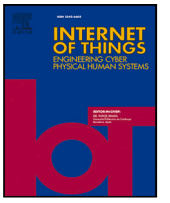
Internet of Things 31 (2025) 101585

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Research article

Proposal for a security and privacy enhancement system for private smart environments

Sonia Solera-Cotanilla [a,*,1], Manuel Álvarez-Campana [a,1], Carmen Sánchez-Zas [a,1], Mario Vega-Barbas [b,2]

[a] ETSI de Telecomunicación, Universidad Politécnica de Madrid, Av. Complutense 30, Madrid, 28040, Spain
[b] ETSI de Sistemas de Telecomunicación, Universidad Politécnica de Madrid, Nikola Tesla St., s/n, Madrid, 28031, Spain

ARTICLE INFO

Keywords:
Internet of Things
Risk
Security
Privacy
Vulnerability

ABSTRACT

Far from being considered a consolidated and regulated paradigm, the Internet of Things has multiple unaddressed challenges that open the way to unresolved security and privacy issues. The reality is that just as technology has evolved, so have attacks on devices, which are becoming increasingly sophisticated and complicated to prevent and detect. This problem is of particular concern in private environments where sensitive data are handled and which, on many occasions, require an early response to conditions of uncertainty. In this sense, this paper contributes to improving the security and privacy of connected devices in private environments. To this end, we propose a system for managing the security and privacy of connected devices that is adaptable to the environment's requirements. This system, integrated in the router, consists of a set of components that address the problem through the tasks of monitoring and data acquisition, information storage, data analysis, event processing, and data visualisation. Finally, a set of mechanisms is proposed to further automate the secure integration and continuous monitoring of devices in order to make processes more secure and efficient. Thus, these mechanisms, which can be integrated into the proposed system, provide the environment with real-time management capabilities of the devices and notification of alerts detected in the home network, with the sole purpose of keeping the environment secure against possible threats and attacks.

1. Introduction

In recent decades, the way we communicate has been modified thanks to the technological advances that have brought us into the current digital era in which we live. The economic development and technological change that we have been undergoing have made information one of the main economic resources.

Thus, the Information Society (IS) and the Information and Communication Technologies (ICT) have undergone a continuous adaptation to these new strategies of creation, acquisition, processing, and transmission of data for the benefit of society. Today, enabling technologies such as ubiquitous computing and ambient intelligence have, to a large extent, enabled the rapid technological advancement that underpins the digital age of communication.

* Correspondence to: Av. Complutense, 30, 28040, Madrid, Spain.
E-mail address: sonia.solera@upm.es (S. Solera-Cotanilla).

[1] Ph.D. in Telecommunication Engineering.

[2] Ph.D. in Systems and Service Engineering for the Information Society.

https://doi.org/10.1016/j.iot.2025.101585
Received 17 April 2024; Received in revised form 17 March 2025; Accepted 17 March 2025
Available online 24 March 2025

Both ubiquitous computing and ambient intelligence enable systems to perceive, understand and adapt to the environment [1]. In this way, devices, thanks to pervasive systems, collect and interpret data to make decisions based on the specific needs of the environment. What is more, they do so without interfering with people's routine activities and tasks. The fact that these devices and systems are omnipresent, invisible, and ubiquitous in the user's daily environment, together with the adaptive capacity that defines them, allows the services offered to the end user to be increasingly personalised and in line with their personal requirements.

This includes the Internet of Things (IoT), which is a digital ecosystem of devices and everyday objects connected to the network and capable of collecting and exchanging data with each other without the need for human intervention. Thus, ubiquitous computing, making use of the IoT infrastructure, keeps smart environments adapted to users' needs.

The rise in connected devices is due, in part, to the wide acceptance of these devices, which allowed them to be quickly integrated into the daily lives of users [2]. However, as IoT devices are deployed in an increasing number of industries, new challenges arise in relation to the security and privacy of the data they handle.

Specifically, this paper focusses on protecting private environments that traditionally did not have intelligence built into them. These are those that currently have advanced technology integrated to automate and control certain aspects of the environment. These can be lighting and temperature control, security and surveillance, entertainment, virtual assistance, and health, among others. This paper addresses this issue through a set of proposed solutions, which are presented in later sections.

2. Background

The rise of IoT devices and their adoption by users in society have allowed the penetration rate of these devices in users' lives to increase considerably over the last few decades. In fact, the usefulness of IoT devices and services depends directly on this adoption in people's daily lives. Thus, as the level of penetration has increased, there has been increased interest in the development and customisation of IoT services and applications [3].

Among others, this expansion and integration of IoT devices was such that IoT then began to be applied to a multitude of different environments, where such technology could be beneficial in performing a variety of tasks. Environments such as telemedicine and e-health services [4], industry 4.0 [5] or smart cities and homes [6,7]. It has also facilitated the creation of new market contexts such as smart toys, the automotive industry, or even healthcare.

A clear example of the usefulness of IoT was the medical environment, where it began to be used to monitor patients, both in the hospital and in the home. Other areas where the benefits of implementing IoT have quickly been discovered include agriculture, industry, and home automation, among others.

In general, an important aspect of IoT networks is their energy management. Several studies, such as [8], analyse operational expenses and battery degradation, proposing innovative strategies that produce effective energy management results and a considerable reduction in operational costs. Also focused on the search for reliable and efficient energy management systems, the authors of [9] study the optimal allocation of energy resources in microgrids with renewable energy sources using machine learning algorithms.

In any field, proper monitoring and data collection for later analysis is a key aspect to consider, always with the aim of generating accurate alerts. Specifically, study [10] proposes a supervision and control system for parameters related to power supply in private environments.

In addition, the use of IoT has improved the quality of life in environments where an early response to disasters is required under uncertain conditions. Using Smart Disaster Response Systems (SDRS), based on ICT, it is possible to improve survival rates.

Research such as [11] examines the importance of a natural disaster response system through remote monitoring, early warning, and proposed solutions to cope with such events in a reliable way. Other authors [12] analyse the challenges of implementing SDRS and how the application of IoT in this area changes people's lives.

In short, over the years it has been implemented in all everyday areas where the automation of tasks transforms processes into more effective and better results.

However, despite the clear advantages offered by the IoT paradigm, it is often plagued by security and privacy weaknesses of the underlying devices and applications. In fact, the use of these devices and the services they offer is directly related to their incidence and penetration in people's daily lives. And therefore, the sharing of sensitive user data involves critical security and privacy issues related to these devices [13].

GSMA security assessments [14] determine that the higher this penetration, the higher the profit for the manufacturers. This is because the greater the impact on users' daily lives, the more IoT devices there will be in smart environments, and therefore the higher the sales figures. Concern about the inefficient security mechanisms on which devices rely has reached such a limit that the authors have proposed a best-practice guide focused on the correct design, development, and implementation to try to improve their security.

Authors present vulnerabilities that arise, precisely because the security and privacy of users are not prioritised in the design and development processes. In many cases, this oversight is due to manufacturers focussing their design processes on more attractive and competent market prices. In some cases, these low-cost devices have long life cycles and do not have a cybersecurity ecosystem that develops patches for them, which can eventually make them vulnerable.

In addition to this fact, these devices, applications, and services are often used by people who lack training on good practices when using them and who are not cybersecurity experts. This human contribution makes them even more vulnerable, which is why studies such as [15] address this aspect to contribute to IoT security through practice guides for manufacturers, vendors and users. Some organisations have been providing recommendations on measures for years, such as INCIBE [16].

As a result, these devices have become one of the most attractive segments for cybercriminal organisations [17]. According to "Nokia Threat Intelligence Report 2020" [18], IoT devices are responsible for 32.72% of all infections observed in mobile networks in 2020. It is therefore necessary to address the weaknesses of such devices from the early stages of development, paying particular attention to the user-technology relationship. In recent years, security and data protection standards have been developed, as well as laws such as the "Internet of Things Cybersecurity Improvement Act of 2020", with the sole objective of improving the security and privacy of connected devices.

One of the main reasons why this issue is of so much interest is that attacks through connected devices have serious implications in the real life of users. For example, an attack on video surveillance systems can have criminal implications or simply the more direct implication of a breach of privacy. Other examples related to impersonation involve, for example, banking institutions and money theft.

However, attackers sometimes focus their efforts on other ways of accessing the network itself. In particular, attacks are common on the Routing Protocol for Low Power and Lossy Networks (RPL) that, although it has some protection measures (e.g. encryption for control messages), are inefficient [19].

In short, although IoT appeared as a technology that, in the eyes of the end user, would give some intelligence to frequently used devices, promising to facilitate multiple daily tasks, the reality is more complex. The uncontrolled growth and adaptation of devices in certain environments with sensitive services leave the user's sensitive data vulnerable. A sensitive service is one that handles the user's private data.

Today, it is clear that the Global Trends 2025 report, published in 2008, was not so far from reality. The report speaks of the global transformation at the technological level that has indeed come along with a multitude of emerging technologies. Historical patterns of development have been left behind and the next generations of the Internet and new ubiquitous information technologies and the IoT have been embraced. In fact, even greater improvements in the economy are expected to develop in the coming years based on the aforementioned rapid adoption of these technologies.

With respect to the future of IoT, the Global Trends 2040 report [20] indicates a major technological breakthrough in terms of human experience. And, as the trend of recent years indicates, technologies and applications derived from IoT will increasingly be in people's daily lives with unquestionable adoption.

Despite the evolution of the IoT over the years, the security and privacy of connected devices continue to be an area of study. The reality is that just as IoT has evolved and technology development has made it more robust, so have cyber attackers evolved in developing strategies to breach the security of devices. An uncontrolled inclusion of questionably secure IoT devices can transform a smart environment into a prime target for cyber-attackers.

3. Proposed security and privacy management system

Unlike previous sections that have focused on exposing existing vulnerabilities and contextualising the problem, this section addresses the issue from the early stages by designing a system to enhance the security and privacy of connected devices. This is a Secure IoT Devices Integration and Management System (SIDIMS).

In Section 3.1, the requirements that the proposed system must meet, and in general, any private environment should meet to address current security gaps, are analysed. Section 3.2 presents possible integration options for this system into the private environment.

3.1. Requirements analysis

A system is proposed to ensure compliance with a set of requirements and to address the security and privacy vulnerabilities that affect the environment. Some examples of requirements that must be met in certain private environments for them to be considered secure are, for example, the challenges of the smart home system [21]. Identifying the requirements in any kind of current private environment (not only digital homes), the proposed system, hereafter referred to as SIDIMS, is based on an architecture that encompasses:

1. Control in the IoT devices integration phase
   The aim is to prevent "accidents" and facilitate understanding and limits of the system. By accidents, we mean situations that lead to undesirable user experiences and arise due to a lack of knowledge about the new technologies.
   This issue is addressed in the phase of integrating devices into the environment, that is, when adding a new device to the private network. It is beneficial to maintain control over this phase to facilitate understanding the limits of the environment concerning devices. This way, both the system and the user will be aware at all times of which devices are part of the private place and under what characteristics and current state they are.
2. Continuous monitoring of device behaviour on the network
   Another key task to address is monitoring the behaviour of devices for potential security and privacy vulnerabilities (known or unknown). To achieve this, the system requires components responsible for analysing network traffic to provide information about what is happening at any given moment in the private network.
   This issue arises under the pretext that implementing new technologies and functionalities in an environment not originally designed for them can alter the user's routines. Therefore, monitoring the evolution and behaviour of these technologies provides the desired control.

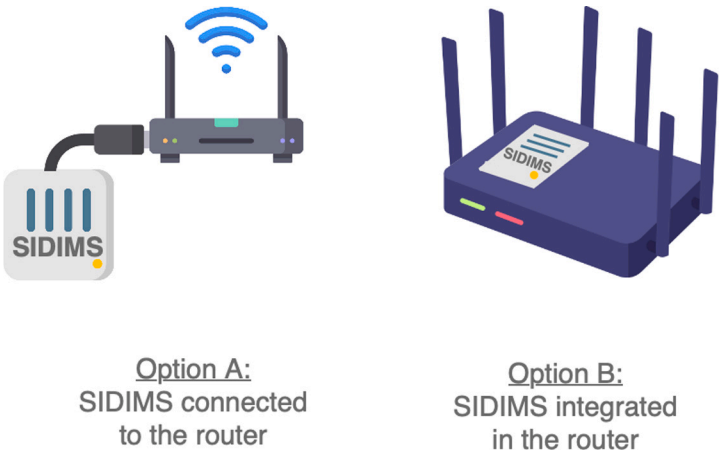


Fig. 1. System integration options in the private environment.

3. Action on devices to solve problems
   The system must be able to infer the complexity of the task at hand. At times, the system will face automated tasks for which, due to their lack of complexity, human intervention in decision-making and action is not required. This configuration should be modifiable by the user to avoid the system's default action and force the consultation of decision-making.
4. Standardised and unified data structure in the system
   Currently, IoT architectures lack a standard to be followed by all of them. This leads to each device operating differently and generally only understanding direct communication with devices of the same family or manufacturer. For this reason, the system must facilitate interoperability between connected devices with disparate designs.
5. Real-time notification using human language
   Existing solutions for the security and privacy often suffer from comprehension issues for users. Therefore, the system must be intelligible to household members without the need for technical knowledge in the field.
   The system should communicate with the user through human language and translate existing problems to be understood by household members. This communication should happen anytime, anywhere, and notify about any object. This way, the user identifies SIDIMS as a reliable system.
6. Security based on zero trust of system components
   It is a crucial requirement to keep access to sensitive resources. The network remains secure at all times through context-based access control. This means that depending on the context, the system must detect if it is a possible intrusion that jeopardises the confidentiality, integrity, and availability of the user's personal data. This also prevents complete system failures that would leave household members without service.
7. "Digital" administrator that learns autonomously
   The system must have the ability to operate without a physical and human administrator managing it. It should be able to make autonomous decisions based on detected behaviour. For this, a prior risk analysis is essential, evaluating critical events by probability and impact. Critical events are the only ones that, by their nature, require human intervention.

To avoid issues associated with the invasion of technology into users' daily routines, the system architecture is designed with a focus on user interaction with the smart environment. Thus, the architecture encompasses the mentioned requirements and reflects the system's behaviour to meet the user's needs.

3.2. Integration of the system into the environment

Ideally, traditional routers should have the capability to protect network security and privacy by protecting against attacks and vulnerabilities. However, the reality is that these routers do not provide the necessary protection mechanisms. In this regard, smart routers do offer certain additional protection mechanisms, but they are not always effective or do not adapt well to all kinds of environment as expected. Additionally, they often come with a high cost, which may not be affordable in non-industrial environments.

The proposed system discussed in this section is designed to work complementarily to the functionalities offered by a router. Therefore, there is the possibility that SIDIMS is integrated into the router or into other hardware and operates in parallel connected to the router. Fig. 1 shows the two exposed options.

Whether SIDIMS is integrated into the router or is connected to it, the system acts as an intermediary between devices and the network. Depending on the requirements to be met, one option may be more suitable than the other.

Option A, with SIDIMS connected to the router, involves having an additional device connected by cable to the router (or through a wireless protocol, typically WiFi). In addition to the physical connection, a simple pre-configuration of system parameters is required for SIDIMS to identify the network to monitor. This involves specifying the range of addresses to analyse. This alternative offers capabilities for threat prevention, detection, and real-time alerts.

Option B, with SIDIMS integrated into the router, does not require two devices in the private environment. Instead, all the "intelligence" of SIDIMS is concentrated in a single device with traditional router capabilities and additional ones provided by SIDIMS. These capabilities include those of option A, as well as action capabilities. In other words, this alternative allows for the prevention or mitigation of detected threats.

A third existing alternative is to have these capabilities at the operator's central hub. The main problem with this option is that the operator would not be able to monitor internal traffic in some private environments as the smart home, and legal issues may arise. Thus, the capabilities that prioritise network security and privacy would not be as effective.

While some operators consider providing additional security mechanisms implemented in their routers, these are often limited to restricting certain actions on the router that could compromise data security. For example, keep ports closed by default and require advanced configuration access to open them. This paper does not focus on the communication segment from the router to the server, so this alternative was discarded directly.

In conclusion, ruling out this third option due to impracticality, the main difference between the two options is that, in the case of the system integrated as a router module (option B), SIDIMS would have monitoring and action capabilities. That is, it would have the ability to prevent and mitigate existing threats, not just alert about monitoring.

In this sense, it is important to weigh the advantages and disadvantages of each proposed option and to consider which one best fits the environment's requirements. In this case, the requirements require the system to take action, either autonomously or through user consultation. Therefore, the selected alternative is option B, SIDIMS as part of the router, to provide action and counteract attacks. Thus, the SIDIMS module will have control over incoming and outgoing traffic from the home and will have capabilities to manage its security and privacy.

4. General architecture of the proposed system

The main goal of SIDIMS is to provide with network management mechanisms that preserve the security and privacy of the private environment. This aims to enable the environment to function as a means to carry out everyday activities using new technologies, ensuring security and privacy guarantees. To this end, the requirements set out in Section 3.1 are addressed to meet the security and privacy challenges that concern it. In this regard, the proposed system integrates into the router, as indicated in Section 3.2, acting as a protective barrier against potential attacks that may compromise the security and privacy of the environment.

Fig. 2 illustrates the typical, but not exclusive, data flow in a private environment, with SIDIMS acting as an intermediary between devices and the network. It includes the user, connected devices, SIDIMS for security and privacy control (integrated into the router), and external servers hosted on the Internet.

Considering that the user provides their digital identity for these devices to act on their behalf, the term "user" will hereafter be used to refer to the digital identity that represents them within the smart home. Furthermore, not only users have a digital identity, but devices as well, as explained in Section 2.

The architecture of SIDIMS addresses the requirements outlined in Section 3.1 in relation to two concepts: UXD [22] and EDA [23]. Designing the architecture with a focus on user experience means concentrating on meeting user needs and the usability of the services. However, the logic of event-driven architectures has been adapted to the design of this specific architecture.

These two concepts together allow for the design of an architecture that caters to the user's needs and maintains the personalised service provided at all times. Moreover, it is done in a simple and reliable manner, through a system of alerts understandable to the user, responding promptly to the needs to be addressed.

The components that make up the proposed architecture are detailed below and are represented in the green box in Fig. 2. According to [24], there are five phases of data that can be observed in the architecture:

- Data Ingestion Phase: This phase is addressed in the component "Monitoring and Data Acquisition", detailed in Section 4.1, and involves three data sources:
  - "User". Since the design is user-centred, all the information coming from the user is of crucial importance. Being an integrated system in a private environment such as the digital home, the user cannot be deprived of the services provided. So, the availability of access to services must be prioritised. The information is obtained through feedback and actions served from the user interface control of the digital home. This component, "E-User interface", is detailed in the subsection "components-interface".
  - "Connected Devices": They generate information both through user usage and internal device actions, such as firmware updates (not required by the user but performed anyway).
  - "External Servers": Specifically, third-party databases hosted on external servers. They provide specific information about IoT devices, such as commercial information and known vulnerabilities associated with them.
- Data Storage Phase: To carry out this phase, a dedicated component is required. Specifically, "Data Storage" is responsible for managing and maintaining databases and logs, detailed in Section 4.2.

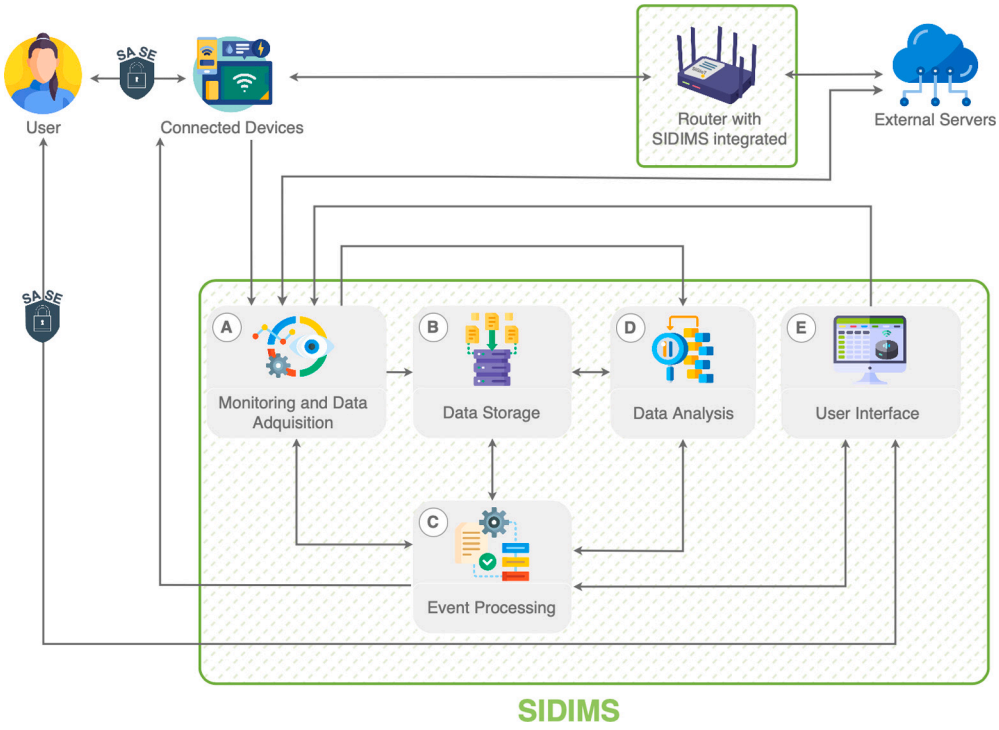


Fig. 2. General architecture of the proposed system.

- Information Processing Phase: This phase is handled by "Event Processing", detailed in Section 4.3, which manages requests from other components and generates events based on them. Events represent alerts that must be addressed by the system and, if required, by the user.
- Stored Information Analysis Phase: This phase is managed by "Data Analysis", detailed in Section 4.4. To perform analytics on monitored data, the component uses other mechanisms to detect irregular behaviours. It also compares behaviours with those stored in a historical record in the system and with behaviours previously characterised as threatening.
- Exploitation or Visualisation Phase: This task is performed through a user interface or dashboard, and the component responsible for it is "User Interface", detailed in Section 4.5.

After presenting the general architecture of the system, each of the five components, their relationships, and the incoming and outgoing data flow of each component is detailed below. It is important to note that all components comprising SIDIMS are assumed to be integrated into a router module.

4.1. Monitoring and data acquisition

This component is responsible for monitoring the incoming and outgoing traffic of the router. Information acquisition is done non-invasive for the user, with the sole purpose of capturing and providing the data flow to other components for monitoring, interpretation, and, if necessary, storage of the information flowing through the network. This component is fed information from different sources, both internal and external to the environment.

Regarding information provided internally to the environment, the component monitors the network in real-time to detect new devices unknown to the system. The captured traffic can represent the typical behaviour of a device due to user-initiated actions (such as turning on a light bulb) or other types of traffic that the device generates independently (such as firmware updates).

This traffic is not captured indiscriminately; instead, it is sampled to monitor in real-time and store only the relevant data. Immediately upon the appearance of a new device in the network, the component provides the new information to "Data Storage" to store its IP address, MAC address and the device's manufacturer. This information, together, uniquely identifies the device within the network. To obtain the MAC address and the device's manufacturer, the system must access databases hosted on external servers. This process is detailed in the next section, Section 3.2.

With respect to information provided externally, the system is fed information stored in external databases. This information is not continuously obtained as real-time monitoring of the network, but involves occasional queries to these databases. These queries may be due to the detection of a new device for which more information is desired or an interest in knowing new vulnerabilities that may exist in devices within the environment.

For the latter case, queries are made periodically to the databases. The system finds information registered by other users about that type of device. The fact that a user has registered an existing vulnerability in a device with similar characteristics does not imply that the device on the network is also infected. It only indicates that, due to the characteristics of the device, it is more susceptible than others to this specific vulnerability.

The interactions of this component with other entities in the environment and the rest of the SIDIMS components are as follows:

A. Monitoring and Data Acquisition ⟵ Connected Devices

This data flow refers to the situation, already mentioned, of the device's behaviour generating traffic on the network. It is useful information for the system and is acquired internally within the environment. This component is not responsible for interpreting the data, only capturing the indicated traffic.

A. Monitoring and Data Acquisition ⟵ E. User Interface

This is the other data flow that involves obtaining information internally within the environment. This data ingestion translates user-initiated actions and feedback provided in SIDIMS notifications from the user interface.

A. Monitoring and Data Acquisition ⟵ External Servers

This data exchange flow refers to information obtained from external data sources, which has also been introduced. An example of a data flow could be the need for a device to access a proprietary database hosted on external servers to fulfil a user request (such as access to third-party skills for new device functionalities).

In addition to queries made by devices to external servers, SIDIMS will periodically query external databases hosted on Internet servers to obtain information about known vulnerabilities. This periodic query will also be performed each time a device appears for the first time on the network.

In this way, the system provides updated information on known external vulnerabilities in the device's behaviour on the network. Some examples include security vulnerabilities associated with open ports with no services listening, outdated firmware requiring security patches to prevent information leaks, or even known attacks on specific devices.

A. Monitoring and Data Acquisition ⟶ D. Data Analysis

Not all captured information is stored; some of it is first analysed in real time, and if anomalous behaviours are detected, an event is generated that, once resolved, may involve the processing and storage of information or even intervention if necessary.

A. Monitoring and Data Acquisition ⟶ B. Data Storage

This data flow corresponds to the storage of data related to detected devices. It is stored in databases and logs that can be queried later if necessary. The initially stored information includes the IP address, the MAC address, the device manufacturer and, if applicable, known vulnerabilities. Each entry in the database will have information that is updated and completed over time, for example, with the detection of new vulnerabilities or irregular behaviours.

A. Monitoring and Data Acquisition ⟷ C. Event Processing

The storage manager and the Event Processing communicate to manage system events. This can occur because the storage manager notifies the existence of a new device in the environment or because the Event Manager.

4.2. Data storage

This component is responsible for the storage resources of SIDIMS. The stored data are organised and interrelated, as shown in the entity-relationship diagram in Fig. 3. This type of diagram allows to represent how information is stored in the system.

The identified entities are User, Role, Device, Device Group, and Vulnerability. In this sense, User and Device could be identified as the main entities generating information for the system. The entities related to these and the attributes they have allow to complete the technical profiles associated with users and devices.

Each entity has a randomly generated identifier. In the case of the Role entity, there are only four possible identifiers associated with the four types of role, so in this case, it is not randomly generated. In other cases, for example, for users and devices, there will be as many randomly generated identifiers as existing digital identities.

As shown in the diagram, a user can have only one associated role, but each existing role can be associated with none or multiple users in the database. The roles considered are as follows:

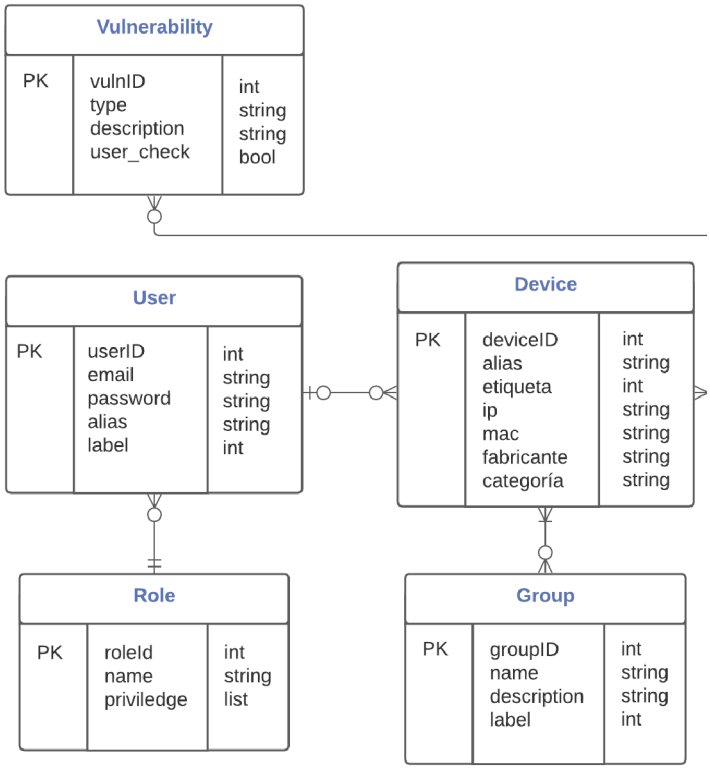


Fig. 3. Entity relationship diagram of the proposed system.

- Guest User Role.
  These are users who make a long stay in the place, so it is desired that they are registered on the control platform. The actions and routines of the guest will not be part of the system's history, but the user will have reduced privileges that allow managing non-critical components to some extent. The privileges are for viewing and editing non-critical components (in Section 5, the distinction between critical and non-critical components will be made). It has no privileges over users, either in viewing or editing.
- Minor User Role.
  Again, this role will not be necessary, in most cases, since minors will use the devices indiscriminately and without prior registration. However, if it is desired to control the access to resources by this user, the role of the "Minor User" has the same limited privileges as the "Guest User" role but also with parental control. Apparently, both are at the same level of privileges, but the history of this role is stored and also analysed based on access to resources and actions that the minor should not perform.
- Adult User Role.
  It has viewing and editing privileges on all devices, including critical ones. This user can act on devices and make decisions to solve problems detected in the network. However, it has limited control over users, only has privileges to create or edit other users, and it cannot delete users from the system.
- Administrator Role.
  It has full privileges over both devices and users. It also has access to histories and platform management. There must be at least one administrator user in charge of managing the other users and with complete control over SIDIMS.

The first three roles represent users integrated into the system, so a complete record of them is required, and they are granted user access credentials. Unlike them, the "Guest User" does not have credentials, only their email is required in the registration to confirm access. Another difference between them is that the system members have an alias that can be used if desired.

In addition, all user types, except the administrator, have a reliability label that is updated based on how secure and reliable they are. It is a score from zero to ten that is updated with each vulnerability in which the user is involved. The user itself will not be related to security issues; its associated devices will be if it has any.

On the other hand, the entity "User" is completely managed from the control interface. This means that by default, there is only one system administrator, but no users associated with the private environment. This is not a mandatory action; if it is desired for users to continue manipulating devices without the need to exist in the system's database, SIDIMS will work the same way in terms of security and privacy improvement.

Regarding the "Device" entity, it has a set of attributes that are self-filled in the database immediately when this device is detected on the network. These attributes are the IP address, the associated MAC address, and the manufacturer. At this moment, it is randomly assigned an identifier and a reliability label that, like in the case of users, will be updated.

The "alias" and "category" attributes can be completed from the user interface. There is the option to enter the device's "category" based on the behaviour analysed in the network. In fact, research such as [25] demonstrates the possibility of classifying devices based on their behaviour independently of their functionality or purpose.

Each device can have none or multiple vulnerabilities associated with it, and a vulnerability must have been detected in at least one device (otherwise, the vulnerability would not exist or would not have been discovered yet). Therefore, vulnerabilities may be due to open ports on devices or more complex vulnerabilities, whether known (with characterised behaviour registered in external databases) or unknown (but detected by "Data Analysis" based on irregular behaviours).

Each time a new vulnerability is detected on one of the devices, the user will receive a notification through the interface that must be addressed to confirm the vulnerability correctly (this is through the "user_check" attribute). This information allows the reliability labels of the devices up-to-date.

In addition, each device can belong to created device groups. A group can be formed by one or multiple devices. Some examples of groups can be associated with some places, such as specific rooms.

The relationship between "User" and "Device" exists because a user can have several associated devices because they are single-use devices for him, such as his personal smartphone. However, a device can have at most one preferred user associated. This relationship must be explicitly indicated through the user interface.

In addition, certain actions taken on devices without a preferred user may indicate that the user who performs them is able to access it from the user interface and access it with his credentials. An example of this is to turn on the lights via the user interface. Thus, in the history, not only the lights' action of turning on would be registered but also which user is manipulating them. Some alternatives with similar reliability include those that include some type of user recognition, such as biometric recognition or voice recognition if the action is performed through a command to a smart virtual assistant.

Regarding the mentioned histories, this store information related to connections, actions taken by digital identities (user and/or device), actions taken by users in response to SIDIMS notifications (for example, to block access to a suspicious device), and other actions related to users and devices such as editing privileges, aliases, etc.

The interactions of this component with the rest, excluding those already explained, are as follows:

Data Storage ⟷ C. Event Processing

The storage manager notifies a new event to "Event Processing" each time a record is included, modified, or deleted from the databases. In turn, "Event Processing" accesses the database resources when it requires information to complete the events generated in the system (for example, an event to view the history of a device).

Data Storage ⟷ D. Data Analysis

If "Data Analysis" detects any anomaly, it is stored in the database, in the information of vulnerabilities associated with a specific device.

4.3. Event processing

There are various types of events that the "Event Processing" will trigger and should be addressed by the corresponding component. The Event Processing is responsible for managing requests from other components and generating events based on them, but it can also create its own events if required. There are two types of events:

- Simple Events (SE): if it only involves the "Event Processing" and, at most, one more component that notifies the need for a new event to address some tasks.
- Complex Events (CE): if it involves "Event Processing" and more than one component of the system. These events require the completion of tasks by more than one component. With the information obtained from the different components involved, "Event Processing" can complete the EC and proceed to broadcast it where appropriate.

The decision of whether it is an SE or CE is made by the "Event Processing" based on the information it requires from other components. Thus, a CE is generated and divided into as many parts as there are involved components. To complete the event and be able to broadcast it, it is necessary to respond to all components that are part of the process (components i and j of Fig. 4). Once completed, the event is passed to the component that should address it, and when it offers a response, the event can be closed by "Event Processing".

The interactions of the "Event Processing" with the rest of the components, excluding those already explained in other components, are specified below through a set of flowcharts that expose the course of an event from its creation until the task is satisfied and the event is closed. The events presented below are organised based on whether they are related to a device, a system user, or a vulnerability, either known by external databases or detected by SIDIMS.

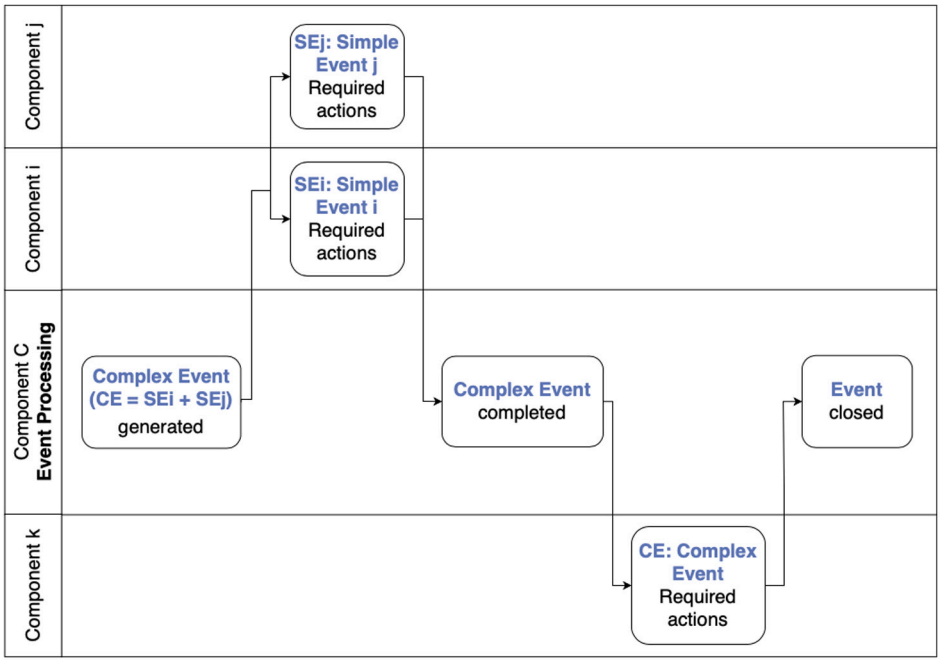


Fig. 4. Logic for creating complex events based on simple events.

Table 1
New device detection event.

New device detection event	
Event generated by:	"B-Data Storage"
Type of event:	Complex Event
Component(s) involved:	"A-Monitoring and Data acquisition" and "B-Data Storage"
Recipient of the event:	"E-User Interface"

4.3.1. Device detection events

This event, with characteristics described in Table 1 and detailed in the flow chart in Fig. 5, is generated after the detection of a new device by "Monitoring and Data Acquisition". In reality, this component lacks the necessary knowledge to identify a device as unknown or new, so it is responsible for providing this information to "Data Storage" to manage it. "Data Storage" makes the decision on whether it is known based on whether it has an entry in the database that needs updating.

In that case, "Data Storage" notifies the information detected to "Event Processing", which is responsible for generating a new event. To do this, "Event Processing" evaluates whether it is an SE or CE. In this case, it is of the latter type, as it requires information from "Monitoring and Data Acquisition" and "Data Storage".

"Data Storage" provides the IP address as soon as it verifies that it is not in the database. "Monitoring and Data Acquisition" queries external servers to determine the device's manufacturer based on its MAC address.

Once the information is gathered to complete the CE, it is sent to "User Interface", which will be responsible for notifying through the user interface the detection of a new device on the network. The event cannot be closed until the user attends to the notification. If the device is trusted and the system does not require any action, the event is closed. In the opposite case, the user does not identify the detected device, action is taken on that device by blocking its access to the network. Finally, the event is closed.

4.3.2. User-requested events

This type of event, with the characteristics outlined in Table 2, is generated when the database is queried and/or modified. The user is responsible for generating a need to be met, which is notified from the user interface. In general, any action that the user takes from the interface will result in the creation of an event that queries and/or modifies the database.

Actions that can be taken on the user database include creating a new user with access to home resources and the user interface, modifying an existing one (such as associated email, password, alias, or privileges), deleting a user, and requesting the activity history of a user. Other actions that involve accessing device database resources include, for example, viewing the activity history of devices, assigning a device to an existing user, modifying, or deleting devices, etc.

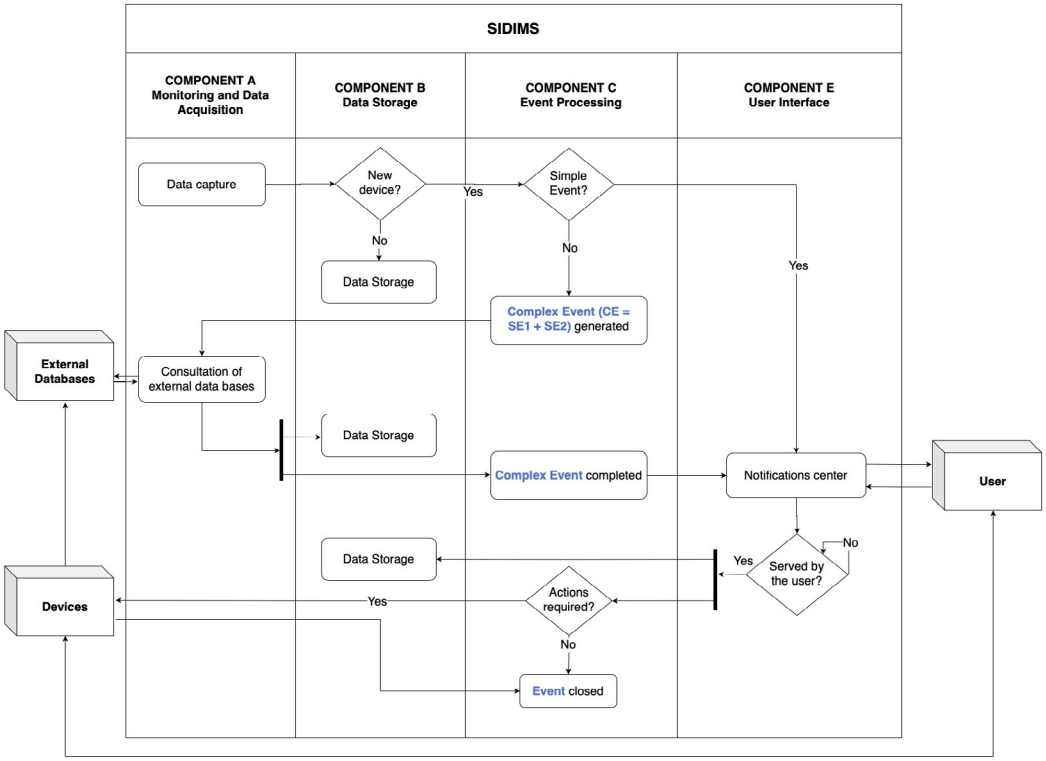


Fig. 5. New device detection flowchart.

Table 2
Event generated by user request.

Event generated by user request	
Event generated by:	"E-User Interface"
Type of event:	Simple Event
Component(s) involved:	"B-Data Storage"
Recipient of the event:	"E-User Interface"

Therefore, from the user interface, the need to address a user's need and, therefore, to attend to a task, is notified to "Event Processing". "Event Processing" generates an event, in this case, it is a simple type because the only involved component is the storage manager.

Depending on whether it is an insertion, modification, deletion, or query to the database, the event will return different information. However, in all cases, the response is displayed in the user interface to notify the user that the task has been completed. The flow chart is shown in Fig. 6.

In this case, the user cannot voluntarily include devices from the user interface, but a notification of device detection by SIDIMS must appear. This type of event would be generated by "Data Storage" once a new entry is identified in the database; it cannot be a process initiated by the user.

4.3.3. Vulnerability-related events

These events, with characteristics described in Table 3, are due to the detection of vulnerabilities, known to the scientific community and reported by external databases or vulnerabilities recently discovered by SIDIMS. In the case of the former, these are associated with reports in external databases made by other users on a specific brand, model, and firmware of a device. In the case of detections of anomalies or attacks by SIDIMS, these are problems detected by analysing home traffic in real-time.

In the first case, databases of known vulnerabilities are periodically consulted, as well as at the time of detecting a new device on the network. This is done by the Monitoring and Data Acquisition component.

However, in the case of vulnerabilities detected by SIDIMS, the detection is carried out by the Data Analysis component. All network traffic is analysed in real-time to find anomalous behaviour.

After this initial phase, where the flow chart differs slightly, the next phase is to store the newly found vulnerability. Both the storage manager and the component that detected the vulnerability notify "Event Processing", and together they generate a complex event.

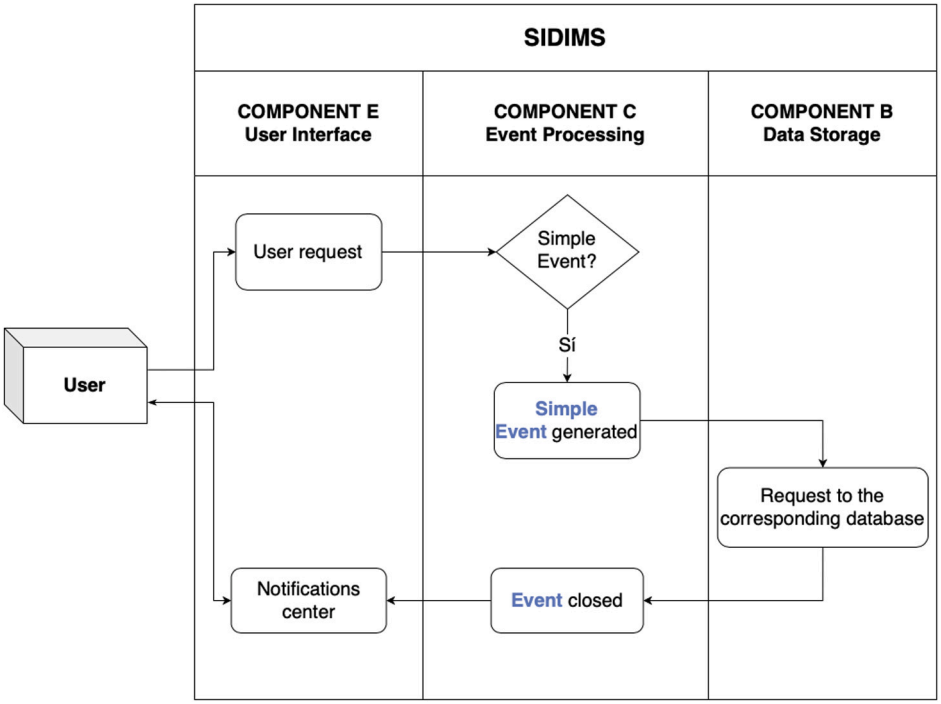


Fig. 6. User-generated event flowchart.

Table 3
Event related to vulnerabilities.

Vulnerability-related event	
Event generated by:	"A-Monitoring and Data Acquisition" and "D-Data Analysis"
Type of event:	Complex Event
Component(s) involved:	"A/D" and "B-Data Storage"
Recipient of the event:	"E-User Interface"

The collected information is notified through the user interface and requires attention from a member of the household with decision-making privileges. If action is required on the device generating the vulnerability, the action is taken; in the opposite case, the event is closed. The flow of the event is shown in Fig. 7.

In some way or another, the fact that a vulnerability has been detected implies that the risk that the home faces has been modified. Regardless of the user's response, the reliability labels of the device related to the vulnerability and, if applicable, also the user (for example, if it is a device with a single associated user managing the device) are updated.

4.4. Data analysis

This component performs retrospective and real-time data analysis. In both cases, the data analytics component is responsible for searching for anomalous network behaviour patterns using two differentiated techniques:

- Detect a previously known and identified traffic pattern as a malicious event. If it finds this match among the real-time monitored traffic, an alarm signal is generated. In this case, one or several specific anomalies are sought, so systems and mechanisms that offer this type of solution tend to have fewer false positives.
- Search for unknown anomalies. This technique looks for unknown attacks or at least attacks whose behaviour has not been characterised, and the devices affected are not registered on external servers either. Since it involves new behaviour, systems or mechanisms offering these solutions have more false positives.

In addition, the system performs personalised learning for each home through user feedback provided through the user interface. Each of the alarms found is notified to the user and the user responds by indicating whether it is suspicious behaviour.

All real-time monitored traffic is not stored; only information indicating an anomalous event is saved. Thus, in the user and device database, information related to known vulnerabilities is also stored.

The logic and operation of this component are defined in the next section, Section 5.3, where this phase is detailed.

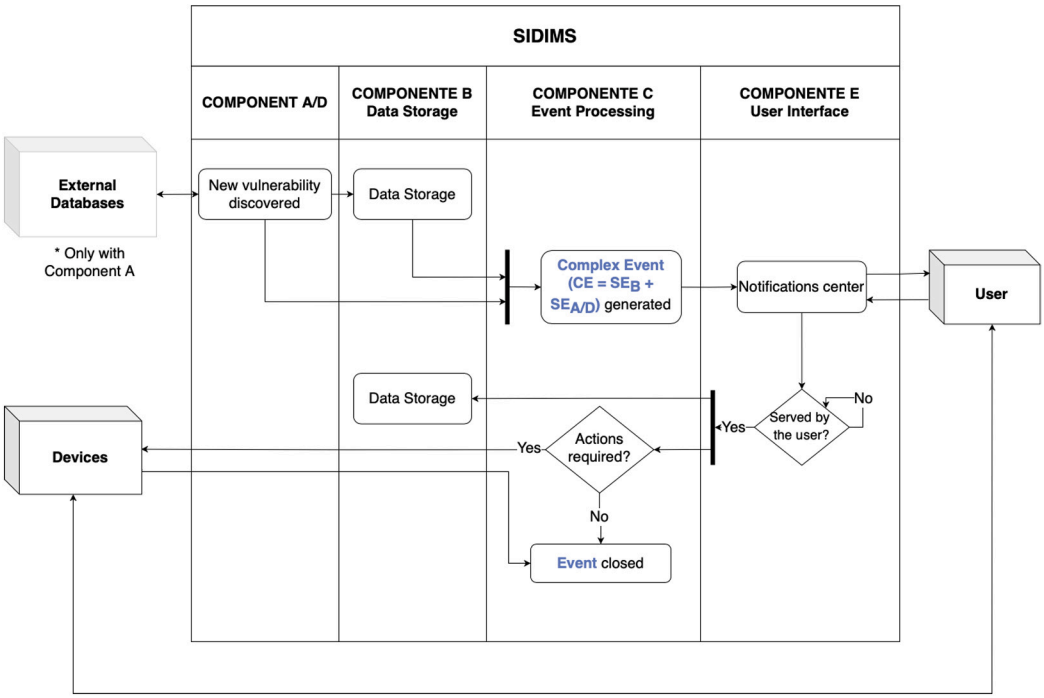


Fig. 7. Vulnerability management flowchart.

4.5. User interface

The user interface provides unified access and complete control of the environment. In this regard, the actions a user can perform through the interface differ depending on the user's role. However, in no case does it require technical knowledge of network or device security and privacy; instead, it involves user control and comprehensive system information. Alerts related to detected vulnerabilities are notified to the user and offer a solution in an understandable and straightforward manner, without the need to address technical details.

In addition to the defined roles, the system distinguishes between identified or known users and unidentified or unknown users. This occurs, for example, with household members who use connected devices without registering on the platform, such as minors using devices through voice commands or proprietary applications.

A user is considered identified or known if a prior registration has been completed, providing the required information in a registration form. This form must be validated by the administrator to grant the necessary privileges and allow access to the user interface. The possible actions to be performed are:

- Irregular Behaviour Management
  Irregular behaviours can result from attacks the network is undergoing, either a known and previously identified attack or anomalous behaviour from an unknown attack. It does not necessarily imply a system security problem, but it needs to be addressed by the user. In the most restrictive case, the user will be warned of the danger and offered a solution, typically blocking access to that device. Another alternative is for the user to consider the alert as non-suspicious, and the system learns from it as a new behaviour that does not compromise security. In both cases, the home risk level and the user and/or device reliability label will be updated.
- Device Management (event notification)
  The logic of this component allows for the management of home devices. The user will have an "image" of the home with identification of each device and technical details associated with each of them. The technical details provide not only information about the device itself (update status, technical model information, etc.), but also a history of the frequency of anomalies related to it and those that are yet to be addressed. This will allow for the assign of a reliability label to each of the devices based on anomalies that have compromised the security of the system.
- User Management
  Similar to devices, this module provides an overview of users, roles, and privileges. In the technical profile of each user, in addition to user-specific information such as private data and verifications on different devices, the actions for which the user is authenticated should appear. This authentication is performed during user registration, where privileges within the system

are granted. They will also have a label with a reliability value based on the number of anomalies in which they have been involved.

User management generally allows the inclusion, modification, and deletion of users, roles, and privileges. To access this information in administrator mode, additional credential verification will be required. From user management, anomalies associated with each user and with which specific device can be viewed.

- Visualisation (user interface)

  A user interface or dashboard will be provided for complete control of the environment. The information to be displayed will include statistics, an overall view of devices, their status, etc. For this, no alert is generated, but the user interface requests information by generating an event according to what is required.

In this sense, any of the aforementioned actions involves a flow of data access to system resources that is checked at all times. This control is carried out through strict security models that verify access to resources, which is very common in industrial environments.

Traditionally, this data flow occurred within the network, so perimeter security was more than sufficient. However, currently users require remote access and control outside the home. In this regard, the Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) security frameworks are in good agreement.

Considering that ZTNA, as introduced earlier, is based on validation at each access point and the principle of least privilege, its integration into SIDIMS would ensure reliable interactions. However, SASE, based on ZTNA, uses the user and device digital identity in conjunction with the context of access to the resource in question. That is, both offer a compromise between usability and security based on context to avoid having to verify the user at all times. However, only SASE modifies access authorisation policies associated with devices based on their actions.

This security framework appears in the outgoing user data flow, that is, when the user requires access to another resource. Additionally, SASE works with groups of known digital identities grouped by privilege type and from which verification and validation are required. This aligns with what was introduced regarding user roles and privileges. Furthermore, it also has risk profiles associated with users and risk scores associated with devices, equivalent to the reliability labels mentioned above.

Thus, in each resource request from the user, SASE verifies and validates access. The context analysis is performed by comparing it with what was previously known, determined by SASE as typical. Therefore, if a user tries to remotely access a sensitive resource or at unusual hours, the system may request additional verification to ensure their authenticity. In case of incorrect verification, ZTNA dynamically manipulates access authorisation policies.

Another scenario in which SASE would come into play is accessing the user interface with registered user credentials but from a recently detected device on the network and not a habitual device for any user. Generally, this may be due to a member of the home accessing a new device with verified access to the system. However, faced with the possibility that it is an intruder who has obtained a member's access credentials, SIDIMS generates an alert due to suspicious resource access by the user.

In summary, one of the main aspects to consider in the user interface is access to resources and the identities that require it. All of this is supported by the logic of events generated by "Data Analysis" as already explained.

5. Enhancing security and privacy mechanisms in private networks

After the proposal of SIDIMS as a key element in preserving the security and privacy of the network, this section focusses on two identified critical tasks: controlled integration of devices into the network and monitoring them for irregular behaviours. Addressing these two main tasks involves delving into certain components that have already been introduced in the system architecture outlined in Section 3.

Currently, private environments lack conducive control when including a device connected to the network. In fact, this integration phase practically involves configuring the new device from the manufacturer's proprietary application. The fact that no analysis is performed on the possible vulnerabilities associated with the device results in allowing the inclusion of any type of device without distinguishing between those that are safe and unsafe for the place and its occupants.

However, once a network is formed by a set of previously included devices, private environments also lack proper management of the security and privacy of the environment. In this way, devices vulnerabilities and potential attacks that they may suffer as a result of exploiting these vulnerabilities are difficult to detect and prevent.

This section proposes a set of mechanisms responsible for the secure integration and management of devices based on a private environment risk analysis. This procedure, detailed in Section 5.1, serves to identify critical risks that the system must prioritise at all times. In this sense, SIDIMS aims for the system to be as autonomous as possible, requiring human intervention for decision making only in cases where it is strictly necessary.

Once risks are identified, the integration and management mechanisms, susceptible to being included in the proposed system to protect the private environment, are outlined in Sections 5.2 and 5.3.

For the proposed mechanisms of secure integration and management of devices in the private environment, a prototype has been developed that addresses the issues of this contribution. The prototype is designed on a Raspberry Pi 4 Model B, which acts as a replacement access point for the router. This simulates the behaviour that SIDIMS would have as a module integrated into the router. The system will have capabilities for traffic monitoring, information processing, event management, alert notification, and action on devices.

In this case, it has been decided to carry out a pilot test on a particularly vulnerable private environment, such as the digital home. This is because the data exchanged are sensitive and private.

5.1. Risk analysis

A common practice in companies to address the cybersecurity of their assets, which is one of the main security strategies, is to perform a risk analysis of the environment. First, it is essential to define and prioritise aspects to cover in the security of the company. However, it is also important to apply a practical and applied approach, not trying to cover all possible threats, which would be entirely unattainable.

In this sense, it is crucial to differentiate between concepts that are often related but slightly differ from each other [26]:

- Threat: Unfavourable situation that generates negative consequences for assets and occurs due to security breaches or vulnerabilities.
- Vulnerability: The weakness of the system that may appear in assets and makes them susceptible to attacks.
- Attack: Action triggered as a result of a security breach that can have implications on the integrity, confidentiality, and availability of data and services.
- Impact: The consequence of the realisation of a threat on an asset by exploiting a vulnerability.
- Probability: The likelihood of the occurrence of an event.
- Risk: Quantitatively measured as the product of impact and probability, but also allows for a qualitative estimation that is more subjective.

The relationship between these concepts implies that a threat exploits an existing vulnerability, and if the attack is carried out, it has consequences on the assets, causing an unfavourable impact on them [27].

In general, vulnerabilities expose systems to threats. However, while these concepts are often related and, in that order, it is possible to be exposed to threats without being particularly vulnerable. This is the case with social engineering.

Risk analysis constitutes a critical component of cybersecurity, especially in the context of IoT systems, where vulnerabilities and threats are known to evolve rapidly. Although quantitative approaches, such as those delineated in [28], provide valuable mathematical models to assess operational, business, and financial risks, it is traditional for cybersecurity risk management to rely on qualitative methods.

This predilection for qualitative approaches is rooted in the unique characteristics of cybersecurity threats, which often involve high levels of uncertainty, dynamic threat landscapes, and the need for rapid decision-making. Frameworks such as NIST and MAGERIT emphasise the identification and prioritisation of risks based on their impact and likelihood, without requiring precise numerical estimates. These methodologies focus on understanding the context, assets, and potential threats to guide the implementation of safeguards and response strategies.

In light of the unique challenges posed by the security of private smart environments, this work adopts a qualitative approach to risk analysis. Quantitative methods, while valuable in some contexts, are less practical in environments where attack vectors change rapidly and incomplete data limits their applicability.

To carry out the mentioned risk analysis, there are multiple methodologies that facilitate the process, including the national MAGERIT already mentioned. Some of the most well-known ones include:

- EBIOS: Originally created for French entities and focused on information systems. Divided into five modules: study of the context, identification of the origin of the risk, risk analysis at the level of primary assets, risk analysis at the level of support assets, and risk evaluation, treatment, and acceptance.
- MAGERIT: CSAE-designed framework that proposes a systematic method of risk analysis along with planning for their treatment. The process involves characterising assets, threats, safeguards, risk estimation, impact and residual risk assessment, and a security plan.
- NATO: A qualitative methodology for monitoring assets. The phases include approval of management, planning and preparation, identification of critical assets, threat analysis, vulnerability analysis, risk calculation, risk assessment, and audit of implemented countermeasures.
- MONARC: A risk management tool based on the capitalisation of previous analyses. It includes setting a context, risk modelling, risk assessment and treatment, and implementation and monitoring.
- ITSRM: A methodology that is part of information security standards. The phases include system characterisation, primary assets, support assets, system modelling, risk identification, risk analysis and evaluation, and risk treatment.
- CRAMM: A qualitative risk analysis methodology with phases including identification and valuation of assets; identification of threats and vulnerabilities and risk calculation; and identification and prioritisation of response measures.

There are many others, such as the NIST or OWASP guides, and they all address a fairly similar set of phases. First, those that offer only qualitative analysis were discarded. Furthermore, it should be noted that all risk analysis methodologies must be initially adapted to the specific IoT system in question.

Of the remaining options, those that seem to offer greater adaptability are ITSRM and MAGERIT. In this case, MAGERIT has been selected as it is a methodology that allows more flexibility by modifying certain aspects of the proposed framework. In addition, it is made up of three books: the first, which outlines the risk analysis and management procedures; the second, which provides a catalogue of assets, threats, and safeguards; and the third, which offers a guide considering legal issues. MAGERIT also provides a tool called PILAR developed by the CNI for risk analysis.

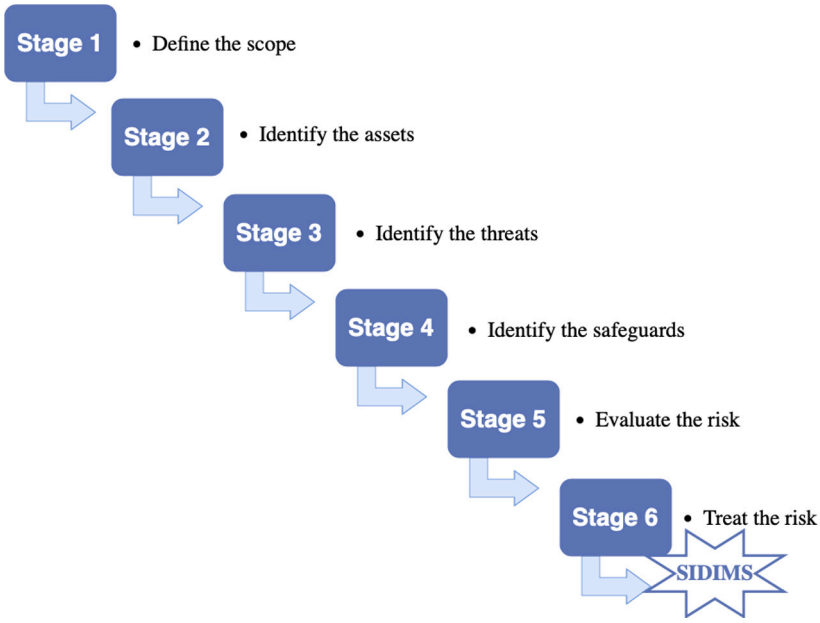


Fig. 8. Stages of the risk analysis.

MAGERIT is maintained by the General Secretariat of Digital Administration (Ministry of Economic Affairs and Digital Transformation) in collaboration with the CCN [29]. Specifically, an adaptation of MAGERIT proposed by INCIBE [30] has been chosen. The phases to be followed are shown in Fig. 8 and are applied in an environment such as the smart home. According to MAGERIT, the dimensions of security are availability, integrity, and confidentiality, with two derived dimensions: authenticity and traceability.

Ideally, risk analysis should be performed before services are operational so that measures can be taken in time to make decisions in the event of a risk. In many cases, prevention may not be possible due to a lack of access to design and development processes, so the only option is to correct and mitigate risks. However, in both cases, prevention or mitigation, risk analysis is a profoundly useful tool.

In this regard, an alternative considered was to apply the risk analysis methodology before designing the system architecture. However, since risk analysis is an evolving process, this would entail a constantly changing architectural design. Precisely due to the lack of a reference IoT architecture, this alternative was discarded, opting for an architecture design based on requirements. Thus, risk analysis makes sense when carried out before proposing mechanisms to improve the security and privacy of the smart home, which work together in the proposed system architecture.

The proper way to carry out risk analysis is to prioritise risks by importance, that is, seeking the highest impact, highest risk, and highest probability. It should be noted that even with a correctly conducted risk analysis, the risk is not reduced to zero but to a level that the home occupants find acceptable.

5.1.1. Scope and asset identification

In corporate environments that require scalability and have many assets, a risk analysis could be performed by selecting a limited set of specific areas. In this practical case of the smart home, the entire scope of the smart home is considered manageable. All types of device connected to the network, whether IoT or non-IoT, are contemplated. These include any identified in previous categories, such as smart thermostats, smart locks, smart TVs, smart bulbs, among many others.

Adapting the MAGERIT catalogue to the smart home, the assets in this case study are divided into different types:

- Essential assets without which the system cannot function.
- Data and information required by the system to provide the service.
- Services offered to meet the needs of users.
- Software or computer applications that use data to perform tasks.
- Hardware or computer equipment, the devices themselves that support the software automating tasks and providing services.
- Communication networks, protection of data transport media.

These catalogues asset types translate into three essential ones studied in this use case: services offered to home occupants, devices that handle specialised software to provide these services, and the managed data exchanged.

Table 4
Identified assets.

ID	Type	Device	Risk value
AS1	Comfort and lighting	Smart bulb	–
AS2	Entertainment	Smart TV	–
AS3		Smart speaker	–
AS4	Security	Security camera	–
AS5	Home appliances	Robot vacuum cleaner	–
AS6	Energy management	Smart plug	–
AS7	Control devices	Smartphone	–
AS8		Tablet	–
AS9		Computer	–
AS10		Router	–
AS11		Smart personal assistant	–
AS12	Health	Wearable	–

In fact, connected devices are considered particularly vulnerable, as described in Section 1. Therefore, special attention will be given to protecting these assets, and, by extension, services and data will also be protected. The different connected devices considered in the study environment are summarised in Table 4.

Table 4 includes devices that are part of the case study in the smart home, without specifying the number of devices connected to the network. Regardless of the quantity, all devices of the same type will have the same result in the risk analysis. In other words, two smart bulbs from different manufacturers may be exposed to different vulnerabilities. But for risk analysis, both are treated the same way. What would be modified based on their brand and model is the reliability label associated with them in the SIDIMS databases.

The column "Type" refers to the scope of application or main purpose of the device, that is, by the facility the device offers and therefore the type of task it covers. Regarding the "Risk level", this is calculated based on the map resulting from the risk analysis. Thus, an asset affected by the risk of the occurrence of various threats will have a risk level weighted as a result of the threats that affect it.

5.1.2. Identification of threats and safeguards

Once the assets to be protected have been identified, the next step is to determine the threats they are exposed to. Unknown threats that do not pose a risk or are not related to the identified assets are excluded from this risk analysis and will not be studied in the next phase.

Although there are multiple types of threats (natural such as earthquakes, accidents derived from human activity such as fire, etc.), this study focusses on intentional attacks that result in errors and failures in the system. The identified threats are shown in Table 5.

As with assets, the qualitative risk value that the identified threats will have in this risk analysis can be estimated logically and coherently. However, the quantitative value will be obtained as a joint result of individual risks. In other words, a threat that is relevant and high-risk for multiple identified assets will have a higher resulting risk value. In fact, these threats imply derived errors, such as monitoring errors (*logs*), information leaks, alteration, and/or leaks of information, or system crashes.

To address the identified threats, there are tools called safeguards that are updated over time and adapt to new vulnerabilities and existing threats. It is as important to identify the tools that address the detected problems as it is to assess how effective they are against the risk. In this case, the existing safeguards for the identified threats are the following:

- Identification and authentication
- Logical access control
- Task segregation
- Incident management
- Intrusion detection and prevention tools
- Vulnerability analysis tools
- Content monitoring tools
- Log analysis tools
- Honey net/honey pot
- Vulnerability management
- Logging and authoring
- Protection of information
- Data security backups
- Data encryption
- Use of electronic signatures
- Updating and maintenance of devices
- Protecting the integrity of exchanged data
- Application of security profiles
- Protection of communications
- Channel authentication
- Ensuring availability
- Cryptographic protection

5.1.3. Risk assessment and treatment

Risk assessment is carried out for each asset-threat pair. Based on the probability that the threat will occur and the impact it would have on the user and the home, the environment-calculated risk is determined. This computation can be performed in quantitative terms because of its consequences and in qualitative terms because of its relative importance.

Table 5
Identified threats.

ID	Threat/Intentional attack	Asset type	Dimensions	Risk value
TH1	Manipulation of activity logs	Data	I	–
TH2	Impersonation of the user's identity	Data, Services Devices	C, Au, I	–
TH3	Abuse of access privileges	Data, Services Devices	C, I, Av	–
TH4	Unintended use	Data, Services, Device	Av, C, I	–
TH5	Dissemination of malware	Devices	Av, I, C	–
TH6	Unauthorised access	Data, Services Devices	C, I, Av	–
TH7	Traffic analysis	Data	C	–
TH8	Interception of information	Data	C	–
TH9	Deliberate modification of info	Data, Services, Devices	I	–
TH10	Destruction of information	Data, Services, Devices	Av	–
TH11	Disclosure of information	Data, Services, Devices	C	–
TH12	Manipulation of programs	Devices	C, I, Av	–
TH13	Denial of service	Services, Devices	Av	–

Fig. 9. Risk assessment for each threat-asset.

Therefore, first, it is necessary to estimate the impact on the asset as a result of the threat; and then, the risk based on the calculated impact and the threat's contingency rate. The quantitative result involves weighting the risk values assigned to assets and threats.

The matrix shown in Fig. 9 is extracted by mapping the inventory of assets and the threats that affect each of them.

The green cells indicate that the risk is negligible or even zero in cases where the probability of that threat affecting the asset is non-existent. The yellow ones also do not imply extreme risk situations. Therefore, the system will consider these as acceptable risks and their attention will not be prioritised, either because it is a very low probability or almost negligible impact.

The values of each cell in the matrix were obtained by assigning values from the MAGERIT scale. This value is not subjectively chosen, but is selected based on standard tables specified in the MAGERIT catalogue that regulate these values of assets.

Considering that impact and probability are scored from 0 to 10, the risk results in a value from 0 to 100, and it is classified as defined in the legend of Fig. 9. Cells outside the matrix also indicate risk values, but these are the weighted results for each threat and asset (the unknown values in Tables 4 and 5).

As a result of the risk analysis, the system prioritises those that are important or critical, that is, with a risk value greater than or equal to 50%. Regarding the rest of the risks considered, with a quantitative value lower than 50%, these are considered acceptable risks since they have very low impact or occur in remote instances, with a very low probability.

Once the risk of each threat is identified and prioritised, solutions proposals are required in this phase. The proposed solutions are detailed in Sections 5.2 and 5.3.

Regarding the resulting risk values for each asset, these are taken into account for the reliability label used by the system. This label will be modified based on the brand and model (for known vulnerabilities thanks to external databases) and vulnerabilities detected by SIDIMS based on their behaviour on the network.

However, this process is cyclical and the phases carried out require monitoring and review, as both assets and threats can change over time. For the proposed resolution of identified threats, existing safeguards related to the identified assets will be used as a reference.

5.2. Mechanisms for integration of connected devices

This section delves into specifying the secure integration process of devices into the smart home. To do so, it is necessary to address the risks identified in Section 5.1. The mechanisms proposed in this section do not tackle risks individually, but suggest a controlled phase for integrating devices into the smart home. This approach improves the security and privacy of the system and, in general, addresses the identified risks. Section 5.3 deals with risks that cannot be assumed with customised mechanisms.

Currently, commercial devices integrated into the smart home come with a proprietary or third-party application responsible for their inclusion in the network. This process usually involves downloading the application, finding the new device on the network, and performing a series of trivial configuration steps. In addition, users are often required to accept a long and complex privacy policy.

In general, there is a lack of adequate control in the device inclusion process at home. There are no mechanisms to verify this device integration phase, such as which user is including it, whether a controlled device is used for configuration, or the vulnerabilities associated with the new device.

There is a possibility that an unauthorised person may integrate devices simply by decrypting the access credentials to the network. The current device integration process does not consider this possibility and therefore does not offer a solution to it. There is also the possibility that an authorised user performing this action may integrate a highly vulnerable device.

Once a device is included in the smart home, users receive no information about its security or the treatment and preservation of the data it handles. To address this issue, a set of mechanisms and tools designed to continuously analyse the network for unknown devices is proposed. In addition to attempting to control newly detected devices, the characteristics accompanying such connected devices are systematically examined, as addressed below.

5.2.1. Unknown devices detection

To detect whether a device is unknown to the system, the component responsible for monitoring and capturing data continuously analyses devices connected to the network. This identification is done by IP address, which is then checked in the database to determine if the device is known or unknown.

Because the IP address associated with a device is not fixed, as soon as a device is detected, the associated MAC address is obtained, allowing for a unique identification within the network. Therefore, for the detection of a new device, only an identifier is needed to check its existence in the database.

To obtain the MAC address associated with the device, the system translates the recently detected IP address using software tools such as ARP. This tool establishes the relationship between the IP address of a device and its corresponding unique MAC address.

This monitoring, acquisition, and storage process is nearly instantaneous. Once these tasks are completed, the component responsible for the system's event processing comes into play. This component generates a complex event formed, on one hand, by this basic information about the new device (with IP/MAC identification), and on the other hand, by additional information obtained from external servers. The purpose of this event is to alert the user of a new device, requiring all possible information associated with the newly detected device.

5.2.2. Characterisation of integrated devices

In addition to the basic identification for device management in the system, connected devices differ according to certain defining characteristics. The technical sheet of a connected home device is shown in Fig. 10.

The technical sheet is fed by a JSON document where all the basic information extracted at the time of detection is recorded, along with additional information about the device characteristics. This additional information extracted from external servers and translated into JSON includes category, brand, model, and associated vulnerabilities. However, information such as the group to which the device belongs, or the owner user may be added manually from the user interface.

Regarding vulnerabilities associated with the device, the system continuously checks listening ports as they can represent access points for attackers, thus posing a threat to the device. Additionally, concerning vulnerabilities, there are multiple databases providing information on attacks recorded over the years on connected devices. Vulnerabilities associated with the device can be queried by device type, manufacturer or seller, model, etc. Some examples of these databases and search engines include:

Fig. 10. Mock-up of the device technical sheet.

- SHODAN [31]
  This is a search engine for systems and services connected to the network. It provides information on vulnerabilities by IP address of the device, port, attack concept, etc. Any machine connected to the Internet appears in this search engine, such as smart TVs or smart locks.
  In our context, this search engine provides information about how exposed a device or service can be, helping to protect it from cyber attackers.
- MITRE ATT&CK and CVE [32,33]
  It is a protection framework that offers data matrices for security evaluation and knowledge of vulnerabilities. These matrices are filled with information on real attack methods, tactics, and techniques. It is an often-updated framework of vulnerabilities aiming to characterise the behaviour of attackers on the network.
  CVE is one of the main and largest glossaries of vulnerabilities and attacks. It is related to MITRE as the latter provides CVE with documented vulnerabilities to keep both updated. It is very up-to-date and allows queries by manufacturer, device, attack date, etc. It also has an internal search engine, such as Bing.
- VARIoT [34]
  It is a database of vulnerabilities and exploits for IoT devices. It draws from multiple data sources and aims to facilitate IoT device security management. Vulnerability searches in the repository are done through an API and allow, for example, to obtain a list of possible vulnerabilities for a provider and model.

There are many others, such as the NVD (National Vulnerability Database) and exploits (exploit-db), that provide more generic information. Since they do not focus on IoT issues, their scope does not align with the research line of this paper.

All the information mentioned is included in the JSON and shown in Fig. 10, which includes:

- ID: It is generated randomly when the device is included in the database.

- Alias (optional): Must be manually included from the user interface.
- Category: The user can manually include device behaviour. This information can also be obtained by using tools that analyse the behaviour of devices in the network, thus identifying this behaviour with a specific type of device [25]. These tools, along with the manufacturer, provide clues about the type of device. However, other alternatives allow this information to be obtained in addition to asking directly from the user interface. Some more sophisticated methods involve including a QR code in the device or its containing box [35]. This idea emerged years ago and is becoming more established in devices.
- IP Address: Various software tools allow device detection in the network using IP address scanning tools such as ARP and NMAP.
- MAC Address: This unique device identifier is obtained by translating the IP address into MAC using software tools such as ARP.
- Brand: Information obtained by querying the OUI. This identifier corresponds to the first three bytes of the MAC address and allows the manufacturer to be identified. This is because each manufacturer reserves a set of 24-bit identifiers with IEEE, and this allows queries to obtain information about manufacturers and reserved address ranges [36].
- Group (optional): Must be manually included from the user interface.
- Owner User (optional): Must be manually included from the interface.
- Connection History: There is a record of the moments when the system has detected the connection or disconnection of a device. SIDIMS continuously monitors the network for changes in connections that need to be recorded. This is also done through software tools like ARP and NMAP.
- Alert History: A record of alerts sent to the user interface is kept of both attended and ignored ones. Each alert has a description of the event, possible solutions offered by the system, and the alternative selected by SIDIMS or, if required, by the user. Examples of alerts include the detection of new devices, discovery of new anomalies in devices, detection of anomalous behaviour in the network, etc. This process is detailed in Section 5.3.
- Vulnerability History: Unlike the alert history, in this case, only known vulnerabilities related to a specific device are recorded. These may be due to open ports discovered in a network port scan with NMAP, known vulnerabilities from queries to external databases, or vulnerabilities due to anomalous behaviours. It only reports vulnerabilities affecting the device that serve to modify the device's reliability label. This process is detailed in Section 5.3.

This combined information allows to assess the security and privacy status of the device integrated into the smart home. The relevant aspects influencing the reliability label value are open ports and known vulnerabilities by manufacturer and device type. These are the factors that will modify the reliability label of each device obtained from the risk analysis in Section 5.1.

The other part of the mentioned complex event is completed with this additional information extracted from external databases. Once the generation of the complex event is complete, it is notified through the user interface for confirmation of the device's inclusion. This notification includes all the information obtained, covering both the device type and manufacturer, as well as device vulnerabilities (due to open ports and registered in external databases).

If this notification is not addressed from the user interface, the device can continue to operate on the network but with a low-reliability label. These reliability labels are integer values from 0 to 5 that identify how reliable the device is (represented in Fig. 10 by stars). This also applies to users. In both cases, the label is modified based on vulnerabilities, attacks, or questionable security actions they are involved in.

However, depending on the acceptable risk level of each specific home, the system may also block or restrict access to an unknown device without the need for human intervention. If an unknown device is considered to pose a critical risk, access to any unknown device will be denied by default, and the user will have to expressly allow its access.

After integration, the user is allowed to complete the device's technical sheet with other parameters already mentioned that do not affect the device's security but allow easy management. These include alias, group, or home location to which it belongs, and the owner user, that is, the predefined user to use this device because they are the sole owner. This initial verification allows the user to be aware of the devices in their smart home and that there are no other non-member users using the private network to connect their devices to the Internet.

5.3. Mechanisms for connected devices monitoring

Despite maintaining control over the integration process of connected devices in the smart home, this does not exempt the environment from the existence of threats to consider. This section presents a set of security and privacy management mechanisms for smart home devices that require continuous monitoring to address these issues.

In addition to comprehensive threat monitoring, management includes a response component to address detected problems. Based on risk analysis, the system determines whether it can autonomously resolve an issue or whether it needs to involve the user for decision-making and subsequent action. The system prioritises alerts based on the risk of involved assets and the threats they pose.

The issues identified as acceptable risks for the user do not require attention, such as those categorised as negligible or low risks in Fig. 9. An example requiring user intervention is a critical risk, such as handling sensitive data resulting in the denial of access to resources by a device.

This section delves into the management of smart home security and privacy through protection mechanisms against vulnerabilities affecting devices and materialising threats once exploited.

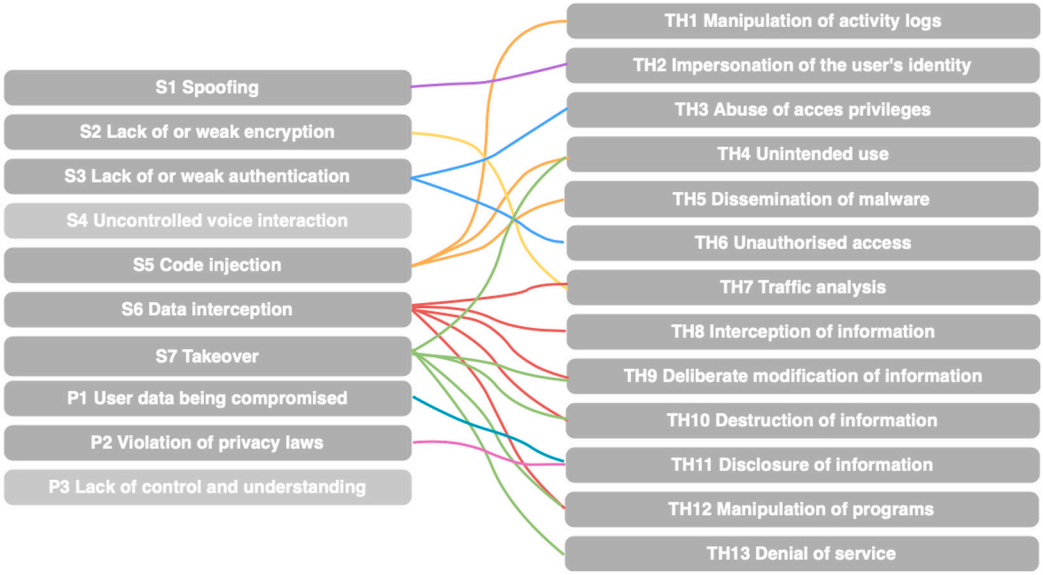


Fig. 11. Threats in relation to security and privacy vulnerabilities.

For this, the system must continuously monitor the network and perform periodic queries to external servers. Since storing and analysing all captured information retroactively would be impractical, the system analyses it in real-time and only stores data related to detected vulnerabilities.

First, a set of mechanisms is presented that address known vulnerabilities and threats, that is, the threats considered in the risk analysis. These threats have a characterisation defined in the risk analysis methodology. They could be a type of attack that behaves in a specific way in the network, knowledge of existing threats due to open ports with listening services, information about vulnerabilities specific to a device based on firmware version, existing threats due to insecure protocols, etc.

Finally, unknown threats to the system will also be detailed, either because they are not addressed in the risk analysis or because they have not materialised before, so they are completely unknown. These situations refer to any irregular or anomalous behaviour that may pose an unforeseen risk to the security and privacy of smart home assets.

5.3.1. Protection against contemplated threats

Threats previously identified by the system are known threats due to their predefined and characterised behaviours at the network level.

In general, and as already mentioned, vulnerabilities expose systems to threats. Therefore, it is of interest to categorise the existing vulnerabilities that affect the type of private environment to be addressed. In this case, we take as reference the vulnerabilities (named with "S") and privacy (named with "P") studied by the authors in [37], which are:

- S1 - Spoofing
- S2 - Lack of or weak encryption
- S3 - Lack of or weak authentication
- S4 - Uncontrolled voice interaction
- S5 - Code injection
- S6 - Data interception
- S7 - Takeover
- P1 - User data being compromised
- P2 - Violation of privacy laws
- P3 - Lack of control and understanding

Considering that a threat is a situation that exists due to the mentioned vulnerabilities, it is interesting to relate the threats identified from the risk analysis, shown in Table 5, and the vulnerabilities of [37]. This relationship is shown in Figs. 11 and 12.

It should be noted that threats related to uncontrolled voice interaction are not inherently considered in MAGERIT due to its recent surge in popularity. Many methodologies in their early versions do not address attacks related to vulnerabilities that generate such threatening situations. However, it could be related to other threats like "AM4 Unintended use", although the MAGERIT catalogue considers this threat in situations with assets not voice-controlled. However, in the characterisation of security vulnerabilities taken as a reference, this security vulnerability is considered. Thus, despite not appearing in Fig. 12, this security vulnerability is not excluded from the proposed mechanisms.

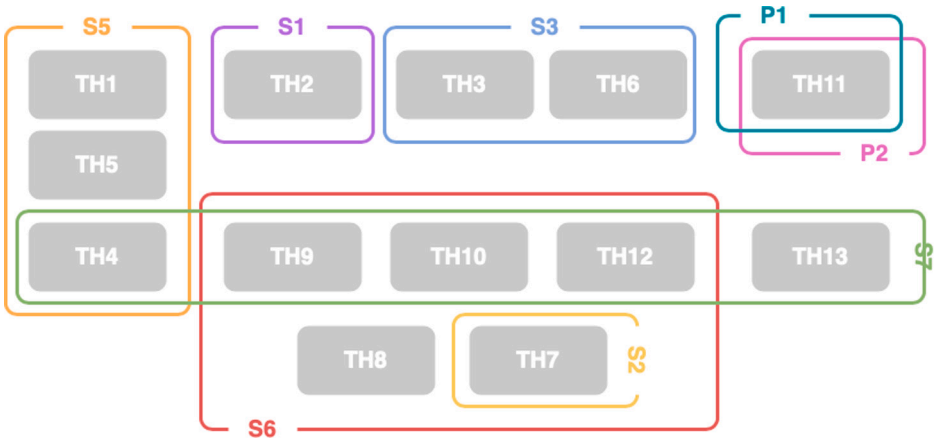


Fig. 12. Summary of threats in relation to security and privacy vulnerabilities.

Regarding the privacy vulnerability related to the lack of control and understanding, Fig. 11 does not associate it with any identified threat. This is not because it lacks implications, but because exploiting this vulnerability involves diverse human factors related to multiple types of threat. Specifically, the three privacy vulnerabilities, being closely related to security vulnerabilities, are directly addressed by protecting the latter.

In conclusion, protection against these vulnerabilities and threats begins with understanding and detecting them. To achieve this, the study is divided into queries to databases hosted on external servers, and specific software tools for intrusions, and AI tools.

External Databases

This data source contains information provided by other organisations and users, including vulnerabilities, attacks, and threats in the context of connected devices. Querying these databases and detecting vulnerabilities related to a specific device does not imply that the device is actually infected; it is susceptible to vulnerabilities registered by other users in the scientific community.

External databases, besides being consulted when detecting a new device, are periodically queried for updates on existing vulnerabilities. The component "Monitoring and Acquisition" is especially responsible for this.

Of the databases listed above, VARIoT and CVE Details are the most comprehensive. Table 6 provides examples of vulnerabilities that affect smart home devices extracted from these databases.

Next, some vulnerabilities existing in the databases are directly included in the security and privacy issues taken as reference:

- "S1 - Spoofing":
  An example in this category of security problems is CVE-2023-34246. It results from a weak authorisation vulnerability with OAuth2 that allows an attacker to spoof the user's identity. This vulnerability highlights the importance of keeping the device firmware updated, as it is resolved in versions higher than 5.6.6.
- "S3 - Lack of or weak authentication":
  Many recent vulnerabilities have been found in Huawei devices. Regarding this security problem, CVE-2022-28479 and CVE-2022-48360 emphasise vulnerabilities related to facial recognition devices that expose user information and confidentiality due to inefficient authentication.
- "S5 - Code Injection":
  CVE-2020-24983 addresses vulnerabilities discovered in Kronos devices, a smartwatch provider, due to SQL code injection to gain unauthorised access by acquiring administrator privileges.
  This privilege escalation issue is also detected in Fujitsu devices, LG TVs, and devices with outdated versions of Amazon Kindle Touch, CVE-2022-27089, CVE-2022-45422, and CVE-2012-4249, respectively.
- "S6 - Data interception":
  Vulnerability CVE-2016-5648 exposes incorrect SSL certificate validation allowing Man-in-the-Middle attacks with falsified SSL certificates. Although not as recent as other vulnerabilities, this has been one of the attack categories tested and included in the proposed methodology in Section 4.
- "S7 - Takeover":
  An example of takeover is CVE-2018-16706, revealing remote control vulnerabilities in LG devices (remote restart) without authentication, through HTTP requests on port 9080.
- "P1 - User data being compromised":
  Generally, this privacy issue can address multiple vulnerabilities. Specifically, CVE-2023-23304 highlights vulnerabilities related to the loss of user data confidentiality. This vulnerability has been recently detected in Garmin devices that may reveal user profile information and even GPS coordinates.

Table 6
Device vulnerabilities from CVE details.

Manufacturer	CVE ID	Definition
ACER	CVE-2022-24285 CVE-2022-24286	Local privilege vulnerability. The normal user obtains information to which he should not have access.
	CVE-2016-5648	The underlying Android application does not validate SSL certificates correctly, which can lead to a MitM attack with a forged SSL certificate.
Doorkeeper and Auth	CVE-2023-34246	It works with an OAuth2 provider, which has recent vulnerabilities related to weak authorization leading to possible cases of user impersonation. Issue resolved in versions higher than 5.6.6.
	CVE-2020-10187	Suffers info disclosure in versions higher than 5.0.0, where the attackercan retrieve the client secret intended only for the owner of the OAuth app.
	CVE-2016-6582	Vulnerability related to partial loss of integrity and availability due to poor resource access control management.
Garmin	CVE-2023-23304 CVE-2023-23299	Vulnerabilities related to the interception of private or sensitive user info, due to a vulnerable component that launchs a malicious app. User profile information and even GPS coordinates can be revealed.
LG	CVE-2022-45422 CVE-2022-23731 CVE-2020-9759	Vulnerabilities related to unauthorized access to higher user role privileges, detected in TVs.
	CVE-2018-16706	Vulnerabilities related to remote control of the device (remote reboot) without any authentication via HTTP requests on port 9080.
Kronos	CVE-2020-14982 CVE-2020-8495	Vulnerabilities affecting data confidentiality, such as SQL injection resulting in unauthorized access with administrator privileges.
Fujitsu	CVE-2022-27089	Privilege escalation vulnerabilities by an attacker are detected.
Huawei	CVE-2023-34157	Vulnerabilities in clock-related applications.
	CVE-2022-48314	Confidentiality problems in the Bluetooth pairing process.
	CVE-2023-34154	Vulnerabilities in virtual reality devices related to third-party apps.
	CVE-2022-48284 CVE-2022-48283	Privilege misassignment vulnerabilities that may allow access to private resources and functions through Huawei's smart home control software.
	CVE-2022-48479 CVE-2022-48478 CVE-2022-48360 CVE-2022-48256	Vulnerabilities related to facial recognition of some devices, which may cause service failures and even affect confidentiality.
Amazon	CVE-2012-4249 CVE-2012-4248	Detection of malicious code execution on Amazon Kindle Touch.
	CVE-2015-7292	Vulnerabilities in Amazon FireOS related to DoS attacks.
Qualcomm	CVE-2020-25859	Calling and handling of functions without input validation leading to privilege issues. Affects LTE and mobile routers.
	CVE-2020-25858	DoS attacks on smartphones, wearables and other IoT devices.

Since these vulnerabilities are alerts that the smart home device might be infected, the system does not act directly, but notifies when discovered (either through a query to external databases at the detection of a new unknown device or through a scheduled periodic query) and offers recommendations. These primarily include updating the device firmware to cover possible security gaps or, alternatively, blocking the device's access to the network if it poses a severe threat.

Software Tools for Intrusion Protection

These tools are designed to analyse network traffic in real-time and alert against potential intrusions. Therefore, the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) is proposed for the tasks of threat detection and prevention in the network. IDS is defined as a passive tool since it lacks the ability to take action, while IPS can actively intervene to prevent intrusion.

Given the objective of protecting against known intrusions or threats in this case, the choice is made for signature-based systems. Signatures are predefined and labelled patterns of network behaviour that enable the system to quickly identify the specific threat. Generally, when working with known rules, these systems offer few false positives in their threat alerts.

An entire scientific community is dedicated to this research area and is actively working on the generation of freely accessible signatures. Some well-known examples include Snort, Suricata, and Zeek.

In the following, we include some rules that directly address the security and privacy issues taken as a reference:

- "S1 - Spoofing"
  This involves detecting when a malicious user is attempting to modify packets, for example, with fraudulent source addresses that simulate a false identity. An example could be a Man-in-the-Middle (MitM) attack where, instead of passive eavesdropping, an attacker impersonates a false identity to intercept information.
  There are multiple ways to perform different types of identity spoofing. IDS rules help detect packets that involve suspicious parameters in their header. For instance, using Snort rules with filters for IP address and port, or using Suricata with rules for address range and any source port.
- "S2 - Lack of or weak encryption"
  One way to detect the absence of encryption, for example, is to continuously monitor packets for those using HTTP instead of HTTPS. In this case, it is also interesting to study the type of content that is exchanged without encryption, as it does not pose the same risk if it involves, for example, the transmission of unencrypted keys.
  Protection against this security issue involves identifying packets that meet the condition stated in the rule. SIDIMS would alert the situation and provide solutions. The most basic but also drastic solution is to block the vulnerable device, since it is creating a threatening situation.
- "S5 - Code Injection"
  In this case, rules are designed to detect requests that include special characters. For example, to detect an SQL injection attack, it searches for delimiters of text strings and comment delimiters.
  If the syntax is not used correctly, the generated SQL query can be misinterpreted to modify databases and execute system commands.
- "S7 - Takeover"
  To carry out a device takeover, one of the most common attacks is a Denial of Service (DoS). To detect it, the system must be capable of finding a match between the rule and a high number of behaviours in the system, and in a short time frame. For example, more than a hundred matches in less than a second.

By default, the IDS already mentioned comes with rules included by the official developers. These can be customised on the basis of the specific characteristics of each environment that you want to monitor. Generally, there is an entire community working on open source code development to create rules against new threats.

Artificial Intelligence Tools

In the cases previously discussed, the characterisation of known threats was stored in databases or structured in rule-based formats interpretable by software systems. In this case, datasets containing classified network traffic information are used, interpreted through AI tools.

One of the most informative datasets on IoT attacks is developed by the CIC [38]. It comprises a dataset of attacks on IoT devices labelled by simulating 33 attacks on a network consisting of 105 devices. The classified attacks and their respective security issues addressed are as follows:

- Identity impersonation attacks using ARP and DNS spoofing.
- Brute force attacks.
- Reconnaissance attacks, including ping scans, OS and port scanning, etc.
- Web-based attacks, such as SQL injection.
- Mirai attacks for flooding devices.
- DoS and DDoS attacks involving ICMP, UDP, HTTP, TCP flooding, etc.

These attacks are included in the security and privacy issues taken as a reference. For example, DoS and DDoS attacks classified in the dataset are included in "S7 - Takeover"; SQL injection attacks are categorised under "S5 - Code Injection"; identity impersonation attacks are in the "S1 - Identity Impersonation" group; and brute force attacks are part of the "S3 - Weak or Absent Authentication" problems.

However, the dataset also provides binary classification of behaviour as benign or malicious. Thus, whether using binary classification or selecting labelled attacks, the use of AI tools is proposed to detect malicious traffic in real time.

This requires pre-processing of data, to be performed by the Real-Time Captured Data Analysis component. This alternative uses algorithms, tools, and ML techniques such as supervised learning. The supervised learning approach requires a model trained on previously labelled data. The model learns known patterns to label the behaviour of the network.

In this case, the model output is a set of real-time labelled data. Traffic labelled as an attack or simply classified as malicious does not automatically trigger alerts; an event must be created for this purpose.

It is the component "Data Analysis" that notifies "Event Processing" of a network anomaly and communicates with the database to store the detected threat in the technical sheet of the corresponding device. The "Event Processing", after collecting threat information, notifies the event through the user interface and, if necessary, takes action on the device.

Depending on the threat, the solution may require more or less severe actions. In any case, SIDIMS has device-blocking capabilities if deemed appropriate.

Both this alternative and the previous ones regarding protection against known threats have a low rate of false positives. This is because alerts arise from the detection of a match when comparing traffic with characterised threats. Therefore, these mechanisms are effective when the system needs protection from known threats.

5.3.2. Protection against unforeseen threats

An unknown threat is defined as one that deviates from the identified norm or has not been considered through the risk analysis methodology. These threats fall outside the scope of the system's protection; however, there are certain mechanisms that prove to be highly useful when dealing with something unforeseen.

The most effective way to address this type of threat is through the use of tools that analyse network traffic compared to historical traffic that has been recorded and labelled normal. This requires a prior behaviour without anomalies.

There are detection (passive) and prevention (active) tools, such as anomaly-based IDS and IPS. These tools aim to detect anomalous behaviour based on deviations from the norm. An example of a system that operates with anomaly-based detection is Zeek. In this case, it does not require known attack signatures or patterns, but relies on the configuration of the typical network profile. This involves providing the tool with specific information to characterise normal behaviour, which should be well defined and have relatively stable characteristics over time.

However, there are other alternatives, such as the use of AI through unsupervised learning. This approach follows the same logic of comparing network behaviour with known traffic considered normal. It detects anomalies by identifying deviations from typical traffic and classifying them as anomalies.

The system detects anomalies at the slightest change in network behaviour, making these mechanisms less suitable for environments with variable network behaviour. Therefore, despite the interest in this alternative, as there are still unidentified threats that may have equally serious implications, this proposal does not delve into this approach. This is mainly because it is not as effective in a smart home environment, mainly due to the large number of alerts it would generate.

Furthermore, using detection and prevention tools like IDPS requires the configuration of the mentioned typical network profile. This is not an action that the system can automate; instead, it must be done manually by an administrator, which does not meet the requirements of SIDIMS. Similarly, with AI, technical knowledge about these tools is required to use them properly and interpret the system's output.

6. Conclusions

This paper highlights the technological advances that have led to the development and implementation of Internet of Things technologies in recent decades. In particular, the impact that this fact has had on the exponential increase in the number of connected devices and what this means in people's daily lives.

As a result of this fact, the security and privacy challenges posed by the use of connected devices in smart environments such as the digital home and the need for adequate mechanisms to protect against the threats that concern them are highlighted. This is due to the widespread lack of efficient protection mechanisms designed for these environments.

This paper addresses such security and privacy issues by proposing a security and privacy management system for connected devices and their integration into private environments.

The proposed system begins with an analysis of the requirements that must be met in private environments to preserve data security and privacy. In this sense, the system, ideally, is a module integrated as part of the router. Thus, the system, called SIDIMS, will have monitoring and action capabilities to effectively manage possible alerts in the network.

In addition, the architecture of the system has been designed with the user and his needs in mind, covering the requirements of the smart environment. It consists of the following components: (A) Monitoring and data acquisition, (B) Data storage, (C) Event processing, (D) Data analysis, and (E) User interface.

Finally, the design of the architecture components is deepened by proposing mechanisms to improve the security and privacy of private environments. Specifically, the digital home is taken as a use case, as it is a sensitive private environment with vulnerable users.

These mechanisms are responsible for the control of vulnerabilities, since these, exploited by an attacker, can lead to the existence and materialisation of threats that jeopardise the integrity, confidentiality, and availability of users' private data. Improving security and privacy on devices is addressed in the following way:

- An analysis of existing risks in the smart environment (digital home taken as a use case) is carried out to assess the existing situation. The result is a set of risks that the system can assume, either due to low impact or low probability, and other risks that must be addressed through the proposed mechanisms that are the focus of this paper.

- A controlled phase of device integration in the smart environment is defined that addresses the problems discussed in previous chapters. In this way, the user has control over the detection of new devices in the private environment, as well as information regarding these devices (such as vulnerabilities associated with this device, etc.).
- Security and privacy improvement mechanisms are proposed, focussing on device monitoring as a key point against threats. In particular, threats included in the risk analysis, which are generally characterised by known behaviour in the network, are addressed. Threats not included in the risk analysis are addressed by proposing software tools that compare the traffic to be analysed with a history known as benign traffic.

In short, as a result of existing severe security and privacy problems, this work introduces SIDIMS (Secure IoT Devices Integration and Management System) as a comprehensive framework to enhance security and privacy in private smart environments. The system architecture, which integrates real-time monitoring, user-centric event management, and advanced data analysis, addresses the growing challenges posed by the proliferation of IoT devices in private environments.

By emphasising user accessibility and implementing robust cybersecurity measures, SIDIMS offers a pragmatic solution to mitigate vulnerabilities while preserving usability for non-technical users. This is because it is a system as independent as possible, capable of autonomously making decisions on non-critical tasks and with immediate solution. In this way, the user does not have to manage the system and does not require any cybersecurity knowledge to use and understand it.

From a research perspective, SIDIMS contributes to the broader field of IoT security and privacy by offering a modular and extensible architecture that can be adapted to a variety of smart environments. The reliance on event-driven architecture (EDA) and zero-trust principles provides a robust foundation for addressing contemporary and future threats.

This work not only demonstrates the feasibility of integrating advanced cybersecurity mechanisms into router-based systems, but also highlights the importance of user-friendly interfaces to foster widespread adoption of secure IoT solutions.

The contributions of this research are relevant for several key areas of the academic and industrial communities:

- Cybersecurity Research: SIDIMS provides a testbed for exploring IoT-specific vulnerabilities, event-driven detection mechanisms, and adaptive threat mitigation.
- IoT Systems Design: The modular architecture and focus on interoperability provide valuable insights for designing scalable, multi-device IoT solutions.
- Human-Computer Interaction: As a user-centric system design, simplicity and clarity in the use of the system are key to bridging the gap between advanced cybersecurity features and usability.

Furthermore, the system's capacity for real-time monitoring and risk assessment paves the way for future research in adaptive threat detection and dynamic policy enforcement in IoT networks.

Beyond the immediate scope of this work, the flexibility and adaptability of the SIDIMS architecture facilitate the possibility of future applications and adaptations of the system to other environments.

As such, the proposed system applies not only to environments such as the one presented in the use case, but also to intelligent environments with different characteristics and requirements. This can range from environments with a large number of devices with high computational capacities and sensitive data, to smaller environments where security and privacy control of the devices connected to the network and the data they handle is also required.

With respect to environments with clearly different requirements, the system would be able to adapt to the new needs of the environment. For instance, integrating disaster response mechanisms could extend its applicability to critical scenarios, such as natural disasters. By leveraging its real-time monitoring capabilities, SIDIMS could detect and mitigate risks from environmental disturbances, such as earthquakes or floods. This could involve prioritising critical devices, automating emergency actions, and maintaining operational continuity under adverse conditions. This extension aligns with recent research advocating for smart disaster response frameworks in uncertain environments.

Another example of environments where the inclusion of SIDIMS is of interest are smart cities. Some notable aspects in which the system would improve the current situation of cities are early warning management and direct communication with emergency services, real-time monitoring of smart devices that improve environmental conditions (traffic, for example), among many others. It is important to mention in the context of this article the importance of energy management in this type of network, as well as the search for reliable and efficient IoT solutions.

Thus, while the present study focusses on smart private environments, the underlying principles and architecture can be extended to other domains, including smart cities, IoT in healthcare and industrial IoT. These extensions have the potential to generate further opportunities for collaboration and development within the research community.

CRediT authorship contribution statement

Sonia Solera-Cotanilla: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Manuel Álvarez-Campana:** Writing – review & editing, Supervision, Investigation, Conceptualization. **Carmen Sánchez-Zas:** Writing – review & editing, Investigation, Formal analysis. **Mario Vega-Barbas:** Writing – review & editing, Methodology, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to thank the RAYUELA project (contract no. 882828) of the Horizon 2020 programme of the European Union for motivating this work. The content of the article reflects the views only of the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

Data availability

No data was used for the research described in the article.

References

[1] M. Weiser, The computer of the 21st century, SIGMOBILE Mob. Comput. Commun. Rev. 265 (3) (1991) 66–75.
[2] K. Ashton, That internet of things thing: In the real world things matter more than ideas, RFID J. (2009).
[3] A. AlHogail, Improving IoT technology adoption through improving consumer trust, Technologies 6 (34) (2018).
[4] M.M. Alam, et al., A survey on the roles of communication technologies in IoT-based personalized healthcare applications, IEEE Access 6 (2018) 36611–36631.
[5] Y. Lu, Industry 4.0: A survey on technologies, applications and open research issues, J. Ind. Inf. Integr. 6 (2017) 1–10.
[6] F. Alam, R. Mehmood, I. Katib, N.N. Albogami, A. Albeshri, Data fusion and IoT for smart ubiquitous environments: A survey, IEEE Access 5 (2017) 9533–9554.
[7] S.H. Shah, I. Yaqoob, A survey: Internet of things (IOT) technologies, applications and challenges, in: 2016 IEEE Smart Energy Grid Engineering, SEGE, 2016, pp. 381–385.
[8] S.T. Ambujam, B. Mallala, P. Aggarwal, P.V. Prasad, Enhanced IoT-enabled community microgrid energy management with hybrid COA-HQNN approach with battery degradation consideration, J. Energy Storage (2025).
[9] G. Senthilkumar, B. Mallala, S. Sivarajan, C. Harish, D. Harsha, L. Natrayan, Maximizing power utilization through machine learning and IoT based power flow strategies in DC micro grids with renewable energy resources, in: 2024 International Conference on Inventive Computation Technologies, ICICT, 2024, pp. 1166–1171.
[10] B. Mallala, M. Faridun Naim Tajuddin, S. Babu Thanikanti, R. Reddy Manyam, Experimental analysis using IoT-based smart power quality analyzer system with remote data access and GSM alerting mechanism, IEEE Access (2025) 1166–1171.
[11] M. Abdel-Basset, R. Mohamed, M. Elhoseny, V. Chang, Evaluation framework for smart disaster response systems in uncertainty environment, Mech. Syst. Signal Process. 145 (2020) 106941.
[12] S. Anand, M. Vinodini Ramesh, An IoT based disaster response solution for ocean environment, in: International Conference on Distributed Computing and Networking, ICDCN, 2021, pp. 19–24.
[13] M. Sun, W.P. Tay, On the relationship between inference and data privacy in decentralized IoT networks, IEEE Trans. Inf. Forensics Secur. 15 (2020) 852–866.
[14] GSMA Association, IoT Security Assessment, Internet of Things, 2021.
[15] IoT Security Foundation, IoT Security Compliance Framework, Dic., 2018.
[16] INCIBE, Riesgos en el uso de dispositivos IoT, 2023, [Online] Available on: https://www.incibe.es/empresas/tematicas/iot. (Accessed August 2023).
[17] H.F. Atlam, A. Alenezi, M.O. Alassafi, A.A. Alshdadi, G.B. Wills, Security, cybercrime and digital forensics for IoT, Intell. Syst. Ref. Libr. (2020) 551–577.
[18] Nokia, Nokia: Threat intelligence report 2020, Comput. Fraud Secur. (11) (2020).
[19] N.V. Rajeesh Kumar, N. Jaya Lakshmi, B. Mallala, et al., Secure trust aware multi-objective routing protocol based on battle competitive swarm optimization in IoT, Artif. Intell. Rev. (2023) 1685–1709.
[20] The National Intelligence Council, Global trends 2040: A more contested world, 2021.
[21] W.K. Edwards, et al., At home with ubiquitous computing: Seven challenges, in: Ubicomp 2001: Ubiquitous Computing, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 256–272.
[22] Interaction Design Foundation, What is user experience (UX) design? 2023, [Online] Available on: https://www.interaction-design.org/literature/topics/ux-design. (Accessed June 2023).
[23] TIBCO, What is event-driven architecture? 2023, [Online] Available on: https://www.tibco.com/glossary/what-is-event-driven-architecture. (Accessed June 2023).
[24] M. Gilarranz, El ciclo de vida de los datos: las 5 fases para llevar a éxito un proyecto de big data, 2019, [Online] Available on: https://piperlab.es/2019/05/14/el-ciclo-de-vida-de-los-datos-las-5-fases-para-llevar-a-exito-un-proyecto-de-big-data/. (Accessed June 2023).
[25] I. Cvitić, D. Peraković, M. Perića, B. Gupta, Brij, Ensemble machine learning approach for classification of IoT devices in smart home, Int. J. Mach. Learn. Cybern. 12 (11) (2021) 3179–3202.
[26] INCIBE, Gestión de riesgos - una guía aproximada para el empresario, 2015, [Online] Available on: https://www.incibe.es. (Accessed July 2023).
[27] INCIBE, Amenaza vs Vulnerabilidad: Cómo Diferenciarlos, Dic., 2020, [Online] Available on: https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-diferenciarlos. (Accessed July 2023).
[28] V. Chang, R. Valverde, M. Ramachandran, C. Li, Toward business integrity modeling and analysis framework for risk measurement and analysis, Appl. Sci. 10 (9) (2020) 3145.
[29] Consejo Superior de Administración Electrónica, MAGERIT - metodología de análisis y gestión de riesgos de los sistemas de información, 2012.
[30] INCIBE, Análisis de riesgos en 6 pasos, 2017, [Online] Available on: https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo. (Accessed March 2023).
[31] Shodan, Search engine for the internet of everything, 2023, [Online] Available on: https://www.shodan.io. (Accessed March 2023).
[32] MITRE Corporation, MITRE ATT & CK, 2023, [Online] Available on: https://attack.mitre.org. (Accessed June 2023).
[33] CVE details - the ultimate security vulnerability datasource, 2023, [Online] Available on: https://www.cvedetails.com. (Accessed August 2023).
[34] VARIoT, Vulnerability and attack repository for IoT, 2023, [Online] Available on: https://www.variot.eu. (Accessed October 2023).

[35] K. Palacios, Internet of things: El código QR busca masificarse como una nueva forma de pagar tus compras, 2019, [Online] Available on: https://www.america-retail.com/tecnologias-emergentes/internet-of-things-el-codigo-qr-busca-masificarse-como-una-nueva-forma-de-pagar-tus-compras/. (Accessed October 2023).
[36] IEEE, OUI - MAC address lookup, 2024, [Online] Available on: https://standards-oui.ieee.org. (Accessed January 2024).
[37] S. Solera-Cotanilla, M. Vega-Barbas, et al., Security and privacy analysis of youth-oriented connected devices, Sensors 22 (11) (2022).
[38] E. Neto, et al., CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, Sensors 23 (13) (2023).