D4.1

Analyses and Feedback on Architecture Requirements and Goals

WP4 – Privacy Aware Analytics for Security and Services

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/05/2021
Actual submission date: 31/05/2021

Responsible partner: CNR
Editor: Paolo Mori
E-mail address: paolo.mori@iit.cnr.it

28/05/2021
Version 1.0

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The SIFIS-Home Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-02-2020 GA 952652

Authors: P. Mori (CNR), A. Saracino (CNR), G. Giorgi (CNR), W. Alabasi (CNR), J. Jämsä (FSEC), O. Isohanni S. Robinson, S.Kakko (RIOTS), A. Monge Roffarello (POLITO), L. De Russis (POLITO)

Approved by: M. Komssi (FSEC), G. Selander (ERI)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	26/01/2021	P. Mori	CNR	Initial ToC
0.2	17/03/2021	G. Giorgi W. Alabasi	CNR	Sections 2.1 and 2.4
0.3	30/03/2021	J. Jämsä O. Isohanni S. Robinson ,S.Kakko	FSEC, CEN, RIOTS	Section 2.2
0.4	30/03/2021	A. Monge Roffarello L. De Russis	POLITO	Section 2.3
0.5	28/04/2021	P. Mori, A. Saracino, G. Giorgi W. Alabasi, J. Jämsä O. Isohanni S. Robinson, S.Kakko, A. Monge Roffarello L. De Russis	CNR, FSEC, CEN, RIOTS, POLITO	Sections 3 and 4
0.6	29/04/2021	P. Mori	CNR	Section 1 and 5
0.7	30/04/2021	W. Alabbasi	CNR	Section 2
1.0	28/04/2021	P. Mori	CNR	Addressed comments from reviewers. All sections.

Executive Summary

This document provides WP1 "Distributed System Architecture" with feedback and additional input, based on an analysis of the deliverable D1.1 "Initial Architecture Requirements Report" carried out in WP4 "Privacy-Aware Analytics for Security and Privacy Services". The contribution of this document is twofold. First, it provides feedback about and request for adaptations of the requirements defined in D1.1. Second, it provides additional requirements related to the privacy aware analytics for security and privacy services, to be additionally considered in the final SIFIS-Home system and its architecture. Both contributions have considered the planned privacy aware analytics to be developed in WP4, and will be seminal for the deliverable D1.2 "Final Architecture Requirements Report", which in turn will be a guideline for the development of the privacy aware analytics in WP4. The present document has the same purpose fulfilled by the companion deliverable D3.1 "Analyses and Feedback on Architecture Requirements and Goals" in WP3 “Network and System Security”.

Table of contents

1 Introduction

The main objective of the SIFIS-Home project is to provide a secure-by-design and consistent software framework for improving resilience of interconnected smart home systems at all stack levels. To address this goal, the software framework shall ensure correct functionality of the smart home system as well as security, privacy and safety of all SIFIS-Home users. This requires for eliciting requirements especially focused on security and privacy aspects, to be considered and ultimately fulfilled by the SIFIS-Home system.

The SIFIS-Home deliverable D1.1 “Initial Architecture Requirements Report” has provided a set of initial requirements for the SIFIS-Home system. These have been classified as Functional, Non-Functional and Security requirements, as well as according to different priority levels. This first set of requirements has been provided as input to WP3 and WP4, for them to produce feedback, requests of amendments as well as further new requirements to be included in the intended final set to be specified by WP1 in its later deliverable D1.2 "Final Architecture Requirements Report".

This document is the first deliverable from WP4 and provides WP1 with such an aggregated feedback, resulting from a revision of the original requirements in the light of the privacy aware analytics developed in WP4. For consistency, the same taxonomy and requirement priorities considered in D1.1 have been used in this document. In particular, the contribution of this document consists of and is organized as follows.

First, Section 2 provides a high-level overview of the different privacy preserving analytics developed in WP4 for the SIFIS-Home system. These are especially related to the activities carried out in the four Tasks of WP4, and their preliminary version will be documented in deliverable D4.2 “Initial Design and Development of Privacy Aware Analytics for Secure Services”.

Second, Section 3 provides a collection of detailed feedback and requests for amendments about the initial set of requirements elicited in WP1 and documented in deliverable D1.1. In particular, feedback and requests for amendment are provided separately for the initial Functional Requirements (see Section 3.1), Non-Functional Requirements (see Section 3.2) and Security Requirements (see Section 3.3) from deliverable D1.1.

Third, Section 4 provides a collection of newly defined requirements to be added to the final requirement set, in the light of privacy aware analytics developed in WP4. Consistently with deliverable D1.1, each of the new requirement has been assigned a priority level and has been associated with other pertinent relatable requirements from the initial set and/or the new set. In addition, the new Functional Requirements have been also mapped to the pertinent Use Cases elicited in Section 5.2 of deliverable D1.1, while the new Security Requirements have been further classified as either Testable or Non-Testable.

The contribution from this document will act as input to WP1, where it will be seminal for the deliverable D1.2, as intended to provide a final, refined set of requirements for the SIFIS-Home system. In turn, deliverable D1.2 will be a guideline for the development of the privacy aware analytics for security and services in WP4.

Finally, this document has the same purpose fulfilled by the companion deliverable D3.1 "Analyses and Feedback on Architecture Requirements and Goals" in WP3 “Network and System Security”. Therefore, the final set of requirements to be specified in deliverable D1.2 will effectively consider feedback and new input from both WP3 and WP4, as aligned with their technical activities.

2 Privacy Aware Analytics

This section describes the main aims and the desired features of the privacy aware analytics that will be defined in WP4 to enhance the security of the SIFIS-Home framework.

2.1 *Anomaly and Misbehaviour Detection*

In the era of smart connected devices and Internet of Things, a great amount of information and private data are being collected and processed. These networks impose the challenging task of preserving data correctness and integrity and triggering anomalous actions. For the defined connected architecture, attacks on software, services, devices, and data should be detected. Moreover, threats such as device faults and physical intrusions must be discovered and prevented.

Main objective: detection of anomalous behaviours of the actors and components of the SIFIS-Home framework at all levels, from the people performing actions in the smart home to the devices building up the SIFIS-Home framework.

In the following, we present the set of analytics that will be used to provide security as a service, by ensuring a multi-level anomaly and misbehaviour detection and prevention.

- **Device Fault Detection**: as part of home automation and IoT, many concerns have been raised about network reliability, service availability, performance, and better monitoring of the smart home. Fault detection is a critical component of network monitoring and data analysis processes for service restoring and correction action time minimization. Device faults can be of different types such as lightning, power outage, ground faults, circuit faults, etc. The process of device fault detection is illustrated in Figure 1, it works by analysing collected sensor data of humidity, temperature, noise, vibration, and air flows. Then comparing the faulty devices' collected data to the proper ones and finding missing devices or abnormal data deviations. If an anomaly is detected, an alarm will be raised to the resident user and the system administrator.

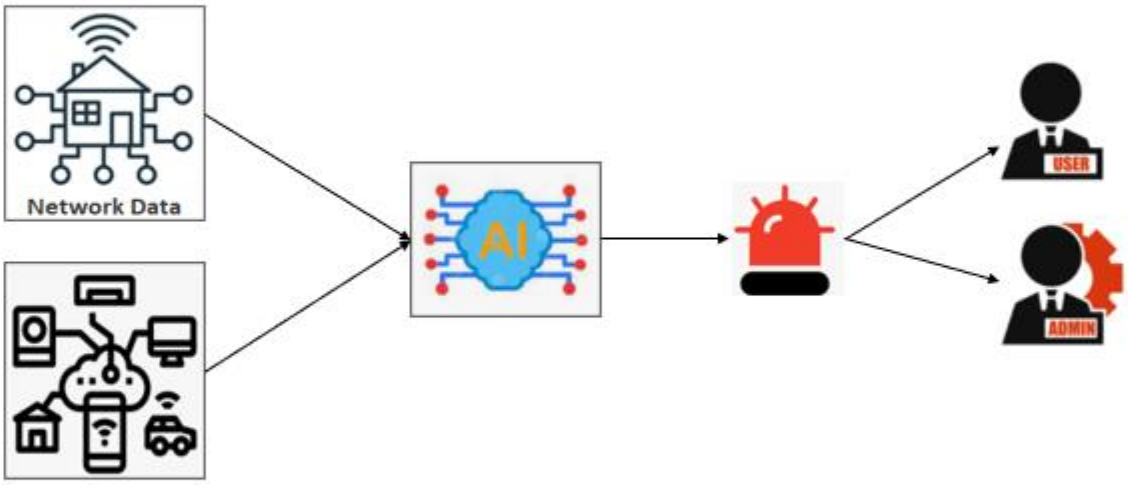

Figure 1: SIFIS-Home-Device Fault Detection

- **Object Detection**: a smart home system must be able to detect anomalous objects that represent major threats and could hardly be identified by humans otherwise. The object detection mechanism is explained in Figure 2, it is done by identifying suspicious objects in captured images or videos and locating them within the image frame. These objects can be an intruder, a fire at home, an elderly person or a small child in a dangerous condition, or harmful objects like sharp tools in an inappropriate location. Therefore, the camera captures images or recording videos, then this collected data is transmitted for analysis. In the analysis phase, object detection is done by identifying the number of objects in an image and classifying them with their specific location in the image, and finally alarming the user if there is any suspicious object detected.

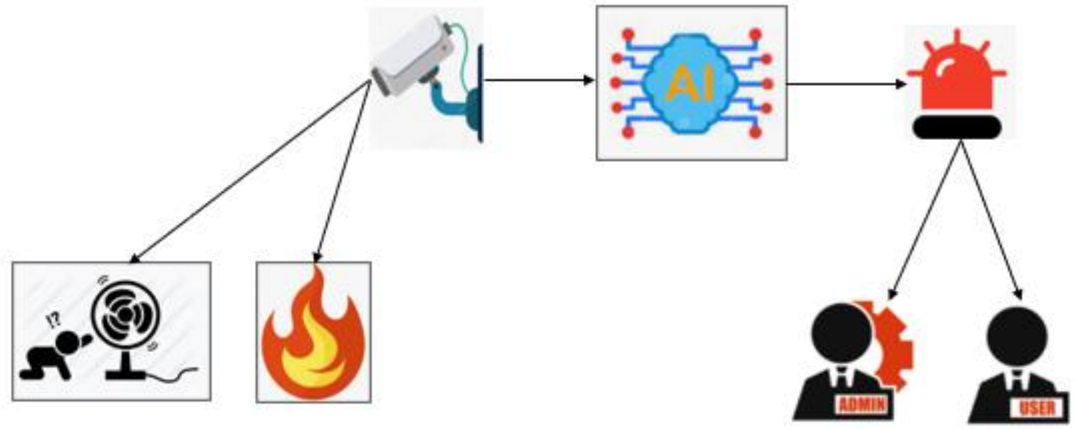

Figure 2: SIFIS-Home- Anomalous Object Detection

- **Parental Control**: Parental control is about monitoring what the children are doing and their behaviour, ensuring that they do not encounter any dangers, restrict their internet access and control their internet usage and smart TV usage for their safety and security. Many examples of situations that children may encounter and cause them danger such as being attacked by someone else, feeling fear or depression, the existence of an unauthorized person at home, being in a harmful physical condition or having a health problem. Parental control can be employed by creating personalized profiles for children based on their behaviours and using predefined rules set by their parents that can be updated continuously based on parents' feedback. Just as Figure 3 shows, the devices continuously collect data, transmit them for analysis, then the system flags any abnormalities with emergency activation based on the risk assessment.

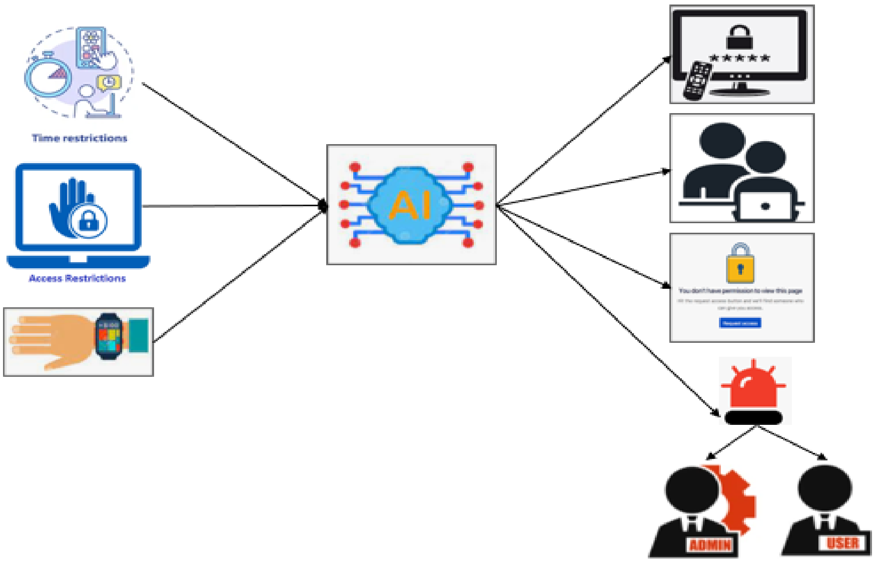

Figure 3: SIFIS-Home Parental Control and Monitoring

- **Face Recognition/ Person Recognition**: Person recognition is critical for identifying home resident users, guests, and intruders. Moreover, to provide smart personalized services to users based on their identities. Face recognition shown in Figure 4 is done by training a model on resident users' images, and when a person enters the home or a certain room in the home, this person’s face image is detected and compared to the trained model to classify the user based on the extracted features.

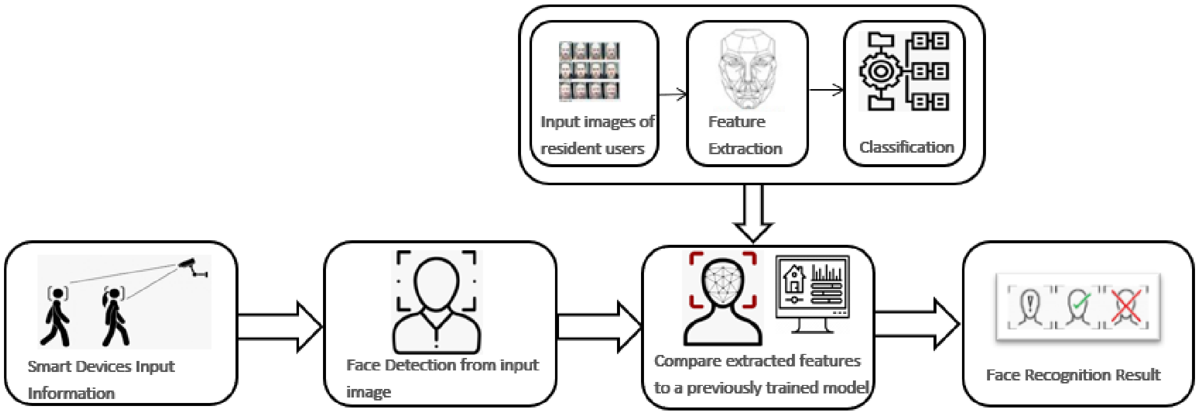
Input images of resident users
Feature Extraction
Classification
Smart Devices Input Information
Face Detection from input image
Compare extracted features to a previously trained model
Face Recognition Result

Figure 4: SIFIS-Home Face/ Person Recognition for user’s identification.

- **Software Intrusion Detection**: Malware is one of the greatest threats to IoT environments due to their heterogeneous architecture. These malware types might be used to perform Distributed Denial of Service (DDoS) attacks, open port scanning, or brute force attacks. The main goals behind these attacks are to stop service or resource availability, to gain access to network resources, or to gain access to private data. There are multiple methods for software intrusion detection: First, there is the signature-based detection method, in which the IDS compares the collected data to a predefined database of features, if there is a match then it is treated as an intrusion. Second, there is rule-based detection, where the IDS compares the collected data characteristics and statistics to a predefined set of rules and thresholds, and it raises an alarm if a threshold is exceeded. Third, there is anomaly-based detection, which compares dataset identified patterns and it enables the detection of new intrusions. The final one is a hybrid technique that combines any of the previous techniques together. Our objective in this project is to use data stream anomaly detection for network resources related to user behaviour and network resources patterns as illustrated in Figure 5.

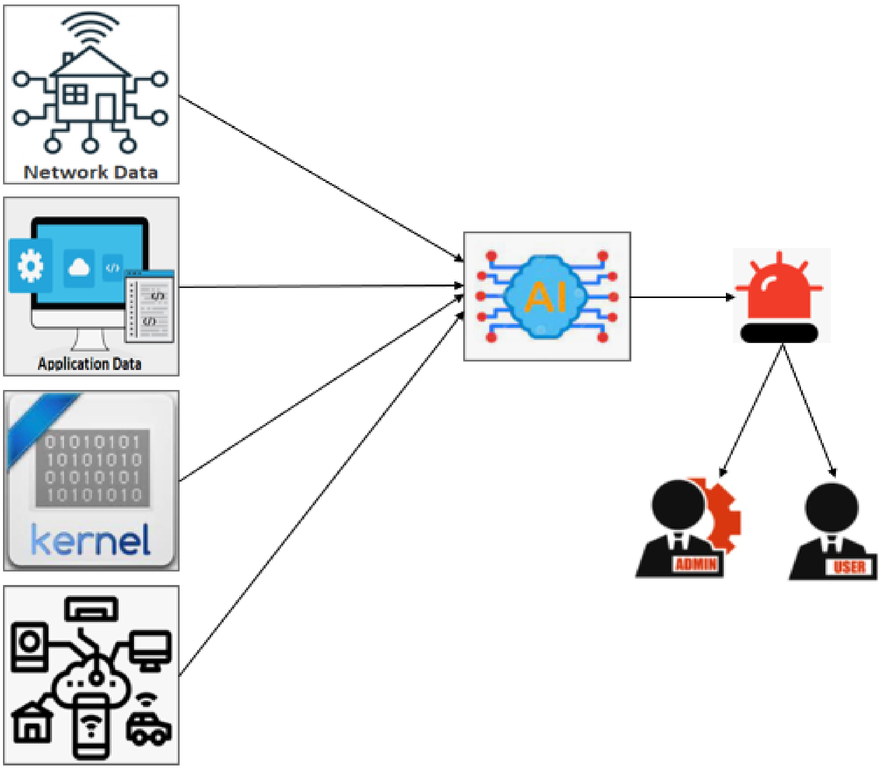

Figure 5: SIFIS-Home Intrusion Detection using data streams anomaly detection

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Detection**: DoS occurs when system resources become overwhelmed and flooded with service requests, causing the service to be denied from its legitimate users. The main purpose behind this attack is to shut down the service and cause system resources to be inaccessible. The major threat of this attack is that the attacked devices can be used as botnets for future DDoS attacks. DoS attacks are one type of malware and can be detected using one of the previously mentioned methods and reported in Figure 5. Our objective in this project is to use data stream anomaly detection for network resources by analysing devices' communication patterns, detecting anomalous outliers, and raising an alert to the resident users and system administrator.
- **Multi-level Intrusion Detection**: This is about detecting intrusions from a whole system perspective at all levels using the same approach illustrated in Figure 5. It aims to flag abnormal behaviours by analysing user, system (kernel), hardware and network collected information and classify them either as an intrusion or a normal behaviour. Data collected such as Network traffic, packets information and flow duration, system calls, and hardware information are analysed by the system. If an intrusion has been flagged, an alert will be raised for the resident users and the system administrator.

2.2 *Network Intrusion Detection*

When we consider IoT networks and devices, security is still a relatively new topic. Many devices are not designed with security built-in, meaning that the security is not at a sufficient level before it is delivered to consumers. By using efficient methods for intrusion detection, the risks of malicious activity can be reduced regardless of the device.

An anomaly based NIDS (network intrusion detection system) monitors all the traffic flowing through the network and compares it to what is established as normal traffic based on protocols, devices, ports, addresses packet counts and bytes. Signature based systems use known threats to identify malicious content but fail to detect zero-day vulnerabilities.

The network intrusion detection task concerns the monitoring and analysis of network traffic with the main objective being able to detect and respond to malicious activity and threats against IoT devices within the SIFIS-Home network (i.e., being enlisted a bot-net etc.)

We aim to detect malicious activity in the SIFIS-Home network via the detection of anomalous network traffic. We assume that we only have access to network flow data and cannot perform packet inspection nor have ability to monitor processes running on devices in the network. Additionally, the proposed solution should be able to handle encrypted traffic, e.g., HTTPS.

The anomaly detection will be carried out in a device specific manner and only for “not-so-smart” devices, that is, devices for which we assume some “baseline” of normal activity can be established. We assume that since a smart phone or personal computer can run arbitrary processes with highly variable network activity, the likelihood that a detected anomaly corresponds to any malicious activity of interest is very low and such a system will result in too many false positive alerts.

Either the output of the anomaly detection feature should be able to be communicated in an understandable and actionable way to the resident (admin) user of the SIFIS-Home system or the response should be automatic. Furthermore, the solution needs to be cost effective from a computational point of view. For example, typical consumer WiFi routers do not have extra computational or memory capacity that can be utilised for additional security features.

Main Objective: The objective of this task is to research methods to use network traffic for developing an anomaly-based detection model that identifies malicious traffic within the network. Network traffic that can be used for this process is either full packet capture format or flow based. Typical values included in the flow are timestamps, source and destination address, ports, layer 4 protocol (TCP, UDP…) and number of bytes and packets.

Security threats are more prevalent and more complex than earlier. Increased traffic line rates demand more resources for analysis. Filtering only the relevant traffic helps to save resources and make the analysis more efficient.

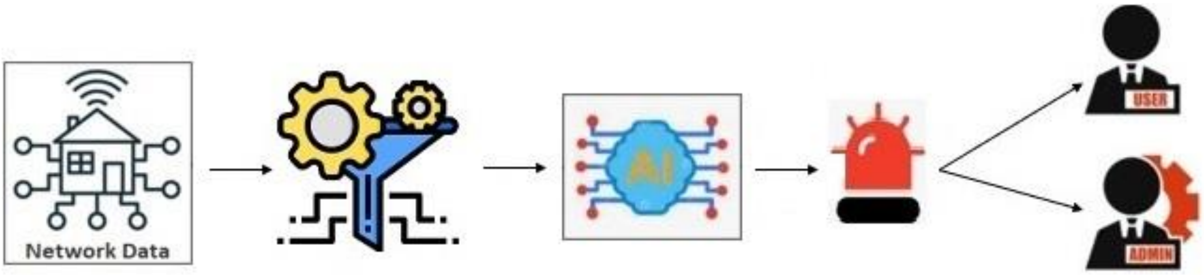

Figure 6: SIFIS-Home Real Time Anomaly Detection

In the first phase, lightweight analysis will be made on an edge network to detect real-time anomalies like in Figure 6, regardless of the result data is sent to the centralized processing engine.

Network data will be analysed by using deep learning methods. This requires baseline network conditions. In this case every allowed node is active and sent their data. Based on the timestamp, header or length, misbehaviour can be detected. Over the normal situation, true false information is needed to learn abnormal traffic.

Comparing Host Based Intrusion Detection (HIDS) In Network-based Intrusion Detection (NIDS), only information that can be seen on flow or captured data can be used as a basis of analysis. This information is time-related data (interval and timestamp), overall byte count, header information, destination/source address, destination/source port and even payload, when it is not encrypted.

Rules should be tight enough to identify malicious network activity. In this way a lot of false alarms will arise. Detected alarms should be informed either to the user or admin based on the alert level. Admin can confirm or reject the alert, for example if a new node is added to the network.

The proposed solution in Figure 7 is an AI-based intrusion detection and response system operating in a cloud backend. The security SDK on the home router sends data to the backend, for which a "baseline" of normal traffic pattern has been learnt at a specific device level. Subsequent network traffic is then compared against the baseline to determine whether an anomaly has occurred. We will compare the proposed solution against the current state of the art and existing solutions.

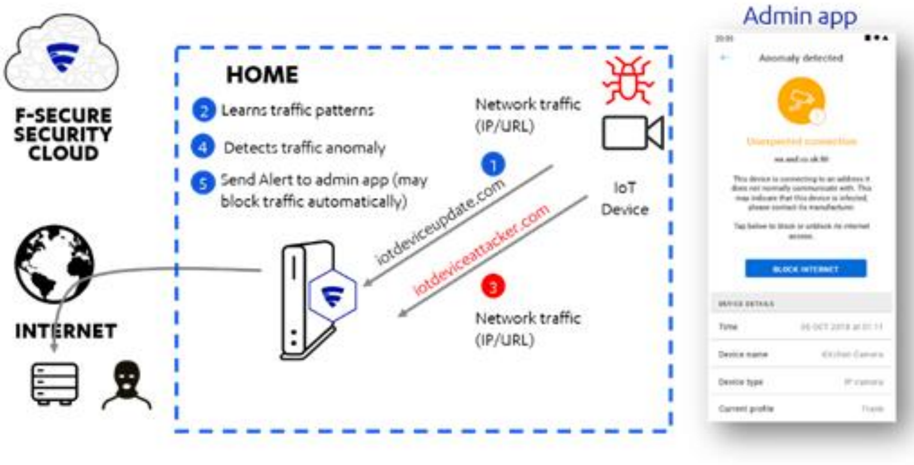
F-SECURE SECURITY CLOUD
HOME
2 Learns traffic patterns
4 Detects traffic anomaly
5 Send Alert to admin app (may block traffic automatically)
Network traffic (IP/URL)
1
iotdeviceupdate.com
iotdeviceattacker.com
3
Network traffic (IP/URL)
IoT Device
INTERNET
Admin app
Anomaly detected
Unexpected connection
This device is connecting to an address it does not normally communicate with. This may indicate that this device is infected, please contact its manufacturer.
Tap below to block or unblock its internet access.
BLOCK INTERNET
DEVICE DETAILS
Time
Device name
Kitchen Camera
Device type
IP camera
Current profile

Figure 7: SIFIS-Home AI-based Intrusion Detection and Response Solution

In addition, we also aim to collect and formulate a set of high-level qualitative parameters for network traffic analysis based on data stream characteristics during task 4.2. illustrated in Figure 8. The data stream is measured on three different levels: 1) network level, 2) device level, and 3) network section level.
The objective is to gain awareness and knowledge of

- the amount of data travelling to and from a specific NSSD/node in the SIFIS-Home network
- the amount of data travelling within the network through NSSDs/nodes.

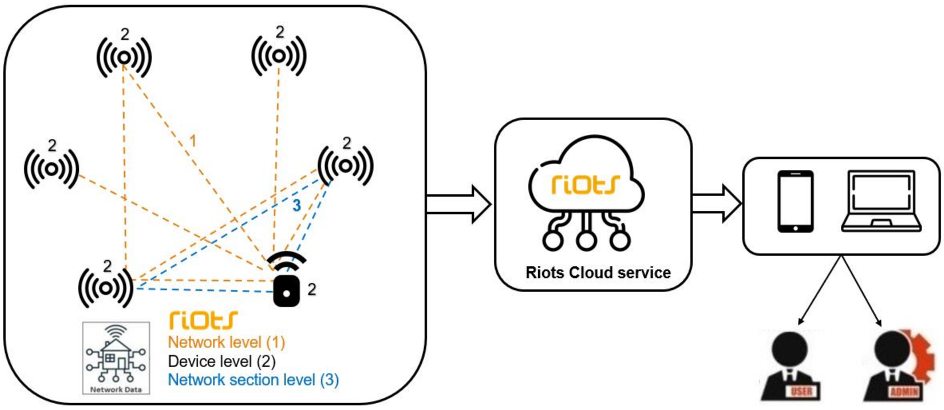

Figure 8: SIFIS-Home Network Traffic Analysis using collected data characteristics

With this type of knowledge of data streams and data flow, the next aim is to augment the gathered data utilization in the form of machine learning and artificial intelligence through which we can examine how the data streams fluctuate based on time, season, and surrounding circumstances, or other parameters of interest derived from the data stream.

2.3 *Policy Enforcement*

In the contemporary Internet of Things (IoT) era, people can interact with a multitude of smart devices and applications, always connected to the Internet, in the majority of today’s environments, including the smart home. The result is a complex network of connected entities, be they physical devices or virtual services, that can communicate with each other, with humans, and with the environment. In this complex scenario, even users who do not have programming skills should be able to easily and efficiently control the behaviours of their devices and services. To preserve the security and the integrity of their smart home environments, in other words, they should be able to define *high-level policies* on their devices and services, without the need of knowing (and specifying) details that strongly depend on the underlying technology. In this section, we summarize the main goals of the Policy Enforcement task, and we present a list of analytics that could allow users to program the behaviour of their smart-home environments via policies expressed in a technology-independent, abstract way.

Main Objective. The Policy Enforcement task aims to support users to express high-level policies like “Do not record sound in the living room tonight”. These policies are defined in previous Work Packages and are responsible for triggering a reconfiguration of all the devices and applications involved in a given smart home to comply with the underlying policies description. The goal is to *map* high-level policies into device-level configurations, when possible. Stemming from a high-level policy, for instance, the system could limit the features of a smart home device, or it could inhibit the operation of a non-reconfigurable device. In addition, it could verify whether a given home configuration is compatible with one or more active (or suggested) policies. Such a translation process, in particular, will leverage the secure API mechanism introduced in Work Package 1, and the Policy-based Software Security Compliance defined in Work Package 2.

Analytics

- **Concept Modelling:** high-level policies need to be modelled with a well-defined formalism in order to be analysed and mapped into device-level configurations. The same is true for other concepts involved in the translation process, e.g., smart-home devices and their capabilities. A straightforward way to model concepts and their relationships is using the Semantic Web framework, and, in particular, ontologies. Ontologies are a fundamental part of the Semantic Web framework that are used for formally defining classes, attributes, and relationships between these concepts in a specific domain. Ontologies and, in general, the Semantic Web framework offer several benefits:
  - *reasoning capabilities:* semantic reasoning can be used to infer information that has not been explicitly spoken about, thus facilitating the mapping between abstract information to low-level details needed to actually execute device-level reconfigurations;
  - *data integration and reuse:* the continuous growing of the IoT ecosystem raises the question of how new connected entities can be easily integrated in existing smart environments. Semantic technologies offer by nature advantages in terms of data reuse and integration, thus making it easy to integrate new devices and online services;
  - *meaningful information:* in a semantic model, and, in particular, in a OWL ontology, data is enriched with semantic information, i.e., meaning. Thanks to such a semantic, we can easily perform queries on the representation such as “which smart devices or online services can perform a particular action?” or “which connected entity can generate a particular event?”;
  - *concept hierarchies:* a semantic model is described as a graph that embeds inheritance relationships among concepts, thus allowing the definition and the linking of multiple levels of abstraction with ease.
- **Policy Mapping:** the most important analysis of the Policy Enforcement task is the mapping of the high-level policies specified by the user into a set of device-level configuration as shown in Figure 9. This process will be implemented by a semantic-powered gateway that will exploit all the capabilities of the Semantic Web framework to perform such a process automatically, by reasoning on the capabilities of the devices owned by the user. For a policy like “Do not record sound in the living room tonight”, in particular, the semantic-powered system will extract all the devices that have the capability of recording audio, and it will produce a set of device-level configurations that should be used to temporarily disable such capabilities.

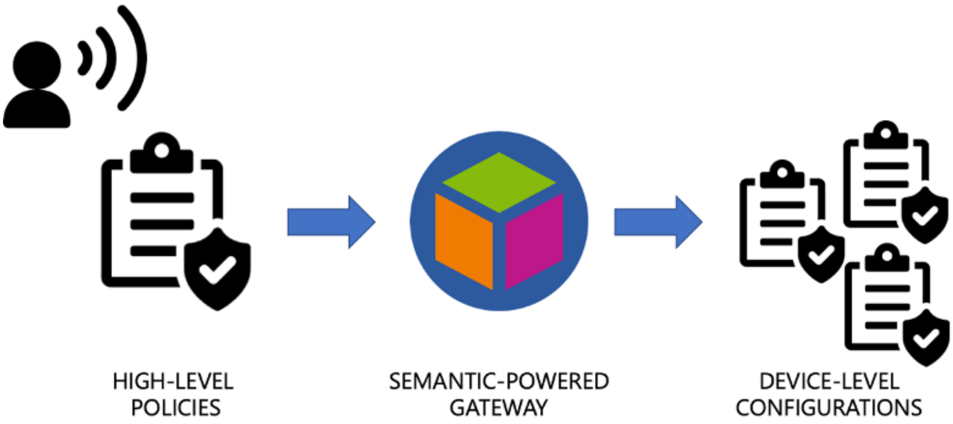

Figure 9: SIFIS-Home High Level Policies Mapping

- **Policy Application:** besides translating high-level policies into device-level configurations, the semantic-powered gateway should also decide *when* to apply the translated configurations and on *which* devices. For a policy like "Do not record sound in the living room tonight", for example, the gateway should select all the devices with audio-recording capabilities that are installed in the living room and that can be activated at night. This process will exploit the reasoning capabilities of the semantic-powered gateway, that will analyse contextual information (e.g., user information, device locations, and time information) to decide how to apply the translated device-level configurations. By reasoning on this information, the gateway will also be able to *check* devices and service with respect to the user's policies, e.g., by generating a list of the devices/apps that respect one (or more) given policies, or by verifying if a newly inserted device/app violates one (or more) policies, this mechanism is illustrated in Figure 10.

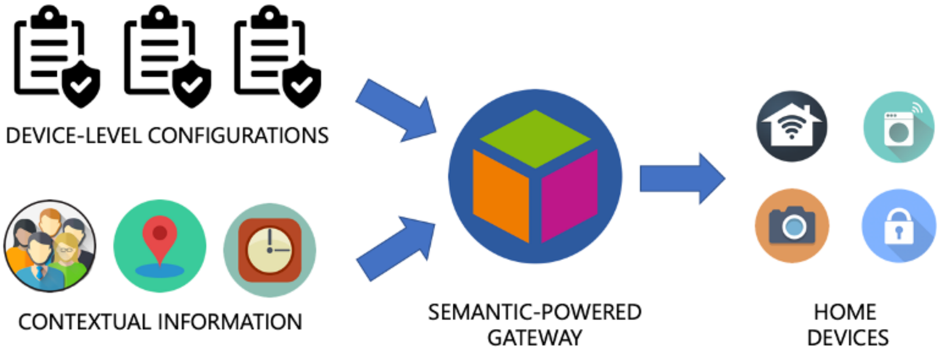

Figure 10: SIFIS-Home High Level Policies Application mechanism

2.4 *Privacy Aware Speech Recognition*

In the smart-home context, sensors and actuators are becoming pervasive and unobtrusive. They can produce a lot of information to enhance the quality of living or ensure the environment's safety and security. Audio information are easily gathered through several smart devices that can have an embedded microphone. With the development of new artificial intelligence techniques, audio information can be exploited to understand the environmental context, the presence or not of persons, their identities but also to detect anomalies or to make easier the control of the smart-environment to the persons with limited physical abilities. However, the audio information can contain personal and sensitive information that can be preserved during the data analysis. This section presents a list of analytics based on audio signals used to enhance the smart-home environment's safety and security, taking into consideration the privacy aspect in the analysis of sensitive information.

Main objective: identification and authentication of users, detection of minors and detection of anomalies through voice analysis, translation of speeches into text.

In the following, we present the set of analytics that will be used for implementing privacy aware speech recognition.

- **Speaker verification through voice analysis:** The speaker verification is the process of authentication of a person exploiting the human biometric voice aspect. The use of this aspect can guarantee unobtrusiveness to the authentication mechanism ensuring a good level of security. Such service is exploited by the SIFIS-HomeHome system to verify the identity of the person which is intended to use a protected smart-device such as in the mechanism illustrated in Figure 11.

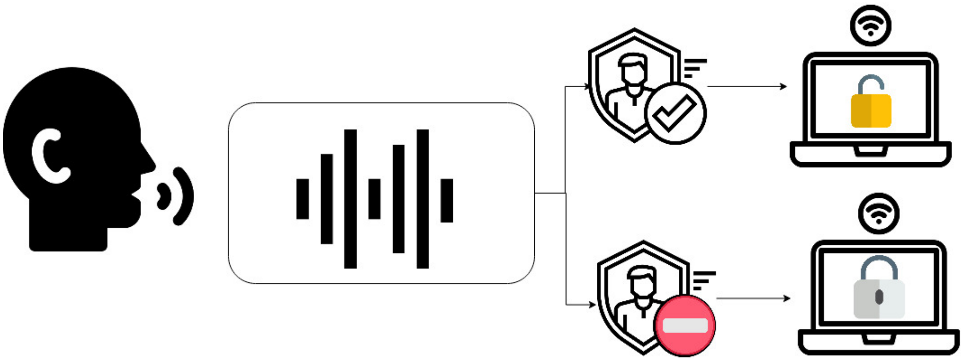

Figure 11: SIFIS-Home Speaker verification using voice analysis techniques

- **Speaker identification through voice analysis:** Speaker recognition is the identification of a person from characteristics of their voice. In the SIFIS-Home environment, it is fundamental to understand the identity of a person in order to grant the right privileges according to the policies set for that person. In our scenario shown in Figure 12, the speaker recognition system will be run in the background to understand the identity of the persons present in the environment and it will communicate them to the smart-home control manager which will grant the execution of some actions on the basis of the policies set, e.g., the use of a smart-device will be possible only if a set of persons are identified in the environment.

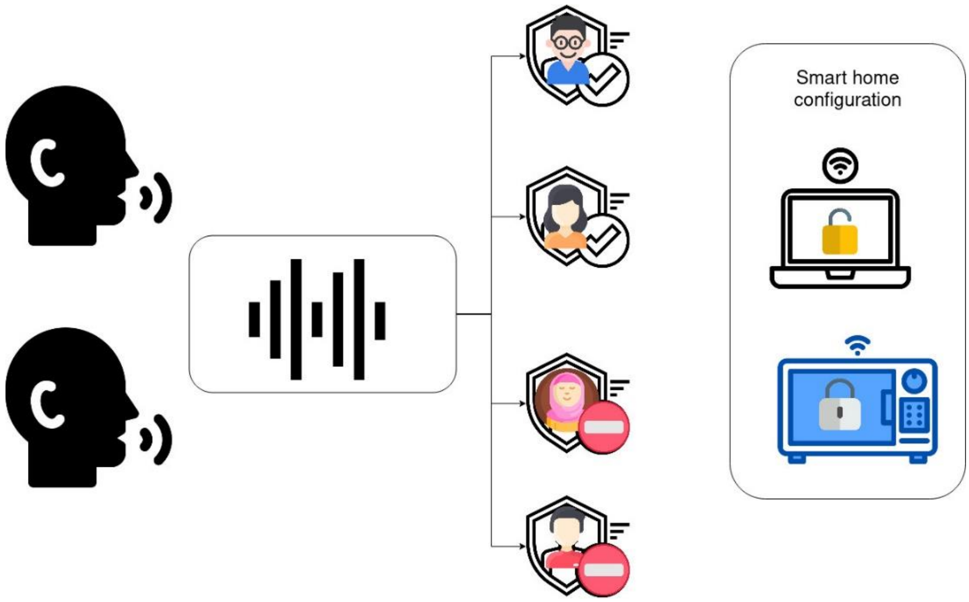

Figure 12: SIFIS-Home user recognition using voice analysis techniques

- **Speech to text for managing smart-home components:** The speech to text or Automatic Speech Recognition (ASR) tool is a system that uses a Natural Language Understanding algorithm to sort auditory signals and transform that information into words. In the SIFIS-Home system, speech understanding is fundamental in order to control the smart-environment, e.g., turning on/off smart devices, regulate the volume, open/close windows and so on. The voice control analysis function illustrated in Figure 13 allows to managesmart-devices without a direct physical interaction, thereby providing not only an easier control of the devices but also allowing persons with limited physical abilities to interact with the smart-home.

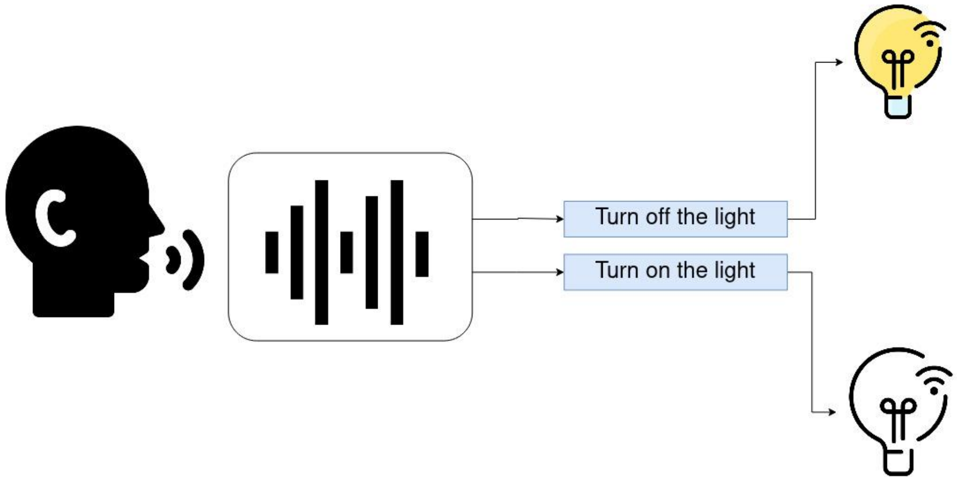

Figure 13: SIFIS-Home Automatic Speech Recognition by converting speech to text

- **Voice anonymization:** The audio information gathered in the smart-home can contain personal and sensitive information of the persons present in the home. Granting cloud-based services the permission to analyse such information can be unsafe. The SIFIS-Home system should provide a voice anonymization analysis such as that shown in Figure 14, which is able to recognize the speech, understand the sensitive information (name, surname, telephone numbers, email addresses, ...) and anonymize them before forwarding them outside. Exploiting this analysis, the SIFIS-Home system can provide an additional level of protection of users' vocal data while maintaining the advantages of using cloud-based services.

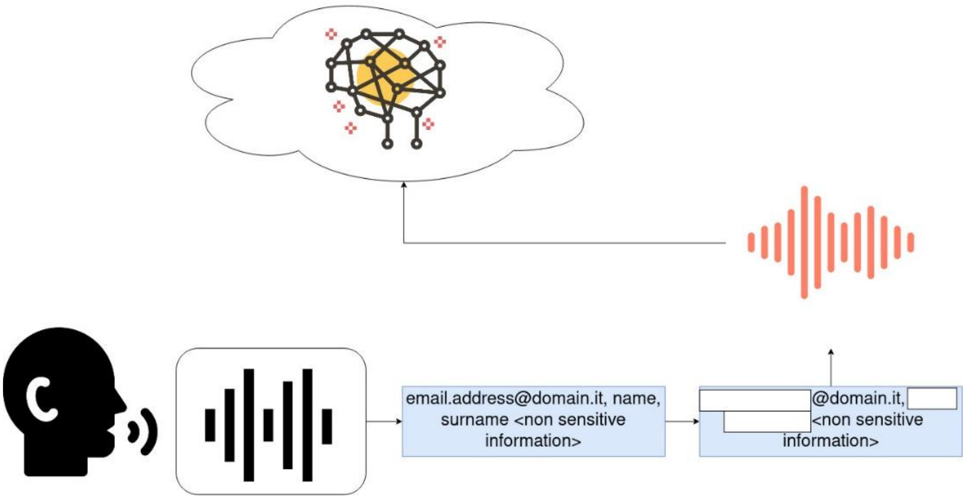
email.address@domain.it, name, surname <non sensitive information>
@domain.it, <non sensitive information>

Figure 14: SIFIS-Home Audio information Anonymization

- **Anomaly detection in audio signal analysis:** Anomaly detection in a smart-home environment is a fundamental task that guarantees safety to the smart-home tenant, its mechanism is explained in Figure 15. A useful level of information analysable to detect anomalies is represented by the audio signal measured in the smart-home. The SIFIS-Home system should provide an anomaly detection system - based on the analysis of audio signals - that is able to distinguish normal audio patterns from abnormal ones. If an anomaly is detected, an alarm will be raised to the resident user and the system administrator.

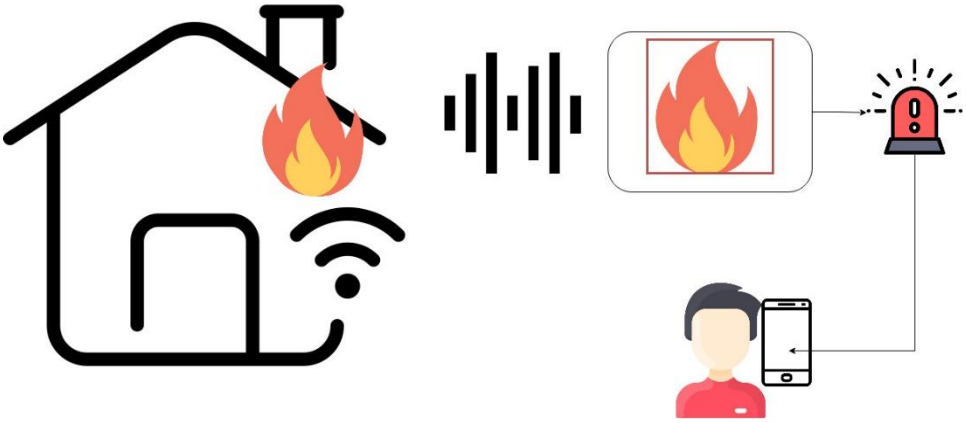

Figure 15: SIFIS-Home Audio Signal Analysis for Anomaly Detection

- **Parental control analysing audio signal:** The smart-home allows the people in the house to easily access a large number of smart devices or contents (e.g., smart-TVs, tablets, PCs, smart-oven), being some of them addressed to adults only, or requiring the presence of an adult for a child to safely use them. Hence, an issue that arises in the smart-home is that children or minors can very easily use devices that are not meant for them. The parental control system becomes a fundamental tool to guarantee safety in the smart-home environment. The analysis of the vocal signal mechanism - illustrated in Figure 16 - is capable of providing useful information about the age of a person. The SIFIS-Home system should provide an age estimator tool that exploits the vocal signal of people to recognize their ages and grant access to the devices according to the policy set.

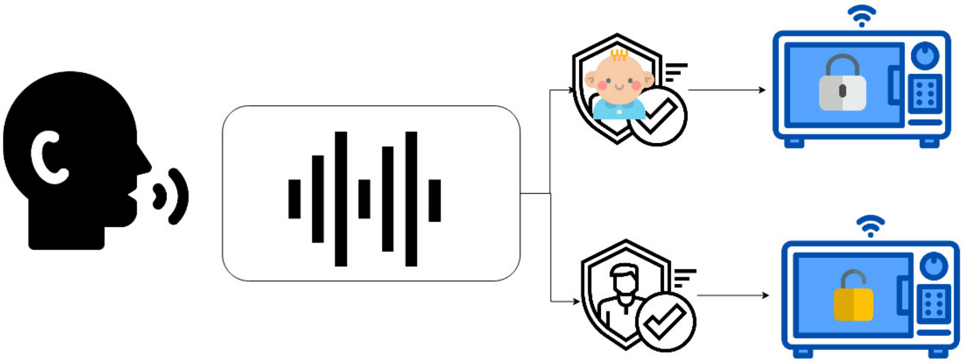

Figure 16: SIFIS-Home Audio Signal Analysis for Parental control and monitoring

3 Feedback and Request for Adaptations to Requirements Defined in D1.1

This section analyses the requirements defined in D1.1 in the light of the security solutions that will be designed in WP3. As a reminder, the requirements are grouped into three different categories associated to their priority level, namely Critical (C), Standard (S) and Optional (O).

For each considered security requirement, an overall feedback is provided under the "Feedback" column of the following tables, with one of the following values defined below. When appropriate, side comments are provided under the "Comments" column of the tables.

- **OK** – The considered requirement is fine as is.
- **Refine** – The considered requirement can be improved to be more accurate and comprehensive, as explained by the side comments.
- **Amend** – The considered requirement conflicts with new requirements related to security solutions from WP3 as listed later in Section 5, and/or with the network & system security solutions as such (see Section 2). Thus, the requirement should be updated in order to solve the conflict, as explained by the side comments.
- **Delete** – The considered requirement is not appropriate and should be removed, due to the reasons explained by the side comments.

3.1 *Functional Requirements Analysis*

The following Table provides a list of feedback and request of amendments to the functional requirements defined in Section 6.1 of D1.1.

Req	**Req. Description**	**Priority**	**Feedback**	**Comments**
F-01	The SIFIS-Home framework shall provide a means of identifying the users inside the smart home through biometrics.	C	ok	
F-02	The SIFIS-Home system shall provide a means of authentication to the resident users and administrators inside the smart home.	S	ok	
F-03	The SIFIS-Home system shall match read biometrics with a database of stored ones.	S	ok	
F-04	The system shall activate features based on the user identity.	S	ok	
F-05	The system shall activate a guest profile when the identity of the biometrics is not recognised.	S	ok	
F-06	The SIFIS-Home system shall provide a means of recognition of allowed users in the smart home.	C	Refine	This requirement seems to overlap with F-01. Assuming that the focus of this requirement is on assigning the access rights to the identified users (to determine if they are allowed to do something), we suggest rephrasing this requirement. Moreover, the non-functional requirements linked to this functional requirement should take into account also accuracy issues (false positive/negative). Hence, we suggest to add a dependency with a non-functional requirement concerning detection accuracy, such as DE-01.
F-07	The SIFIS-Home system shall provide Automatic Speech Recognition (ASR) to provide the residents the facility to control their home appliances through their speech.	C	Refine	This requirement applies only to resident users. However, administrators should be able to control home appliances through voice commands as well.
F-08	The SIFIS-Home system shall receive	C	Refine	The SIFIS-Home system

	and interpret the voice commands provided by the user.			shall receive the voice commands provided by the user and it shall be able to interpret those commands belonging to a predefined command set.
F-09	The SIFIS-Home system shall be able to execute all the recognisable voice commands.	C	Refine	Since the sentence "all the recognizable voice commands" could be ambiguous, this sentence should be replaced with "a predefined set of recognizable voice commands".
F-10	The SIFIS-Home system shall signal the presence of an intruder when the identity is not recognised, and no residents are at home.	C	ok	
F-11	The SIFIS-Home system shall record intruder actions through cameras.	S	ok	
F-12	The SIFIS-Home system shall store the identity of the intruder if the face is recognised.	O	Refine	This requirement does not specify any constraint in the case the intruder is not recognized, which is a possible situation. Hence, this requirement should be integrated by specifying that, in case the intruder is not recognized, the video and audio recordings must be stored by the system as well.
F-13	The SIFIS-Home system may grant the access to recording to the maintainer.	S	ok	
F-14	The SIFIS-Home system may allow to contact police to receive assistance in case of intrusions.	O	ok	
F-15	The SIFIS-Home system shall provide a means of identifying anomaly behaviours inside the smart home.	C	ok	
F-16	The SIFIS-Home system shall provide a means of recognition of allowed users in unusual locations or performing dangerous actions.	S	ok	
F-17	The SIFIS-Home system shall provide a means of recognition the prohibited objects inside the smart home.	S	Refine	The non-functional requirements linked to this functional requirement should take into account

				also accuracy issues (false positive/negative). Hence, we suggest to add a dependency with a non-functional requirement concerning detection accuracy, such as DE-01.
F-18	The SIFIS-Home system shall provide a means of recognition of allowed objects in unusual positions.	O	Refine	The non-functional requirements linked to this functional requirement should take into account also accuracy issues (false positive/negative). Hence, we suggest to add a dependency with a non-functional requirement concerning detection accuracy , such as DE-01.
F-19	The SIFIS-Home system shall identify and isolate infected devices.	C	Refine	A precise definition of "isolation" should be given. The definition could be embedded in this requirement or in a general definition table valid for all requirements.
F-20	The SIFIS-Home system shall notify the user when malware is detected.	C	ok	
F-21	The SIFIS-Home system may execute self-healing algorithms to transfer functionalities of isolated devices to the others.	C	Refine	This requirement may need to be rephrased once a precise definition of "isolation" has been given.
F-22	The SIFIS-Home system may allow means of verifying that the malware has not spread to other devices.	S	ok	
F-23	The SIFIS-Home system shall allow the resident user to register a new device.	C	ok	
F-24	The SIFIS-Home system shall provide a list of the registered devices to the user along with their characteristics.	C	ok	
F-25	The SIFIS-Home system shall allow the user to unregister a registered device.	C	Refine	Since the users allowed to unregister a device will be "resident users" and "administrators", the requirement should specify "resident users and administrators" instead of "user".
F-26	The SIFIS-Home systems shall	C	ok	

	expose a section where the resident users and administrators can configure the devices.			
F-27	The SIFIS-Home system shall prompt the user when unsolicited configuration changes are propagated to the devices.	S	ok	
F-28	The SIFIS-Home system must provide a marketplace function for the download of third-party applications on smart devices.	C	ok	
F-29	The SIFIS-Home system shall provide information about the safety and security aspects of an application to the user.	C	ok	
F-30	The SIFIS-Home system must provide a feature to show the administrator a list of currently active policies.	S	ok	
F-31	The SIFIS-Home system must allow the administrator to configure the policies to restrict/enable access to functionalities.	C	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-32	The SIFIS-Home system must allow the administrator to configure policies for groups of users.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-33	The SIFIS-Home system must allow the administrator to configure policies for group of devices.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-34	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of users.	S	ok	
F-35	The SIFIS-Home system must allow the administrator to see the list of features/resources that are allowed or forbidden for all groups of devices.	S	ok	
F-36	The SIFIS-Home system must provide the user with a feature to list all the currently available profiles.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the

				whole document.
F-37	The SIFIS-Home system must allow the user to configure its profiles.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-38	The SIFIS-Home system must allow the user to switch his/her current profile.	O	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-39	The SIFIS-Home system should show the user a summary of the preferences associated to its current profile.	O	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-40	The SIFIS-Home system should show notifications to the user when the current profile is changed.	O	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-41	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of devices to the administrator.	S	ok	
F-42	The SIFIS-Home system should offer aggregate analytics and statistics about the usage of profiles to the administrator.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-43	The SIFIS-Home system must offer remote log-in features to a configurer/maintainer of user profiles.	S	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
F-44	The SIFIS-Home system shall offer a panel with the remote houses that can be managed by a maintainer.	S	ok	
F-45	The SIFIS-Home system must offer the maintainer a panel to react in case of intrusions.	S	ok	
F-46	The SIFIS-Home system shall store personal resident information (video, audio, text).	C	ok	

3.2 *Non-Functional Requirements Analysis*

The following Table provides a list a list of feedback and request of amendments to the non-functional requirements defined in Section 6.2 of D1.1.

Req	Req. Description	Priority	Feedback	Comments
PE-01	The user authentication shall happen in less than 2s.	C	Refine	This requirement overrides requirement PE-04 which requires that the user authentication must be performed in less than 5 seconds.
PE-02	The user recognition (identification) shall happen in less than 2s.	C	Refine	Since the automatic identification of users will be performed through biometric means (face recognition, voice recognition), requirements PE-02 and PE-03 should be merged in one requirement.
PE-03	Identification through biometrics should be performed in less than 5 seconds.	S	Delete	Same as PE-02.
PE-04	Biometric-based authentication should be performed in less than 5 seconds.	S	Refine	This requirement is somehow in conflict with requirement PE-01 which requires that user authentication must be performed in less than 2 seconds.
PE-05	Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.	S	ok	
PE-06	Recognition of the start of an interaction through voice command should be performed in less than 2 seconds.	S	ok	
PE-07	The interpretation of the voice commands provided by the user should be performed in less than 2 seconds.	S	ok	
PE-08	The execution of the commands should be performed in less than 5 seconds.	S	Refine	This requirement supposes that the execution time of all the commands supported by the SIFIS-Home framework will be less than 5 seconds. Since we cannot make this

				assumption, this requirement should be refined as follows: "A command should be invoked within 5 seconds from the event that triggered its execution".
PE-09	The maintainer must be able to access and watch the recording in less than one minute.	S	ok	
PE-10	The SIFIS-Home system shall contact police to receive assistance in less than 30 seconds.	O	Refine	Instead of the term “police”, it would be better to be more general. For instance, “police” could be replaced with “law enforcement or private surveillance services”.
PE-11	Identification of installed malware should be completed in less than 60 seconds from the execution of malware.	O	Refine	Depending on the detection technique used, the presence of a malware can be detected only when the malware begins to behave maliciously. Hence, this requirement should be refined to take into account the time elapsed from the moment when the malware begins to behave maliciously.
PE-12	The user should be informed of the presence of a malware in 5 seconds after the malware is recognised.	S	ok	
PE-13	Self-healing algorithms should be started in less than 60 seconds if available when malware is recognised.	C	ok	
PE-14	The registration of a new device should be completed in less than 30 seconds.	S	ok	
PE-15	The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.	S	ok	
PE-16	The de-registration of a device should be completed in less than 30 seconds.	S	ok	
PE-17	The configuration changes should be propagated successfully in less than 30 seconds.	C	Refine	A precise definition of "configuration" should be given in a definition table and should be used throughout the whole document. This would help

				in evaluating the time required to propagate it.
PE-18	The current configuration of a device should be retrieved in less than 10 seconds.	S	ok	
PE-19	The marketplace should be accessed in less than 60 seconds.	S	ok	
PE-20	The configuration of policies for groups of users should be applied in less than 60 seconds.	C	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
PE-21	The configuration of policies for groups of devices should be applied in less than 60 seconds.	C	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
PE-22	The list of policies should be retrieved in less than 30 seconds.	S	ok	
PE-23	The configuration of profiles should be applied in less than 60 seconds.	C	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
PE-24	The change of current profile should be performed in less than 60 seconds.	C	Refine	A precise definition of "policy" and "user profile" should be given in a definition table and should be used throughout the whole document.
PE-25	The statistics about usage of devices should be presented to the administrator in less than 30 seconds.	S	ok	
PE-26	The statistics about usage of profiles should be presented to the administrator in less than 30 seconds.	S	ok	
PE-27	Remote log-in should be performed in less than 60 second.	C	ok	
RE-01	The system shall not fail more than once a week (on average).	C	ok	
RE-02	The system shall not take more than one day to be repaired (on average).	C	ok	
AV-01	The system shall be available 99%	C	ok	

	of the time.			
AV-02	The SIFIS-Home system shall ensure basic services availability in case of system failures.	C	ok	
US-01	The system shall be easy to use for average tech users.	C	Refine	A precise definition of "average tech users" should be given in a definition table and should be used throughout the whole document.
US-02	The SIFIS-Home system shall anticipate strange, dangerous, or critical situations and raise an alert.	C	Refine	The requirement should be rephrased to better specify what "anticipate" means.
US-03	The SIFIS-Home system shall be autonomous and learn based on the users' habits.	C	ok	
US-04	The SIFIS-Home system shall consider special cases in its design, such as colour blindness.	O	ok	
US-05	The SIFIS-Home system shall preserve consistency among all devices, related database and constraints.	C	ok	
US-06	The SIFIS-Home hardware components should be easy to use for the elderly and users with no engineering background.	O	ok	
US-07	The SIFIS-Home system shall have an explorable interface.	S	ok	
US-08	Proper and easy hardware installation should be considered.	S	ok	
US-09	The identification through biometrics should be performed by the system in a radius of at least 10 metres from the device.	S	Refine	This requirement should be refined by specifying that it refers to a single room (interior) or to an open space (exterior).
US-10	An untrained user should be able to recognise an intrusion in the SIFIS-Home system and contact the authorities in less than 1 minute.	C	Refine	This requirement should better specify which are the actions that an untrained user should be able to perform to recognize an intrusion in the SIFIS-Home.
US-11	An untrained user should be able to recognise a software intrusion in less than one minute.	C	Refine	This requirement should better specify which are the actions that an untrained user should be able to perform to recognize a software intrusion.
US-12	An untrained user should be able to perform the device registration	S	ok	

	procedure in less than 5 minutes.			
US-13	An untrained user should be able to perform the device de-registration procedure in less than 5 minutes.	S	ok	
US-14	An untrained user should be able to perform the configuration of devices in less than 5 minutes.	S	ok	
US-15	An untrained user should be able to perform the installation of an application in less than 5 minutes.	S	ok	
US-16	An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.	S	ok	
US-17	An untrained user should be able to complete the configuration of policies for groups of devices in less than 5 minutes.	S	ok	
US-18	An untrained user should be able to complete the configuration of profiles in less than 5 minutes.	S	ok	
US-19	An untrained user should be able to perform a profile change in less than 30 seconds.	S	ok	
US-20	An untrained user should be able to visualize and interpret the statistics in less than 5 minutes.	S	ok	
DE-01	The identification through biometrics should be performed correctly in more than 95% cases.	C	ok	
DE-02	The start of interaction command should be recognised properly in more than 99% of cases.	C	ok	
DE-03	The commands to execute should be recognised properly in more than 95% of cases.	C	ok	
DE-04	Record of intrusions must be available for six months after the recording.	S	ok	
DE-05	Identity of the intruders must be available for six months after the recording.	S	Refine	This requirement should specify that it does not apply in the case the intruder is not recognized, which is a possible situation.
DE-06	Core functionalities should be replicated on multiple devices to avoid single points of failure.	C	ok	
DE-07	The registration of a new device should be successful in at least 99% of the cases.	C	ok	

DE-08	The de-registration of a new device should be successful in at least 99% of the cases.	C	ok	
DE-09	The configuration changes should be propagated successfully to the devices in more than 99% of times.	C	ok	
DE-10	The SIFIS-Home system should be able to restore the previous configurations if there are error in the application of configuration changes.	S	ok	
DE-11	The installation of the selected app should be completed successfully in at least 95% of cases.	C	ok	
DE-12	The application of policies should be completed successfully in at least 99% of cases.	C	ok	
DE-13	The configuration of profiles should be completed successfully in at least 99% of cases.	C	ok	
DE-14	The change of current profile should be completed successfully in at least 99% of cases.	C	ok	
DE-15	The statistics must be shown correctly in at least 99% of cases.	C	ok	
DE-16	Remote log-in for the configurer should be successful in at least 99% cases.	C	ok	
DE-17	The SIFIS-Home system should be able to distribute the processing among multiple machines in different places if required.	C	ok	
DE-18	The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.	C	ok	
DE-19	The SIFIS-Home system is required to be scalable dynamically by adding or removing nodes according to demand.	C	ok	

3.3 *Security Requirements Analysis*

The following Table provides a list a list of feedback and request of amendments to the security requirements defined in Section 6.2 of D1.1.

ID	Req. Description	Priority	Feedback	Comments
SE-01	APIs for the communication with internal devices must be secured.	C	ok	

SE-02	APIs for the communication with external devices must be secured.	C	ok	
SE-03	Personal data stored must be encrypted.	C	ok	
SE-04	The system shall protect and avoid disclosure of sensitive information.	C	ok	
SE-05	The SIFIS-Home system shall prevent data alteration or deletion.	C	ok	
SE-06	WiFi access should be protected against known WiFi security attacks.	C	ok	
SE-07	Biometrics must be stored safely in the SIFIS-Home database.	C	ok	
SE-08	Log-in information should be stored in a protected database.	C	ok	
SE-09	The information about the registered devices, their characteristics and their configurations should be stored in a protected database.	C	ok	
SE-10	The information about policies should be stored in a protected database.	C	ok	
SE-11	The information about user profiles and configuration aspects should be stored in a protected database.	C	ok	
SE-12	Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.	C	ok	
SE-13	Data confidentiality shall be ensured all the time.	C	ok	
SE-14	The system should not be affected by MITM attacks.	C	ok	
SE-15	Software and apps shall only be installed with authorisation of the smart home administrator or resident users.	C	ok	
SE-16	Users must be able to configure and allow the usage of data by the SIFIS-Home framework and third party software.	C	Refine	This requirement should specify to which data it refers to.
SE-17	Anomalous device behaviours should be identified and signalled in less than 60 seconds.	C	Refine	This is a non-functional performance requirement. Moreover, since 60 seconds is the duration of the temporal window that is typically used as an observation period, please refine changing 60 seconds

				to 61 seconds in order to give the time (1 second) to perform the computation.
SE-18	Minimum needed privilege principle must always be enforced.	C	ok	
SE-19	Access to devices functionalities should be protected and controlled.	C	ok	
SE-20	Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.	C	ok	
SE-21	Privacy preferences shall be configurable for data, analytics and functionalities.	C	ok	
SE-22	Analytics shall be able to work with anonymized data when possible.	C	ok	
SE-23	The SIFIS-Home architecture shall be resilient to network-based attacks.	C	ok	
SE-24	The SIFIS-Home architecture shall be resilient DoS attacks.	C	ok	
SE-25	The SIFIS-Home architecture shall be resilient to sybil attacks.	C	ok	
SE-26	The SIFIS-Home architecture shall be resilient to device compromising attacks.	C	ok	
SE-27	The SIFIS-Home architecture shall be resilient to Internet connection failure.	C	ok	
SE-28	The SIFIS-Home architecture shall be resilient to physical device damage or failure.	C	ok	
SE-29	Devices must have unique identifiers.	C	ok	

4 Additional Requirements

This section defines new network & system security requirements that are requested for WP1 to be added in its next deliverable D1.2 “Final Architecture Requirements Report”.

These requirements have been formulated by taking into account the requirements originally defined in D1.1 “Initial Architecture Requirements Report”, as well as the scope, functionality and goals of the network & system security solutions to be developed in WP3.

The definition of new requirements adheres to the same taxonomy and classification of requirements introduced in Section 6 of D1.1. That is the new requirements below are separately defined for the different subset “Functional requirements”, “Non-functional requirements” and “Security requirements”. Furthermore, also consistent with D1.1:

The new functional requirements are mapped to the related use cases and non-functional requirements. The new non-functional and security requirements are mapped to the related functional requirements. The new security requirements are split into "Testable" and "Non-testable" security requirements.

Similar to the original requirements defined in D1.1, the new requirements are also grouped into three different categories associated to their priority level, namely Critical (C), Standard (S) and Optional (O).

4.1 *New Functional Requirements*

The following Table provides a list of new functional requirements to be added to the initial set defined in Section 6.1 of deliverable D1.1.

The table is composed of the following columns:

- **ID:** unique identifier assigned to the requirement.
- **Description:** description of the requirement.
- **UC:** identifier(s) of the use case(s) this requirement refers to. For a detailed description of the Use Cases, please refer to their definition in Section 5.2 of deliverable D1.1.
- **Priority:** priority of this requirement, i.e., critical, standard, or optional.
- **NFR-ID:** unique identifier of the non-functional requirement(s) this requirement refers to.
- **NFR-Type:** type(s) of the corresponding non-functional requirement(s) under "NFR-ID".

ID	Description	UC	Priority	NFR-ID	NFR-Type
WP4-F-01	The system should support multiple languages.	UC-02	S	PE-07 DE03	Performance Dependability
WP4-F-02	The SIFIS-Home system must be able to map a policy defined by the administrator into one or more device-level policies.	all	C	TE-01 AV-01 DE-20	Technical Availability Dependability
WP4-F-03	The SIFIS-Home should be able to map the device-level policies with the capabilities of the involved devices.	all	C	TE-01 AV-01 DE-20	Technical Availability Dependability
WP4-F-04	The SIFIS-Home must be able to apply the active device-level policies to the actual devices.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
WP4-F-05	The SIFIS-Home must be able to apply the active device-level policies when needed.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
WP4-F-06	The SIFIS-Home should notify when a device-level policy cannot be mapped onto any device.	all	C	TE-01 TE-02 AV-01 DE-20	Technical Availability Dependability
WP4-	The SIFIS-Home should be able to identify	all	S	TE-01	Technical

F-07	redundant or conflicting policies.			TE-02 AV-01 DE-20	Availability Dependability
WP4-F-08	The description of the policies must be available.	all	C	TE-02	Technical

4.2 *New Non-Functional Requirements*

The following Table provides a list of new non-functional requirements to be added to the initial set defined in Section 6.2 of deliverable D1.1.

The table is composed of the following columns:

- **ID:** unique identifier assigned to the requirement.
- **Description:** description of the requirement.
- **FR-ID:** unique identifier of the non-functional requirement(s) this requirement refers to.
- **Priority:** priority of this requirement, i.e. critical, standard or optional.

ID	**Description**	**FR-ID**	**Priority**
WP4-US-01	The Multi-Level Anomaly Detection system (MLADS) must monitor network traffic provided by several input sources and several locations.	F-15 F-16 F-17 F-18	C
WP4-US-02	The workload of the devices should be available to the MLADS.	F-15 F-16 F-17 F-18	C
WP4-US-03	The list of applications running on each device should be available to MLADS.	F-15 F-16 F-17 F-18	C
WP4-US-04	Raw sensor data must be available to be analysed by MLADS.	F-15 F-16 F-17 F-18	C
WP4-US-05	Features from different devices should be aggregable directly or by means of pre-processing through specific analysis tools.	F-15 F-16 F-17 F-18	C
WP4-US-06	When possible, a dataset[1] should not be present as a whole on a single device for analysis.	All	S
WP4-US-07	The presence of a GPU is needed to perform DL-based analysis.	F-15 F-16	S

[1] E.g., the set of measures collected by a sensor, the set of speeches collected by a microphone, the set of images captured by a camera, etc.

		F-17 F-18	
WP4-TE-01	The SIFIS-Home system needs Java version 8 or higher to interact with the ontology.		C
WP4-TE-02	The process for getting and inserting information into the ontology will be through APIs provided via HTTP(S).		C
WP4-TE-03	The software for handling the ontology should be hosted on a high-availability server.		C
WP4-TE-04	Internet connectivity should be present.		S

4.3 *New Security Requirements*

The following Table provides a list of new security requirements to be added to the initial set defined in Section 6.3 of deliverable D1.1.

The table is composed of the following columns:

- **ID:** unique identifier assigned to the requirement.
- **Description:** description of the requirement.
- **FR-ID:** unique identifier of the non-functional requirement(s) this requirement refers to.
- **Testable:** whether this requirement is testable (yes) or non-testable (no).
- **Priority:** priority of this requirement, i.e., critical, standard, or optional.

ID	Description	FR-ID	Testable	Priority
WP4-SE-01	Device administrable domain should be known.	all	n	S
WP4-SE-02	Definition of a template for each type of device which describes the features of the specific type of device.	all	n	S
WP4-SE-03	The identity of the speaker should not be identifiable if the analysis is outsourced to external services.	UC-02	n	S
WP4-SE-04	The background noises in the audio streams must be anonymized if the analysis is outsourced to external services.	UC-02	n	S
WP4-SE-05	Personal information recognizable from audio (e.g., name, telephone number, email address, age, physical condition) must be anonymized if the analysis is outsourced to external services.	UC-02	n	S

5 Conclusion

This document is the first deliverable from WP4 and has provided WP1 with feedback as well as requests for amendment and additions to the initial set of requirements defined in deliverable D1.1 "Initial Architecture Requirements Report".

Feedback, requests for updates, and new requirements to add have been especially brought up in the light of the planned privacy aware analytics under development in WP4. For the sake of clarity, the same taxonomy and classification of requirements introduced in deliverable D1.1 has been used in this document.

A relevant finding of this deliverable is the necessity to provide clear and unique definitions to some concepts used in the requirements, e.g., “isolation”, “policy”, “user profile”, “configuration”, in such a way that such terms can be used consistently for all the requirements.

This deliverable also identified a few overlaps between some requirements. These overlaps could be solved either by merging the overlapping requirements, or through a clearer specification of these requirements aimed at differentiating the specific scenarios where each of them is applicable.

Finally, this deliverable contributes by proposing a number of new requirements, both functional and non-functional, which are specific to the analysis defined in WP4, and that are not covered by the general requirements defined in D1.1.

Together with the analogous feedback and input from WP3 provided in the deliverable D3.1 accompanying the present document, this contribution will be considered by WP1 to produce its next deliverable D1.2 "Final Architecture Requirements Report". Following on this joint effort, the security solutions developed in WP4 will keep taking into account the guidelines from WP1, and especially the final set of requirements from its deliverable D1.2.

Glossary

Acronym	Definition
DHT	Distributed Hash Table
FR	Functional Requirements
NFR	Non-functional requirement
OS	Operative System
P2P	Peer to Peer
SIFIS-Home	Secure Interoperable Full Stack Internet of Things for Smart Home
UC	Use case
US	User story
SD	Smart Device
NSSD	Not So Smart Device