
Involves a process, system or technology for which the privacy risks are not known or well documented	YES
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	YES
Involves information sharing (internal and external)	YES
Involves the need to identify, authenticate or authorize users – public and/or internal staff	YES
Other activities that may impact privacy. (Please explain below.)	

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The service is set up by us for a case study and has no previous PIA assessments so all programs, processes and services can be considered new.
2. The privacy issues with a smart home and by extension a smart thermostat are not well enough documented / explored and smart home devices are ever increasing in complexity as well.
3. A database of user interaction is stored on the device itself as well as user data in the clouds needed to service the user.
4. Information is shared between the smart fridge and the user as well as between the smart thermostat and the smart hub(change of state or order to change state).
5. Users will have to use login credentials to connect to the thermostat from outside of the same network and to access cloud services.

3.3 Identify any changes that will result from the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves a change in business owner	NO
Involves a change to legislative authority	NO
Involves procuring goods or services	NO
Involves a change in users (internal and external) of a related process or system	NO
Involves a change in partners or service providers (internal and external)	NO
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	NO
Involves a change to the purposes for which personal information will be collected, used or disclosed	NO
Involves a change from direct to indirect collection of personal information	NO
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information	NO
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information	NO
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software	NO
Involves a change to an information system or database containing personal information	NO
Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients	NO
Involves a change in the security requirements or measures	NO
Other (Please specify change or proposed change below.)	NO
The answer is no to all of them as there are no changes made. (Might change to all yes as everything is new)	

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

NA

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

NA

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply).

Question	**Answer (YES, NO, UNKNOWN)**
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services	YES
Involves logging information, usage or preferences, for example, IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology	YES
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	YES
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools	YES
Involves processing or storing of personal information in a virtual environment, for example, cloud computing	YES
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors	NO
Involves developing, or customizing, software, hardware or IT support services "in-house"	YES

Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information	NO
Involves a system or application that will automatically collect, use, disclose or retain personal information	YES
Other (Please explain below.)	

4.2 **If you answered yes to any of the above**, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The smart thermostat has built in sensors that track if there are anyone at home and what rooms they are in. The thermostat does not need to know the identity of the person but know that the person is in a room.
2. The smart thermostat logs the usage of the user, temperatures and timeslots.
3. A website is used to connect to the thermostat if the user is not connected to the same network.
4. The thermostat stores loges on how much it is used and time to desired temperature reached.
5. The cloud stores login information.
6. The smart thermostat and its software is created and owned by the same company.
7. The logs on when a user is at home and in what room is stored. This can be considered personal information as it contains user habits.

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role

INSTITUTION/THIRD PARTY	PROJECT ROLE
The smart hub	Can be used to monitor and control communication between the smart thermostat and other smart appliances.

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information on behalf of your institution

INSTITUTION/THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE
NONE (must defend in report)		

5.3 Identify any location outside of the EU where personal information may be retained or stored, and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY
None		

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	Relation RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5

Identify how other institutions or third parties will be bound to follow relevant

privacy and security re/quirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts				
Memoranda of Understanding				
Agreements (service level and trade)				
Other (Please explain below.)				

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and

activity relevant to the project. Consider the factors identified in the guide. Attach all

related documentation to your completed Project Analysis Questionnaire.

N/A

7. PERSONAL INFORMATION FLOWS

7.1 Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project’s and your institution’s needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis Questionnaire

B.8 Smart Hub PIA

PIA of smart home case for master Smart Hub

Questionary A: PRELIMINARY ANALYSIS QUESTIONNAIRE

0 PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity, that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

3. COLLECTION, USE AND DISCLOSURE

1.1 Identify the kinds of information involved in the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Information about individuals in their personal capacity	YES
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	NO
Information about institutions, for example, for profit and not-for-profit institutions and government institutions	NO
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	YES
Each smart hub comes up with a unique serial number. Additionally, the smart hub does provide anonymization. **Anonymization** is done under various categories. 1. Data suppression: Here some of data fields will be removed in a dataset. 2. Character Masking: Here will some characters in a dataset be changed. For instance, User's name will be hiding with stars (Håvard --> H*****). 3. Data Generalisation: Reduction of data precision. Moreover, a smart hub provides **Pseudonymization** which is also divided into different categories. 1. Swapping: We can consider that we have a dataset, in the dataset data will be shuffled in order to hide the original values. 2. Hash/ Look-up: The values from an original dataset will be replaced with other data. By using hash/ look-up, it will be possible to re-identify the data. 3. Data Perturbation: Data distortion is used to modify the original data values, and by using additive noise, data values will be randomly modified.	

1.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	Collect	Use	Retain	Disclose	Secure	Dispose
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Smart Appliances	X	X	X		X	X
Username & Password	X	X	X		X	X
Meta data	X	X	X	X	X	X
Account number	X	X	X		X	
Smart hub serial number	X	X	X		X	
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as- necessary.)						
Usage data	X	X	X	X	X	X
Smart hub settings and configuration	X	X	X	X	X	
Usage pattern	X	X	X		X	
Smart appliances data	X	X	X		X	
Smart appliances states	X	X	X		X	

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

The user / owner of the smart fridge.

2.1 Public Records and Excluded Personal Information

Question	Answer (YES, NO, UNKNOWN)
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	NONE
No personal information will be available to the public.	

3.1

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.
YES The PIA process will be continued as there is personal information collected and used and a PIA is a good way for the Master Thesis Report to examine how privacy can be impacted and protected in a smart home.

QUESTIONARY B: PROJECT ANALYSIS QUESTIONNAIRE

1 Scope of PIA

This PIA review is for the smart Hub that is considered in the smart home architecture created for our case used in the master thesis. The scope of the PIA includes the Smart Hub and it's communication with other parties. The other parties are the user and the various smart appliances. (Next is not decided) Business aspects are considered out of scope as this master report focuses more on the technical aspects. And the only legal aspects considered are the GDPR as we are stationed in Europe.

Define the scope of the PIA review and analysis, that is, what aspects of the project

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

All services that uses, stores or moves personal data is under the regulation of GDPR.

3. PROJECT CHARACTERISTICS

3.1 Identify key characteristics of the project (check all that apply).

Question	**Answer (YES, NO, UNKNOWN)**
Involves creating a new program, process, service, technology, information system or other type of IT application	YES
Involves a change to an existing program, process, service, technology, information system or other type of IT application	NO
Involves procuring goods or services	
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information	NO
Involves developing a request for bids, proposals or services	NO
Involves a process, system or technology for which the privacy risks are not known or well documented	YES
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	YES
Involves information sharing (internal and external)	YES
Involves the need to identify, authenticate or authorize users – public and/or internal staff	YES
Other activities that may impact privacy. (Please explain below.)	

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The service is set up by us for a case study and has no previous PIA assessments so all programs, processes, and services can be considered new.

2. The privacy issues with a smart home and by extinction a smart Hub are not well enough documented / explored and smart home devices are ever increasing in complexity as well.
3. A database of user interaction is stored on the device itself as well as user data in the clouds needed to service the user.
4. The smart hub involves information sharing, the smart hub responsibility is to control and monitor communication from different appliances. Smart appliances share information with the smart hub, then smart hub can either change or order to change the state of a smart appliance that is connected to the smart hub.
5. Users will have to use login credentials to connect to the smart hub from outside of the same network and to access cloud services.

3.3 Identify any changes that will result from the project (check all that apply).

Question	**Answer (YES, NO, UNKNOWN)**
Involves a change in business owner	NO
Involves a change to legislative authority	NO
Involves procuring goods or services	NO
Involves a change in users (internal and external) of a related process or system	NO
Involves a change in partners or service providers (internal and external)	NO
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	NO
Involves a change to the purposes for which personal information will be collected, used or disclosed	NO
Involves a change from direct to indirect collection of personal information	NO
Involves a change in roles and responsibilities, that is, who can do what, when, where, why and how with personal information	NO
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information	NO
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software	NO
Involves a change to an information system or database containing personal information	NO

Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the, creation of a new website to provide services to clients	NO
Involves a change in the security requirements or measures	NO
Other (Please specify change or proposed change below.)	NO
The answer is no to all of them as there are no changes made. (Might change to all yes as everything is new)	

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

3.5 Document any additional business processes identified from your analysis of the

factors identified in the guide. Attach all relevant documentation to your completed Project

Analysis Questionnaire.

N/A

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves technology designed to monitor, track or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services	NO

Involves logging information, usage or preferences, for example, IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual’s use of technology	YES
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	YES
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools	YES
Involves processing or storing of personal information in a virtual environment, for example, cloud computing	YES
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors	NO
Involves developing, or customizing, software, hardware or IT support services “in-house”	YES
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information	NO
Involves a system or application that will automatically collect, use, disclose or retain personal information	YES
Other (Please explain below.)	

4.2 **If you answered yes to any of the above**, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The smart hub itself doesn’t involve any technology that tracks, monitors or observes users or their transactions. But some of the devices that might be connected to it may involve these technologies and may not be sent to the smart hub.
2. Smar hub involves usage and preferences, data sent from connected smart appliances transferers to the smart hub and then to a cloud service. The smart hub can monitor the usage, for instance of a smart thermostat and its state.
3. The smart hub involves public-facing internet communication and services where the smart hub allows users to make change of the state of their connected smart appliances to the smart hub by using their phone.
4. ---
5. The smart hub involves processing and storing personal information in the cloud. The state of different connected devices to the smart hub will be transferred from the smart hub to a cloud service, where users can remotely access it by using their phone.
6. Different smart appliances that automatically collect, use and retain users' personal information will be connected to the smart hub.

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role

INSTITUTION/THIRD PARTY	PROJECT ROLE
Cloud services	Different data from different appliances will be collected then transferred to cloud services where users can remotely access these data via phone when they are outside their smart home.

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information on behalf of your institution

INSTITUTION/THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE
NONE (must defend in report)		

5.3 Identify any location outside of the EU where personal information may be retained or stored, and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY
None		

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	Relation RELATIONSHIP TO PROJECT	PROJECT ROLE
N/A		

5.5

Identify how other institutions or third parties will be bound to follow relevant

privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts	N/A	N/A	N/A	N/A
Memoranda of Understanding	N/A	N/A	N/A	N/A
Agreements (service level and trade)	N/A	N/A	N/A	N/A
Other (Please explain below.)	N/A	N/A	N/A	N/A

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and

activity relevant to the project. Consider the factors identified in the guide. Attach all

related documentation to your completed Project Analysis Questionnaire.

N/A

7. PERSONAL INFORMATION FLOWS

7.1 Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis Questionnaire

B.9 Smart Meter PIA

PIA of smart home case for master Smart Meter

Questionary A: PRELIMINARY ANALYSIS QUESTIONNAIRE

0 PROJECT DESCRIPTION

Describe the project, that is, the program, system, application or activity, that is the subject of the PIA including its purpose, scope and key objectives. Attach relevant project documentation, if necessary.

1. COLLECTION, USE AND DISCLOSURE

1.1 Identify the kinds of information involved in the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Information about individuals in their personal capacity	YES
Information about individuals acting in their business, professional or official capacity, for example, name, job title, and business contact information	NO
Information about institutions, for example, for profit and not-for-profit institutions and government institutions	NO
Aggregated, anonymized or de-identified information. Outline in the row below the process followed to aggregate, anonymize or de-identify the information and whether it is possible to identify/re-identify individuals from that information.	YES
Smart meter owners have unique user identifiers, meaning that user's identities are anonymized. Each user has a different smart meter ID, energy providers could identify users by using that ID. Additionally, the consumption data collected by a smart meter are aggregated before it is sent to the utility. Then, the utility can use some methods such as Non-intrusive Load Monitoring (NILM) to disaggregate these data which allows them to extract details about the energy consumption of devices used.	

1.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	Collect	Use	Retain	Disclose	Secure	Dispose
List the types of personal information involved in the project and indicate in the columns on the right whether this personal information will be collected, used, disclosed, retained, secured or disposed of. -- (Add rows as necessary.) If third parties will be involved in the project, think about what they may be doing with personal information as well. (Add rows as necessary.)						
Smart meter ID	X	X	X	X	X	
Username & Password	X	X	X		X	X
Users' location	X	X	X		X	X
Meta data	X	X	X	X	X	X
Name, address, phone number	X	X	X	X	X	
Account number	X	X	X		X	
SM/consumer billing profile	X	X	X	X	X	
Previous Billings	X	X	X		X	
List each element of non-personal information that, when combined or linked, may enable identification of an individual, and indicate in the columns on the right whether that information will be collected, used, disclosed, retained, secured or disposed of. (Add rows as- necessary.)						
Usage data	X	X	X	X	X	
Usage pattern	X	X	X	X	X	
Householders	X	X	X		X	
Power usage	X	X	X	X	X	
Subscription	X	X	X	X	X	

4.3 To whom does the personal information relate? List all the individuals whose personal information will be involved in the project, that is, the data subjects.

The user(s) / owner of the smart meter.
Users are considered anyone living in a house with a smart meter installed.
Only the owner will be registered with PII such as name, address, billing information etc.

2.1 Public Records and Excluded Personal Information

Question	Answer (YES, NO, UNKNOWN)
Identify any personal information that will be maintained for the purpose of creating a record that is available to the general public. What is the type of personal information, and why and how is it made available to the general public? (Please explain in row below.)	NONE
No personal information will be available to the public.	

3.1

Indicate whether or not you will proceed with the PIA process and the reasons for your decision.
YES The PIA process will be continued as there is personal information collected and used and a PIA is a good way for the Master Thesis Report to examine how privacy can be impacted and protected in a smart home.

QUESTIONARY B: PROJECT ANALYSIS QUESTIONNAIRE

1 Scope of PIA

This PIA review is for the smart meter that is considered in the smart home architecture created for our case used in the master thesis. The scope of the PIA includes the Smart meter and it’s communication with other parties. The other parties are the user, power suppliers as well as communication with the smart hub. (Next is not decided) Business aspects are considered out of scope as this master report focuses more on the technical aspects. And the only legal aspects considered are the GDPR as we are stationed in Europe.

Define the scope of the PIA review and analysis, that is, what aspects of the project

2. PROJECT AUTHORITY

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understandings, agreements, contracts and other relevant instruments).

All services that use, store or move personal data are under the regulation of GDPR.

3. PROJECT CHARACTERISTICS

3.1 Identify key characteristics of the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves creating a new program, process, service, technology, information system or other type of IT application	YES
Involves a change to an existing program, process, service, technology, information system or other type of IT application	NO
Involves procuring goods or services	NO
Involves outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information	NO
Involves developing a request for bids, proposals or services	NO
Involves a process, system or technology for which the privacy risks are not known or well documented	YES
Involves creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases	YES
Involves information sharing (internal and external)	YES
Involves the need to identify, authenticate or authorize users – public and/or internal staff	YES
Other activities that may impact privacy. (Please explain below.)	

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The service is set up by us for a case study and has no previous PIA assessments so all programs, processes, and services can be considered new.
2. The privacy issues with a smart home and by extinction a smart meter are not well enough documented / explored and smart home devices are ever increasing in complexity as well.
3. A database of user interaction is stored on the device itself as well as user data in the clouds needed to service the user.
4. Information is shared between the smart meter and the user as well as between the smart meter and the smart hub (change of state or order to change state).
5. Users will have to use login credentials to connect to the smart meter from outside of the same network and to access cloud services.

3.3 Identify any changes that will result from the project (check all that apply).

Question	**Answer (YES, NO, UNKNOWN)**
Involves a change in business owner	NO
Involves a change to legislative authority	NO
Involves procuring goods or services	NO
Involves a change in users (internal and external) of a related process or system	NO
Involves a change in partners or service providers (internal and external)	NO
Involves a change in the amount, type of or ways that personal information is collected, used, disclosed, retained, secured or disposed of	NO
Involves a change to the purposes for which personal information will be collected, used or disclosed	NO
Involves a change from direct to indirect collection of personal information	NO
Involves a change in roles and responsibilities, that is, who can do what, when, where, why, and how with personal information	NO
Involves a change to, or elimination of, existing practices of anonymizing or de-identifying information	NO
Involves a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information, for example, hardware and software	NO
Involves a change to an information system or database containing personal information	NO

Involves a change of medium or service delivery channels, for example, the automation of manual process, conversion from paper to electronic records or the creation of a new website to provide services to clients	NO
Involves a change in the security requirements or measures	NO
Other (Please specify change or proposed change below.)	NO

The answer is no to all of them as there are no changes made.
(Might change to all yes as everything is new)

3.4 If you answered yes to any of the above, explain the change, that is, what specifically will change and why it is necessary. Attach all relevant documentation to your completed Project Analysis Questionnaire.

3.5 Document any additional business processes identified from your analysis of the

factors identified in the guide. Attach all relevant documentation to your completed Project

Analysis Questionnaire.

N/A

4. TECHNOLOGY

4.1 Identify technology-related characteristics of the project (check all that apply).

Question	Answer (YES, NO, UNKNOWN)
Involves technology designed to monitor, track, or observe an individual or their transactions, for example, video cameras, cell phones and geospatial or location-based services	YES

Involves logging information, usage or preferences, for example, IP addresses, traffic data, access, or transaction logs, cookies, or other mechanisms for recording an individual's use of technology	YES
Involves public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media	YES
Involves using analytics or performance measurements, for example, web analytics, social media analytics, or business intelligence tools	YES
Involves processing or storing personal information in a virtual environment, for example, cloud computing	YES
Involves acquiring, or customizing, commercial software, hardware or IT support services by external vendors	NO
Involves developing, or customizing, software, hardware or IT support services "in-house"	YES
Involves creating information systems or other types of IT applications that will be populated by others, for example, clients of system or service will supply information	NO
Involves a system or application that will automatically collect, use, disclose or retain personal information	YES
Other (Please explain below.)	

4.2 **If you answered yes to any of the above**, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed Project Analysis Questionnaire.

1. The smart meter has been developed with some technology that provides power suppliers with the ability to know users'/smart meter location. In addition, the smart meter will measure overall users' power usage and then generate billing based on that.
2. Smart meters users have logging information to login to the web-portal to monitor their power usage when they are outside of their homes.
3. The smart meter does involve public-facing internet communication and services, where users power consumption transfers from smart meter to the power suppliers.
4. The smart meter involves using analytics and performance measurements. It measures users power consumption usage. Additionally, the smart meter can analyze power used each hour, and by using analytics it can detect any data tampering.
5. The smart meter data will be stored in a cloud-based service, where user can access data via their phone.
6. The smart meter and its software are created and owned by the same company.
7. The smart meter automatically collects user power usage, uses the collected data and transfers it to the power suppliers and retains it.

5. ROLES AND RESPONSIBILITIES

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role

INSTITUTION/THIRD PARTY	PROJECT ROLE
The smart hub	Can be used to monitor and control communication between the smart meter and other smart appliances.
Cloud services	Smart meter data will be collected then transferred to the cloud services where users can remotely access these data via phone when they are outside their smart home.

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information on behalf of your institution

INSTITUTION/THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE
NONE (must defend in report)		

5.3 Identify any location outside of the EU where personal information may be retained or stored, and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY
None		

5.4 List all other parties that will have access to, or use, the personal information, for example, other program areas, IT staff, legal counsel, etc.

PARTY	Relation RELATIONSHIP TO PROJECT	PROJECT ROLE
N/A		

5.5

Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
Contracts	N/A	N/A	N/A	N/A
Memoranda of Understanding	N/A	N/A	N/A	N/A
Agreements (service level and trade)	N/A	N/A	N/A	N/A
Other (Please explain below.)	N/A	N/A	N/A	N/A

6. RELEVANT INFORMATION

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed Project Analysis Questionnaire.

N/A

7. PERSONAL INFORMATION FLOWS

7.1 Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your definition of personal information flow throughout the project to your completed Project Analysis Questionnaire

See DFD and extra tables included in main report

Appendix C

CyberComply DPIA

CYBERCOMPLY

SMART FRIDGE DPIA REPORT

uia.no

Issued **18 May 2022**

Process description

SCOPE OF PROCESSING

1. What type of processing is involved?
   The fridge takes not of when a food item is added to the fridge, and when the food item is used.
   The fridge collects user patterns to deliver shopping lists, meal suggestions and set the fridge settings to limit power consumption.
2. What categories of personal data do you process?
   Account details, Authentication details, Behavioural information, Device details, Location, Ownership details, Preferences and interests, Other
3. What type and volume of personal data do you process?
   Personal data items: Address, Email address, IP address, Login/username, Name, Phone number, Voice recording
4. What is the extent and frequency of the processing?
   Several times a day
5. What is the duration of processing?
   Not answered
6. How many data subjects are involved?
   ☑ 0-10
   ☐ 10-50 ☐ 50+
7. What is the geographical area covered?
   Norway

NATURE OF PROCESSING

1. How do you collect personal data?
   Personal data is collected upon initial setup of the accompanying app as well as collecting user logs when the user uses the smart fridge and app.
2. How do you store personal data?
   Personal data is stored on the smart fridge as well as on the phone with the accompanying app.

3. How do you use personal data?
   Personal data is used to create a personalized experience for the user with custom shopping lists and meal plans suggestions.
4. Who has access to personal data?
   The user and the smart fridge with app.
5. Who do you share personal data with?
   The app can share the created shopping list with a shopping service along with needed user account information.
6. Do you use any processors? ☐ Yes ☑ No
   Details: No other entity processes the PII for the fridge.
7. How long is personal data retained for?
   Not answered
8. What are the security measures for protecting personal data?
   The data is encrypted during transit and storage.

CONTEXT OF PROCESSING

1. Where do you source the personal data from?
   Data Subject
2. What is the nature of the relationship with individuals?
   the individual is the user of the fridge.
3. To what extent do individuals have control over their personal data?
   The user can choose if they want to share the shopping list and other necessary data with the shopping service.'
   The user can choose for there not to be collected user data needed for the user patterns.
   This would remove functionalities of the fridge.
4. To what extent are individuals likely to expect the processing?
   The user will be asked if they want to have their data collected and will be asked or have to actively choose if they want to share and use the shopping service as well.

5. Do you have any previous experience of this type of processing? □ Yes ☑ No
   Details: Neither writer of this master thesis have no experience with this type of processing?
6. Does the process make use of any relevant advances in technology or security? □ Yes ☑ No
   Details: This process uses only standard security technology. This PIA is done to find security and privacy risks and thereafter find relevant advances in technology or security to be used.
7. Are there any current issues of public concern? ☑ Yes □ No
   Details: The privacy implications from smart homes and subsequent smart appliances are not documented enough.
8. Have you considered/complied with any relevant codes of practice? □ Yes ☑ No
   Details: No

PURPOSE OF PROCESSING

1. What does the process aim to achieve?
   The process aims to help the user with making meal plans, shopping list and keep order on what food items they have in the fridge.
2. What are your legitimate interests (if applicable)?
   Our (imaginary for the assignment) interest is to sell more smart fridges while making sure that the users will have their privacy.
3. What is the intended outcome for individuals?
   The intended outcome for the user is for them to have a easier time dealing with food and planing of shopping for food as well as planing dinners.
4. What are the expected benefits of processing for you or society as a whole?
   For people to have an easier time keeping track of food items in their fridge.

Screening questions

ARTICLE 35, 3

1. Arcticle 35, clause 1 of the GDPR states that a DPIA is required if the "type of processing in particular using new technologies,
and taking into account the nature, scope, context and purposes of the processing,
is likely to result in a high risk to the rights and freedoms of natural persons".

   Is a data privacy impact assessment required: ☐ Yes ☑ No

INFORMATION COMMISSIONER'S OFFICE

1. Does the processing involve a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person? (Article 35(3)(a)) ☑ Yes ☐ No
2. Does the process involve large-scale processing of special categories of personal data or of personal data relating to criminal convictions and offences? (Article 35(3)(b)) ☐ Yes ☑ No
3. Does the process involve systematic monitoring of a publicly accessible area on a large scale? (Article 35(3)(c)) ☐ Yes ☑ No

EDPB

1. Does the process involve the use of new technologies, or using technologies in an innovative way? ☑ Yes ☐ No
2. Does the process use profiling or special category data (sensitive data) to decide on access to services? ☐ Yes ☑ No
3. Does the process involve profiling individuals on a large scale? ☐ Yes ☑ No
4. Does the process involve biometric data? ☐ Yes ☑ No
5. Does the process involve genetic data? ☐ Yes ☑ No

6. Does the process match data or combine datasets from different sources? ☐ Yes ☑ No
7. Does the process involve collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')? ☐ Yes ☑ No
8. Does the process involve tracking individuals' location or behaviour? ☑ Yes ☐ No
9. Does the process involve profiling or targeting marketing to children or other vulnerable individuals, or directly offering online services to children? ☐ Yes ☑ No
10. Does the process involve data that might endanger the individual's physical health or safety in the event of a security breach? ☐ Yes ☑ No

DETERMINATION

According to your responses, a DPIA is mandatory

1. Does the processing involve new or innovative technological or organisational solutions? ☐ Yes ☑ No
2. Does the processing involve the evaluation or scoring (including profiling and predicting) of aspects specific to the individual? ☐ Yes ☑ No
3. Does the processing involve automated decision-making that produces a legal or similarly significant effect on the individual? ☐ Yes ☑ No
4. Does the processing involve systematic monitoring of individuals, including in a publicly accessible area? ☑ Yes ☐ No
5. Does the processing involve special categories of data (sensitive data) or data of a highly sensitive nature? ☐ Yes ☑ No
6. Is the data being processed on a large scale? ☐ Yes ☑ No
7. Does the processing involve data sets being matched or combined? ☐ Yes ☑ No
8. Does the data relate to vulnerable individuals? ☐ Yes ☑ No
9. Could the processing prevent individuals from exercising their rights, using a service or fulfilling a contract? ☐ Yes ☑ No

Consultation

1. Has the advice of the DPO been sought? (Article 35(2)) ☐ Yes ☐ No ☑ Not applicable
   Details: There is no DPO as this is a master thesis assignment.
2. Have the views of data subject(s) or their representative(s) been sought? (Article 35(9)) ☐ Yes ☐ No ☑ Not applicable
   Details: There are no real data subjects.
3. Have any processors involved been consulted/requested to assist? (ICO guidance) ☐ Yes ☐ No ☑ Not applicable
   Details: This is a fictional processes.
4. Have all appropriate internal stakeholders been consulted? (ICO guidance) ☐ Yes ☐ No ☑ Not applicable
   Details: This is a fictional processes.
5. Has any expert advice (e.g. from lawyers, IT experts, sociologists or ethicists) been sought? (ICO guidance) ☑ Yes ☐ No ☐ Not applicable
   Details: The assignment has two advisors.

Privacy risk assessment

Risk Description	Initial risk	Response	Residual risk

Is a consultation with the supervisory authority required? ☐ Yes ☑ No

Details:

Principles questionnaire

PURPOSE LIMITATION

1. Is the personal data processed for specified purposes? (Article 5(1)(b)) ☑ Yes ☐ No ☐ Don't know

Details: The data is processed to give the user a personalized experience with custom shopping lists and meal plans based on usage patterns.

2. Is the personal data processed for explicit purposes? (Article 5(1)(b)) ☑ Yes ☐ No ☐ Don't know
   Details: The data is processed to give the user a personalized experience with custom shopping lists and meal plans based on usage patterns.
3. Is the personal data processed for legitimate purposes? (Article 5(1)(b)) ☑ Yes ☐ No ☐ Don't know
   Details: The data is processed to give the user a personalized experience with custom shopping lists and meal plans based on usage patterns.
4. Is the personal data not further processed in a manner that is incompatible with those purposes? (Article 5(1)(b)) ☑ Yes ☐ No ☐ Don't know
   Details: The data is processed to give the user a personalized experience with custom shopping lists and meal plans based on usage patterns.
   Data collected is minimized to only what is needed.

LAWFULNESS, FAIRNESS AND TRANSPARENCY

1. Is the personal data processed lawfully? (Article 6) ☑ Yes ☐ No ☐ Don't know
   Details: The user is asked for permission, the data is only used for specified purposes.
2. Is the personal data processed fairly? (Article 6) ☐ Yes ☐ No ☑ Don't know
   Details: We are not sure what constitutes fair processing.
3. Is the personal data processed in a manner that is transparent to the data subject(s)? (Article 6) ☑ Yes ☐ No ☐ Don't know
   Details: The user will be explained how the data is used to give a custom experience.

DATA MINIMISATION

1. Is the personal data adequate for the purposes of processing? (Article 5(1)(c)) ☑ Yes ☐ No ☐ Don't know
   Details: The data collected should be no more and no less than needed.
2. Is the personal data relevant to the purposes of processing? (Article 5(1)(c)) ☑ Yes ☐ No ☐ Don't know
   Details: The data collected should be no more and no less than needed.
3. Is the personal data limited to what is necessary for the purposes of processing? (Article 5(1)(c)) ☑ Yes ☐ No ☐ Don't know

Details: The data collected should be no more and no less than needed.

ACCURACY

1. Is the personal data accurate? (Article 5(1)(d)) ☑ Yes ☐ No ☐ Don't know
   Details: The data collected by the fridge is based on user patterns and data given by user can be changes by user.
2. Is the personal data kept up to date? (Article 5(1)(d)) ☑ Yes ☐ No ☐ Don't know
   Details: Data given by user can be changes by user.

STORAGE LIMITATION

1. Is the personal data kept in a form that permits identification of data subject(s) for no longer than is necessary for the specified purposes of processing? (Article 5(1)(e)) ☑ Yes ☐ No ☐ Don't know
   Details: The data is stored as long as the user is a customer/ user of the smart fridge.

INTEGRITY AND CONFIDENTIALITY

1. Is the personal data processed in a manner that ensures appropriate security? (Article 5(1)(f)) ☑ Yes ☐ No ☐ Don't know
   Details: The data is encrypted during storage and sending of data. And only stored on the users own devices.

DATA SUBJECT RIGHTS

1. Is fair processing information provided to the data subject(s)? (Article 12, Article 13, Article 14) ☑ Yes ☐ No ☐ Don't know
   Details: The user will be informed when setting up their account and can read later as well.
2. Is there a suitable process for responding to a valid data subject access request? (Article 15) ☑ Yes ☐ No ☐ Don't know
   Details: There will be an automated process for giving the subject their data when requested.
3. Is there a suitable process to update data following a valid rectification request? (Article 16, Article 19) ☐ Yes ☐ No ☑ Don't know
   Details: There will be one for the account however there will be none for the user patterns.
4. Is there a suitable process to erase data following a valid erasure request? (Article 17, Article 19) ☑ Yes ☐ No ☐ Don't know

Details: For the account there will be. For the fridge the user must do it themself.

5. Is there a suitable process to restrict processing following a valid request? (Article 18, Article 19)
   Details: The user will be able to retract permission to process and collect their data.
   This will remove functionalities from the fridge.
   ☑ Yes ☐ No ☐ Don't know

6. Can the data subject(s) obtain and reuse their personal data with a different service provider? (Article 20)
   Details: The user will be able to download all their data.
   ☑ Yes ☐ No ☐ Don't know

7. Can the data subject(s) object to processing? (Article 21)
   Details: This will remove functionalities.
   ☑ Yes ☐ No ☐ Don't know

8. If the process constitutes automated decision making, can the data subject(s) obtain human intervention? (Article 22(3))
   Details: The user can decline this would however limit functions of the fridge.
   ☑ Yes ☐ No ☐ Don't know

9. If the process constitutes automated decision making, can the data subject(s) express their point of view? (Article 22(3))
   Details: There is not a set plan for the user to give their point of view.
   ☐ Yes ☐ No ☑ Don't know

10. If the process constitutes automated decision making, can the data subject(s) challenge the decision? (Article 22(3))
    Details: The user can decline this would however limit functions of the fridge.
    ☐ Yes ☐ No ☑ Don't know

ADDITIONAL MEASURES TO PROTECT DATA SUBJECTS

1. Are processors bound by a suitable contract or legal act that outlines the processor’s data protection obligations? (Article 28(3))
   Details: We have not created or decided on any legally binding contract for this assignment.
   ☐ Yes ☑ No ☐ Don't know
   ☐ Not applicable

2. Do processors have sufficient technical and organisational measures in place to protect the rights of the data subject(s)? (Article 28(1))
   Details: This PIA and subsequent risk analysis is to find out this.
   ☐ Yes ☐ No ☑ Don't know
   ☐ Not applicable

3. Are processors given the specific or general authorisation of the controller? (Article 28(2))
   Details: The processor and controller are the same company.
   ☑ Yes ☐ No ☐ Don't know
   ☐ Not applicable

4. Are any transfers to third countries or international organisations made only to locations that have been subject to an EC adequacy decision or, if not, is transferred data protected by appropriate safeguards or only transferred in the exceptional circumstances detailed within Chapter V of the GDPR? (Chapter V)
   Details: The data is stored in the location of the fridge and the connected smart phone. Account information is only stored in the EU.

☐ Yes ☐ No ☐ Don't know
☑ Not applicable

Review

1. Has the content of the DPIA been reviewed and approved by the DPO or another person with sufficient authority and expertise? ☑ Yes ☐ No
   Details: The DPI has been reviewed by the writers.
2. Is the processing authorised to go ahead? ☑ Yes ☐ No
   Details: Yes.

Appendix D

Risk Assessment Report

Smart Fridge

Risk Owner:	The manufacturer of the Smart Fridge
Risk applies to:	**Confidentiality** Property that information is not made available or disclosed to unauthorised individuals, entities, or processes. (ISO 27000:2018) **Integrity** Property of accuracy and completeness. (ISO 27000:2018) **Availability** Property of being accessible and usable on demand by an authorised entity. (ISO 27000:2018)
Initial risk to organisation:	🟥 Intolerable
Initial risk to data subject:	No initial risk to data subject selected
Response:	Amend/Treat
Residual risk to organisation:	🟧 Tolerable
Residual risk to data subject:	No residual risk to data subject selected

Related controls

ISO/IEC 27001: 2013 A.13.1.3
Segregation in networks

NIST 800-53 CA.1
Security Assessment and Authorization Policies and Procedures

NIST 800-53 CA.6
Security Authorization

NIST 800-53 IA.1
Identification and Authentication Policy and Procedures

NIST 800-53 IA.3
Device Identification and Authentication

NIST 800-53 IA.7
Cryptographic Module Authentication

NIST 800-53 IA.8
Identification and Authentication (Non-organizational Users)

NIST 800-53 SC.13
Use of Cryptography

ISO/IEC 27032:2012 12.2.f
User authentication of service

ISO/IEC 27032:2012 12.3.b
Testing and deploying security updates

ISO/IEC 27032:2012 12.4.h.2
Customer firewalls and HIDS

ISO/IEC 27032:2012 12.4.i
Enable automated updates

ISO/IEC 27032:2012 12.5.5.a
Strong authentication

CSA CCM v3 IPY.04
Standardized Network Protocols

ISO/IEC 27018 A.11.6
Encryption of PII transmitted over public data-transmission networks

SOC 2 TSC CC6.1G
Manages identification and authentication

SOC 2 TSC CC6.1I
Uses encryption to protect data

SOC 2 TSC CC6.1J
Protects encryption keys

SOC 2 TSC CC6.6B
Protects identification and authentication credentials

SOC 2 TSC CC6.6C
Requires additional authentication or credentials

SOC 2 TSC CC6.7B
Uses encryption technologies or secure communication channels to protect data

SOC 2 TSC P5.2B
Permits data subjects to update or correct personal information

NIST SP 800-171 3.1.13
Encryption of remote access sessions

NIST SP 800-171 3.1.16
Wireless access authorization

NIST SP 800-171 3.1.17
Wireless authentication and encryption

NIST SP 800-171 3.1.19
Encryption of mobile data

NIST SP 800-171 3.5.3
Multifactor authentication

NIST SP 800-171 3.5.4
Replay-resistant authentication

NIST SP 800-171 3.5.7
Password complexity

NIST SP 800-171 3.5.8
Prevent password reuse

NIST SP 800-171 3.5.10
Password encryption

NIST SP 800-171 3.13.6
Network access and control

NIST SP 800-171 3.13.11
Use of cryptography

NIST SP 800-171 3.14.4
Antivirus and anti-malware updates

ISO/IEC 27001:2013/27701:2019 - Privacy A.13.1.2
Security of network services

Cyber Essentials (2021) CES4.a
Firewalls

Cyber Essentials (2021) CES4.e
Firewall rules

Cyber Essentials (2021) CES4.f
Permissive firewall rules

Cyber Essentials (2021) CES4.g
Host-based firewalls

Cyber Essentials (2021) CES4.c
Internet access to firewall configuration

Cyber Essentials (2021) CES5.c
Change default passwords

Cyber Essentials (2021) CES5.g
Technical password control

Cyber Essentials (2021) CES5.i
Minimum password length

Cyber Essentials (2021) CES5.j
No maximum password length

Cyber Essentials (2021) CES5.k
Password compromise

Cyber Essentials (2021) CES8.b
Anti-malware software - automatic updates

Cyber Essentials (2021) CES6.d
Automated software updates

NIST CSF PR.AC-5
Network integrity

NIST CSF PR.PT-4
Communication and control networks

ECC 2018 2-5-4
Review of requirements for network security management

Threats:

- Compromise of information: Eavesdropping
- Compromise of information: Position detection
- Compromise of information: Remote spying
- Compromise of information: Tampering with software
- Data becomes corrupted or ransomed
- Data breach
- Denial of service attack
- Hacking
- Lack of monitoring (resulting in breaches)
- Malicious code - Virus / Trojan Horse infection
- Malware
- Network intrusion
- Transmission errors
- Unable to access data
- Unauthorised access to exposed weakness
- Unauthorised access to facilities
- Unauthorised access to records
- Unauthorised actions: Corruption of data
- User device compromised or unusable
- Users not able to log in

Vulnerabilities:

- Compromise of assets
- Compromise of security
- Data could be shared inappropriately with a third party
- Default factory settings not changed
- Development process does not identify vulnerabilities
- Disgruntled or disruptive employee(s)
- Failure to apply relevant software patches
- Failure to comply with legal/contractual requirements
- Failure to comply with policies, standards and technical compliance
- Hacked or stolen password
- Inadequate Intrusion Detection System(s)
- Inadequate anti-malware software
- Inadequate anti-malware software updating
- Inadequate confidentiality agreements (third parties)
- Inadequate control/management of cryptographic keys
- Inadequate controls & procedures for remote access
- Inadequate controls for data processing
- Inadequate firewall
- Inadequate firewall policy
- Inadequate identification/authentication
- Inadequate incident reporting arrangements
- Inadequate information security policy
- Inadequate mechanisms to anonymize user
- Inadequate monitoring mechanisms
- Inadequate network capacity
- Inadequate network infrastructure
- Inadequate or insufficient software testing
- Inadequate or poor specifications for developers
- Inadequate password management

- Inadequate physical access controls
- Inadequate physical protection for the premises
- Inadequate physical security
- Inadequate policy to ensure return of asset(s)
- Inadequate proof of message receipt
- Inadequate security awareness/training for suppliers
- Inadequate segregation of networks
- Inadequate software malfunction handling
- Inadequate software testing
- Inadequate software updating
- Inadequate systems documentation
- Inadequate testing of new systems before release
- Inadequate updates for malicious code protection
- Inadequate validation of processed data
- Inadequate wireless network security controls
- Inadequately configured / maintained firewall
- Inadequately constructed contracts with third parties
- Inadequately documented software
- Inadequately maintained operating system
- Inadequately maintained security features
- Inappropriate use of cryptography
- Information corrupted due to systems failure
- Insecure configuration of Remote Access clients
- Lack of policies and procedures around access to source code
- Loss of telecoms
- Lost or stolen mobile device
- Network: Unprotected sensitive traffic
- Operating system vulnerabilities
- Organization: Lack of established monitoring mechanisms for security breaches
- Organization: Lack of fault reports recorded in administrator and operator logs
- Organization: Lack of procedures for reporting security weaknesses
- Organization: Lack of proper allocation of information security responsibilities
- Software failure
- Software: Lack of identification and authentication mechanisms like user authentication
- Software: Poor password management
- Software: Unprotected password tables
- Software: Well-known flaws in the software
- Transmission of confidential data
- Unauthorised equipment connected to network
- Unauthorised software
- Unauthorised use/access to systems by visitors etc.

Bibliography

[1] Abbas Acar et al. "A Survey on Homomorphic Encryption Schemes: Theory and Implementation." In: *ACM Comput. Surv.* 51.4 (July 2018). ISSN: 0360-0300. DOI: 10.1145/3214303. URL: https://doi.org/10.1145/3214303.

[2] HAYES ADAM. *What Is a Smart Home?* https://www.investopedia.com/terms/s/smart-home.asp. Accessed: Feb. 24, 2022. 2022.

[3] Iftikhar Alam, Shah Khusro, and Mumtaz Khan. "Personalized content recommendations on smart TV: Challenges, opportunities, and future research directions." In: *Entertainment Computing* 38 (2021), p. 100418. ISSN: 1875-9521. DOI: https://doi.org/10.1016/j.entcom.2021.100418. URL: https://www.sciencedirect.com/science/article/pii/S187595212100015X.

[4] Frances K. Aldrich. *Smart Homes: Past, Present and Future*. https://link.springer.com/chapter/10.1007/1-85233-854-7_2. Accessed: Feb. 24, 2022. 2003.

[5] Soumya Banerjee et al. *Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions*. https://ieeexplore.ieee.org/document/8754672. Accessed: May. 22, 2022. 2019.

[6] Joseph Bugeja. *On Privacy and Security in Smart Connected Homes (Part I)*. https://www.researchgate.net/publication/349297209_On_Privacy_and_Security_in_Smart_Connected_Homes_Part_I. Accessed: May. 11, 2022. 2021.

[7] Ismail Butun, Alexios Lekidis, and Daniel dos Santos. *Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities*. https://www.researchgate.net/publication/339815575_Security_and_Privacy_in_Smart_

Grids_Challenges_Current_Solutions_and_Future_Opportunities. Accessed: Apr. 26, 2022. 2020.

[8] Wesley Chai, Sharon Shea, and Ivy Wigmore. *smart home hub (home automation hub)*. Accessed: Mar. 09, 2022.

[9] Intersoft Consulting. *Data protection impact assessment*. https://gdpr-info.eu/art-35-gdpr/. Accessed: Apr. 26, 2022. Na.

[10] Intersoft Consulting. *Data protection impact assessment*. https://gdpr-info.eu/art-35-gdpr/. Accessed: Apr. 26, 2022. Na.

[11] Drew D.Ritchie. *Safe House? How Smart Home Devices Pose Digital Security Risks*. Accessed: Mar. 09, 2022. 2021.

[12] Barb Darrow. *Code On vows to dramatically speed up Wi-Fi, cell, satellite transmissions — with math*. https://laptrinhx.com/code-on-vows-to-dramatically-speed-up-wi-fi-cell-satellite-transmissions-with-math-1672483663/. Accessed: May. 29, 2022. 2020.

[13] John R. Delaney. *Ecobee Smart Thermostat With Voice Control Review*. URL: https://www.pcmag.com/reviews/ecobee-smart-thermostat-with-voice-control. (accessed: 15.03.2022).

[14] John R. Delaney. *Nest Learning Thermostat (3rd Generation) Review*. URL: https://www.pcmag.com/reviews/nest-learning-thermostat-3rd-generation. (accessed: 15.03.2022).

[15] John R. Delaney. *Wyze Thermostat Review*. URL: https://www.pcmag.com/reviews/wyze-thermostat. (accessed: 15.03.2022).

[16] Sanket Desai et al. *A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure*. https://doi.org/10.1007/s10586-018-2820-9). Accessed: Jun. 02, 2022. 2019.

[17] Shreya Dey and Ashraf Hossain. *Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography*. https://ieeexplore.ieee.org/document/8667393. Accessed: May. 22, 2022. 2019.

[18] USA DoJ. *E-Government Act of 2002*. https://www.justice.gov/opcl/e-government-act-2002. Accessed: Apr. 26, 2022. 2019.

[19] Eugen. *Can Smart Light Bulbs Be Hacked To Spy On You?* Accessed: Mar. 09, 2022. 2021.

[20] Moneer Fakroon et al. *Secure remote anonymous user authentication scheme for smart home environment*. https://www.sciencedirect.com/science/article/pii/S2542660520300019. Accessed: May. 22, 2022. 2020.

[21] Mateo Florez Cardenas and Gabriel Acar. *Ethical Hacking of a Smart Fridge : Evaluating the cybersecurity of an IoT device through gray box hacking*. 2021. URL: https://www.diva-portal.org/smash/record.jsf?pid=diva2%5C%3A1596057&dswid=-6042.

[22] Masashi Fujiwara et al. "A Smart Fridge for Efficient Foodstuff Management with Weight Sensor and Voice Interface." In: *Proceedings of the 47th International Conference on Parallel Processing Companion*. ICPP '18. Eugene, OR, USA: Association for Computing Machinery, 2018. ISBN: 9781450365239. DOI: 10.1145/3229710.3229727. URL: https://doi.org/10.1145/3229710.3229727.

[23] Gurjot Singh Gaba et al. *Robust and Lightweight Mutual Authentication Scheme in Distributed Smart Environments*. https://ieeexplore.ieee.org/document/9060967. Accessed: May. 22, 2022. 2020.

[24] GDPR. *A guide to GDPR data privacy requirements*. https://gdpr.eu/data-privacy/. Accessed: Feb. 28, 2022.

[25] Dimitris Geneiatakis et al. "Security and privacy issues for an IoT based smart home." In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2017, pp. 1292–1297. DOI: 10.23919/MIPRO.2017.7973622.

[26] Jin-Hee Han, YongSung Jeon, and JeongNyeo Kim. "Security considerations for secure and trustworthy smart home system in the IoT environment." In: *2015 International Conference on Information and Communication Technology Convergence (ICTC)*. 2015, pp. 1116–1118. DOI: 10.1109/ICTC.2015.7354752.

[27] historyofinformation. *Kevin Ashton Invents the Term "The Internet of Things"*. https://www.historyofinformation.com/detail.php?id=3411. Accessed: May. 21, 2022.

[28] Mike Hogan and Ben Piccarreta. *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)*. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf. Accessed: May. 31, 2022. 2018.

[29] IAPP. *Demonstrating privacy accountability*. https://iapp.org/news/a/demonstrating-privacy-accountability/. Accessed: Apr. 25, 2022. 2011.

[30] iberdrola. *Smart meters, a building block for the digitisation of the grid*. https://www.iberdrola.com/innovation/smart-meters. Accessed: Mar. 28, 2022.

[31] infineon. *Smart Home: Everything you need to know*. https://www.infineon.com/cms/en/discoveries/smart-home-basics/. Accessed: Feb. 24, 2022. 2017.

[32] ipc. *Planning for Success: Privacy Impact Assessment Guide*. https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf. Accessed: Apr. 19, 2022. 2015.

[33] Ashwin Karale. "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws." In: *Internet of Things* 15 (2021), p. 100420. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2021.100420. URL: https://www.sciencedirect.com/science/article/pii/S2542660521000640.

[34] Trong Nghia Le et al. *Advanced Metering Infrastructure Based on Smart Meters in Smart Grid*. https://doi.org/10.5772/63631. Accessed: Mar. 15, 2022. 2016.

[35] Younghun Lee et al. *A blockchain-based smart home gateway architecture for preventing data forgery*. https://doi.org/10.1186/s13673-020-0214-5. Accessed: May. 26, 2022. 2020.

[36] LG. *OWNER'S MANUAL LRMDS3006 / LRMVS3006 / LRMDC2306 / LRMVC2306 / LLMXS3006*. https://www.lg.com/us/support/product/lg-LRMVS3006S.ASTCNA0. Accessed: Mar. 14, 2022. 2020.

[37] Gurusha Lulla et al. "IoT based Smart Security and Surveillance System." In: *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*. 2021, pp. 385–390. DOI: 10.1109/ESCI50559.2021.9396843.

[38] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. *A Systematic Review of the Smart Home Literature: A user perspective*. https://eprints.ncl.ac.uk/file_store/production/250611/21B6CF4D-77E2-42F5-BB97-F3FF8076AB5A.pdf. Accessed: Feb. 24, 2022. 2019.

[39] Alan Meier et al. “Thermostat Interface and Usability: A Survey.” In: (Sept. 2010). DOI: 10.2172/1004198. URL: https://www.osti.gov/biblio/1004198.

[40] Sarah Mennicken and Elaine M. Huang. *Hacking the Natural Habitat: An In-the-Wild Study of Smart Homes, Their Development, and the People Who Live in Them).* https://link.springer.com/chapter/10.1007/978-3-642-31205-2_10#citeas. Accessed: May. 04, 2022. 2012.

[41] Microsoft. *A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes.* https://www.microsoft.com/en-us/research/project/homomorphic-encryption/. Accessed: May. 18, 2022. 2016.

[42] JiHyeon Oh et al. *A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes.* https://www.mdpi.com/1424-8220/21/4/1488. Accessed: May. 22, 2022. 2021.

[43] Kumar Pankaj and Chouhan Lokesh. *A privacy and session key based authentication scheme for medical IoT networks.* https://www.sciencedirect.com/science/article/pii/S014036642032003X. Accessed: May. 22, 2022. 2021.

[44] Goiuri Peralta et al. “Homomorphic Encryption and Network Coding in IoT Architectures: Advantages and Future Challenges.” In: *Electronics* 8.8 (2019). ISSN: 2079-9292. DOI: 10.3390/electronics8080827. URL: https://www.mdpi.com/2079-9292/8/8/827.

[45] Geong Sen Poh, Prosanta Gope, and Jianting Ning. *PrivHome: Privacy-preserving authenticated communication in smart home environment.* https://eprints.whiterose.ac.uk/153150/1/SmartHomeSE.pdf. Accessed: May. 21, 2022. 2021.

[46] privacyinternational. *What Is Privacy?* https://privacyinternational.org/explainer/56/what-privacy. Accessed: Feb. 28, 2022. 2017.

[47] Amanda Push. *The pros and cons of a smart home hub.* https://www.cnet.com/home/smart-home/the-pros-and-cons-of-a-smart-home-hub/. Accessed: Mar. 14, 2022. 2021.

[48] Vincent Ricquebourg et al. *The Smart Home Concept : our immediate future.* https://www.researchgate.net/publication/224696459_The_Smart_Home_Concept_our_immediate_future. Accessed: Feb. 24, 2022. 2007.

[49] Anthony Rose et al. *SECURING BLUETOOTH LOW ENERGY LOCKS FROM UNAUTHORIZEDACCESS AND SURVEILLANCE.* Ed. by Mason Rice and Sujeet Shenoi. Cham: Springer International Publishing, 2017, pp. 319–338. ISBN: 978-3-319-70395-4.

[50] Alexander S. Gillis. *What is the internet of things (IoT)?* https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT. Accessed: May. 21, 2022.

[51] Samsung. *What can your Family Hub™ do for you?* https://www.samsung.com/us/explore/family-hub-refrigerator/overview/#smarthome. Accessed: Mar. 14, 2022. NA.

[52] Freddy K Santoso and Nicholas C H Vun. *Securing IoT for smart home system.* https://ieeexplore.ieee.org/document/7177843. Accessed: May. 22, 2022. 2015.

[53] Sharon Shea. *Privacy Impact Assessment).* https://en.wikipedia.org/wiki/Privacy_Impact_Assessment. Accessed: May. 05, 2022.

[54] Sharon Shea. *smart home or building (home automation or domotics).* https://www.techtarget.com/iotagenda/definition/smart-home-or-building. Accessed: May. 04, 2022. 2020.

[55] smarthomeenergy.co.uk. *What is a Smart Home?* https://smarthomeenergy.co.uk/what-smart-home/. Accessed: Feb. 24, 2022.

[56] Jenny Stanley. *The History of Smart Home Technology.* https://www.familyhandyman.com/article/the-history-of-smart-home-technology/. Accessed: May. 04, 2022. 2021.

[57] EUROPEAN DATA PROTECTION SUPERVISOR. *TechDispatch 2: Smart Meters in Smart Homes.* https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en. Accessed: Mar. 15, 2022.

[58] Vahid Nazari Talooki et al. "Security concerns and countermeasures in network coding based communication systems: A survey." In: *Computer Networks* 83 (2015), pp. 422–445. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2015.03.010. URL: https://www.sciencedirect.com/science/article/pii/S1389128615000961.

[59] Usability.gov. *Usability Evaluation Basics.* https://www.usability.gov/what-and-why/usability-evaluation.html. Accessed: Apr. 25, 2022.

[60] Kaisa Väänänen and Tiiu Koskela. *Evolution towards smart home environments: Empirical evaluation of three user interfaces*. https://www.researchgate.net/publication/220141860_Evolution_towards_smart_home_environments_Empirical_evaluation_of_three_user_interfaces. Accessed: Feb. 24, 2022. 2004.

[61] Wikipedia. *X10 (industry standard)*. https://en.wikipedia.org/wiki/X10_(industry_standard). Accessed: Jun. 02, 2022.

[62] Anhao Xiang and Jun Zheng. *A Situation-Aware Scheme for Efficient Device Authentication in Smart Grid-Enabled Home Area Networks*. https://www.mdpi.com/2079-9292/9/6/989. Accessed: May. 22, 2022. 2020.

[63] Sadık Yıldız and Mustafa Burunkaya. "Web Based Smart Meter for General Purpose Smart Home Systems with ESP8266." In: *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. 2019, pp. 1–6. DOI: 10.1109/ISMSIT.2019.8932931.

[64] TOMASZ ZĄBKOWSKI and KRZYSZTOFl GAJOWNICZEK. *SMART METERING AND DATA PRIVACY ISSUES*. http://krzysztof_gajowniczek.users.sggw.pl/articles/SMART%20METERING%20AND%20DATA%20PRIVACY%20ISSUES.pdf. Accessed: Apr. 28, 2022. 2013.