Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Generic Reference Model for the Internet of Things

Jochen Seitz

Jochen.Seitz@tu-ilmenau.de

Technische Universität Ilmenau

Ariel Aguirre

Technische Universität Ilmenau

Maik Debes

Technische Universität Ilmenau

Hubert Djuitcheu

ADTRAN (United States)

Ahmed Kashkool

Technische Universität Ilmenau

Raheleh Samadi

Technische Universität Ilmenau

Sindhu -

Technische Universität Ilmenau

Method Article

Keywords: Internet of Things, Reference Model

Posted Date: August 21st, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10382863/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A Generic Reference Model for the Internet of Things

Jochen Seitz, Ariel Aguirre, Maik Debes, Hubert Djuitcheu, Ahmed Kashkool, Raheleh Samadi, Sindhu

Communication Networks Group, Faculty of Electrical Engineering and Information Technology, Technische Universität Ilmenau, Helmholtzplatz 2, 98693 Ilmenau, Thuringia, Germany.

*Corresponding author(s). E-mail(s): Jochen.Seitz@tu-ilmenau.de;
Contributing authors: Ariel.Aguirre@tu-ilmenau.de; Maik.Debes@tu-ilmenau.de; Hubert.Djuitcheu@adtran.com; Ahmed.Kashkool@tu-ilmenau.de; Sindhu@tu-ilmenau.de; Samadi.Raheleh@tu-ilmenau.de;

Abstract

The Internet of Things (IoT) is far more than just a technical buzzword these days–it is the nervous system of the modern world. We are constantly surrounded by it today, as everyday objects communicate with one another autonomously and provide us with useful information and various services. The relevance of the IoT has become existential. We are in a phase where the physical and digital worlds are inextricably merging. It is no longer a question of whether we use the Internet of Things, but how we process the vast amounts of data securely and ethically. To specify an IoT system, a reference model must be defined that includes the essential aspects and describes the IoT system comprehensively, clearly, and yet simply. Over the past few years, several such reference models have been published; while all have their merits, they are very difficult to apply due to their complexity. Therefore, this paper presents a reference model that focuses on communication technology and is thus easy to apply.

Keywords: Internet of Things, Reference Model

1 Introduction

The Internet of Things (IoT) has its roots in the 80's of last century. Mark Weiser [35] defined the idea of ubiquitous computing, which is based on various sensors providing information about the environment that can be leveraged by different smart end devices to assist the user in everyday tasks.

Key application areas of the Internet of Things include Industry 4.0, smart cities, smart homes, and eHealth. For Industry 4.0, the IoT enables predictive maintenance and supply chain transparency through intelligent networking. In smart cities, the IoT can be used to design sustainable energy management and control traffic in an environmentally friendly manner. In smart homes, the IoT can help reduce energy consumption and increase personal safety. For eHealth, the IoT enables continuous monitoring of vital signs as well as the ability to call for help in an emergency.

There are manifold aspects to be considered when defining an IoT system. Thus, IoT reference models have been introduced that help holistically describe an IoT system. Due to the different backgrounds of the organizations that defined these reference models, the models became very complex and rather cumbersome to apply. Therefore, especially for teaching IoT to students, we tried to come up with a quite generic IoT reference model concentrating on the different components of the IoT system and how these communicate and interact. This paper presents our generic IoT reference model.

Therefore, we first have a look at existing IoT reference models which we introduce in section 2. Our proposed generic IoT reference model is explained in section 3. To show how to apply this model, we describe three different IoT use cases in section 4. Finally, section 5 concludes the paper.

2 Overview on Standardized IoT Reference Models

2.1 ITU-T Reference Model

In [23], the International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) defines the Fundamental Characteristics (FC) of the IoT:

1. **Interconnectivity** indicates that anything can be globally interconnected.
2. **Things-related services** shift the focus to thing-centric services, instead of human-centric services.
3. **Heterogeneity** refers to the adoption of different hardware, platforms, and networks.
4. **Dynamicity** refers to the fact that state, quantity and context of the interconnected things may change, and this variation should be handled.
5. **Scalability** expresses the expected vast number of devices for the IoT.

Based on these characteristics, a set of High Level Requirements (HLR) was defined as follows: identification-based connectivity, interoperability, autonomic networking, autonomic service provisioning, location-based capabilities, security, privacy protection, high-quality and highly secure human-body-related services, plug and play, and manageability.

According to these characteristics and requirements, the ITU-T proposes the reference model depicted in Figure 1. It specifies four horizontal layers, and two cross-layers within which a set of capabilities are defined as follows.

- **Horizontal Layers:**
  - **Application Layer:** This layer provides IoT applications to end users or business processes. They process and analyze data from lower layers and provide an interface for interpreting the data.

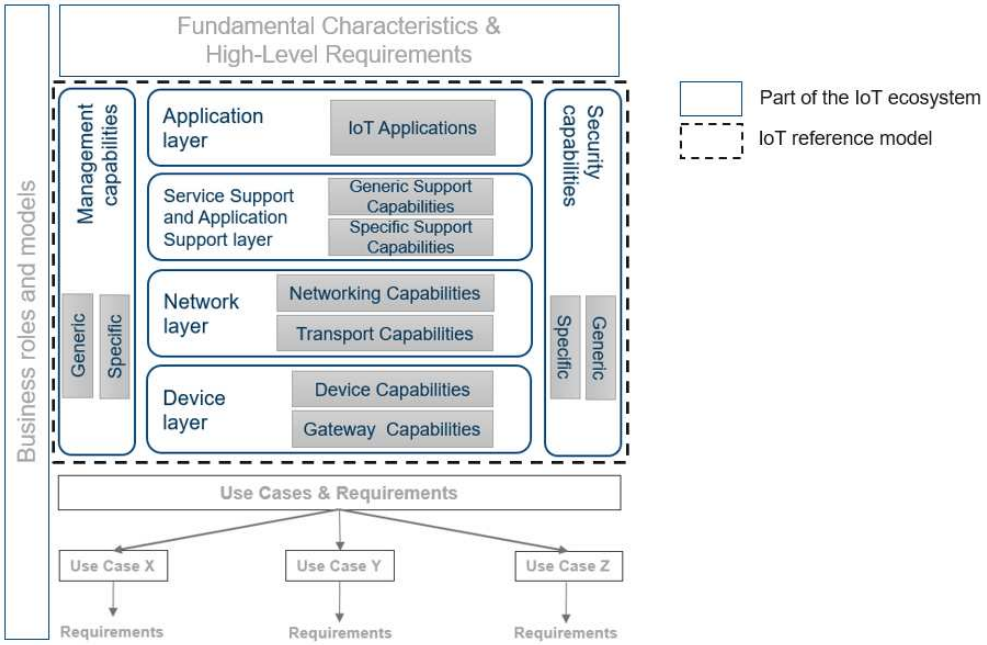


Fig. 1 ITU-T Reference Model adapted from [23]

- **Service Support and Application Support Layer:** The layer's generic capabilities include data processing and storage. Additionally, event management capabilities and interoperability functions are provided.
- **Network Layer:** The networking capabilities focus on control functions of network connectivity, while the transport capabilities target the transport of general data and IoT-specific control information.
- **Device Layer:** The device capabilities embrace direct and indirect communication, ad-hoc, sleeping and waking-up functionalities. As part of the gateway capabilities, multi-interface support and protocol conversion are considered.

- **Cross-Layer:**
  - **Management:** Similarly to classical communication systems, this layer covers fault, configuration, accounting, and performance management. The basic management activities regarding any system fall into generic capabilities, while the

specific capabilities provide space to accommodate the particularity of specific IoT implementations.

– **Security:** Generic security capabilities cover authorization, authentication, access control, confidentiality, privacy, and security audit activities. Additionally, specific capabilities allow to integrate fine-grained security requirements, for example, securing mobile payments.

2.2 Industrial Internet of Things (IIoT)

Industrial environments are subject to unique architecture challenges compared to standard IoT systems. While IoT enterprises and consumers emphasize on convenience, connectivity, and efficiency, industrial environments require more stringent systems, with particular emphasis on safety, reliability, fault tolerance, and real-time performance. As a result, IIoT covers the domain of machine-to-machine (M2M) communication rolling as a specialized branch to extend the principles of IoT in the industrial field [32]. Several reference models, such as Industrial Internet Reference Architecture (IIRA) [18] and Reference Architectural Model for Industry 4.0 (RAMI 4.0) [9] have been standardized for IIoT to improve productivity, reliability, and quality in an industrial environment.

2.2.1 Industrial Internet Reference Architecture (IIRA)

The Industrial Internet Reference Architecture (IIRA), developed by the Industrial Internet Consortium (IIC) provides guidance to system architects in building IIoT systems [18]. IIoT is not organized in layers, rather in tiers, viewpoints, and functional domains (see Figure 2).

1. **Three Tiers:**

   These tiers provide the following functions in the processing of the data flow and control flow.

- **Edge** collects data from edge nodes, for instance, sensors, controllers, and gateways.
- **Platform** receives, analyzes, and manages the data flow from the edge tier to the enterprise tier.
- **Enterprise** implements specific applications to provide the user-interface to the end user.

2. **Four Viewpoints:** They analyze various IIoT use cases, identifying the business point of view of the IIoT system, and determining the concerns of the expected system.

- **Business** is concerned about the vision, values, and objectives of the stakeholders to establish an IIoT system.
- **Usage** frames the typical activity of the expected system.
- **Functional** focuses on the functions of the system, including control and management.
- **Implementation** is concerned with the technologies required to implement the functional view.

3. **Five Functional Domains:** The decomposition of a typical IIoT system into functional domains highlights the importance of each building block.

- **Control and Monitoring** contains the functions performed by the physical components, such as the control units in autonomous vehicles.
- **Information** comprises functions as a collection of data for decision-making and system optimization to improve the long-term model of the system.
- **Application** applies rules, models, and application logic to realize specific business functionality.
- **Business** supports business activities that must be integrated to enable end-to-end operation of an IIoT system.

- **System Management** manages several distributed functional components.

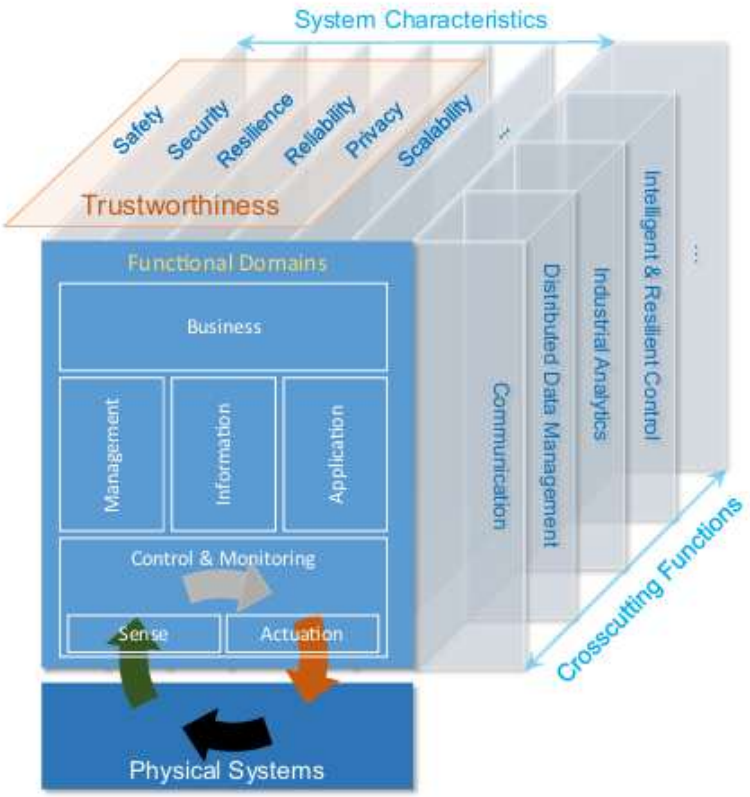


Fig. 2 Industrial Internet Reference Architecture (IIRA) according to [18]

2.2.2 Reference Architectural Model for Industry 4.0 (RAMI 4.0)

The Reference Architectural Model for Industry 4.0 (RAMI 4.0), developed by the German Industry 4.0 platform [9], extends the IoT concepts in the industry field and reveals the most important aspects of Industry 4.0 in a three-dimensional coordinate system.

Figure 3 shows the crucial three-dimensional axis of RAMI 4.0, which is the hierarchy levels axis, the life cycle value stream axis, and the layers axis.

1. **Hierarchy Levels Axis**: The right horizontal axis is a level of International Electrotechnical Commission (IEC) 62264 [19]. It reveals the position of the industrial elements in a hierarchical way, from the bottom products (items being manufactured), field devices (sensors, actuators), to the connected world (linking partners or supply chains).
2. **Life Cycle and Value Stream Axis**: It represents the life cycle of an industrial asset or product. It has two phases: prototype and, when prototyping is finished, an instance that is to be produced.
3. **Layers Axis**: The vertical axis consists of six layers, as stated below:

   - Business Layers: describes the commercial view, such as ordering conditions and monetary (price, availability of resources, and discounts).
   - Functional Layer: describes the logical functions of a technical functionality considering its role in the industrial 4.0 system, such as runtime and modeling environment for business processes.
   - Information Layer: describes the data have been used or modified by the technical functionality of the asset, such as rules and formal description of the model.
   - Communication Layer: describes the access of an asset to the information and functions of other connected assets, such as providing services about the asset's lifetime.
   - Integration Layer: describes the transition from the physical world to the information world, such as a Human-Machine-Interface (HMI).
   - Asset Layer: describes the asset that exists in the physical world and represents the interface between humans and the information world.

2.3 Comparison of the IoT Reference Models

The IoT reference models introduced above provide the foundation for the interoperability of IoT devices from different manufacturers without prescribing specific

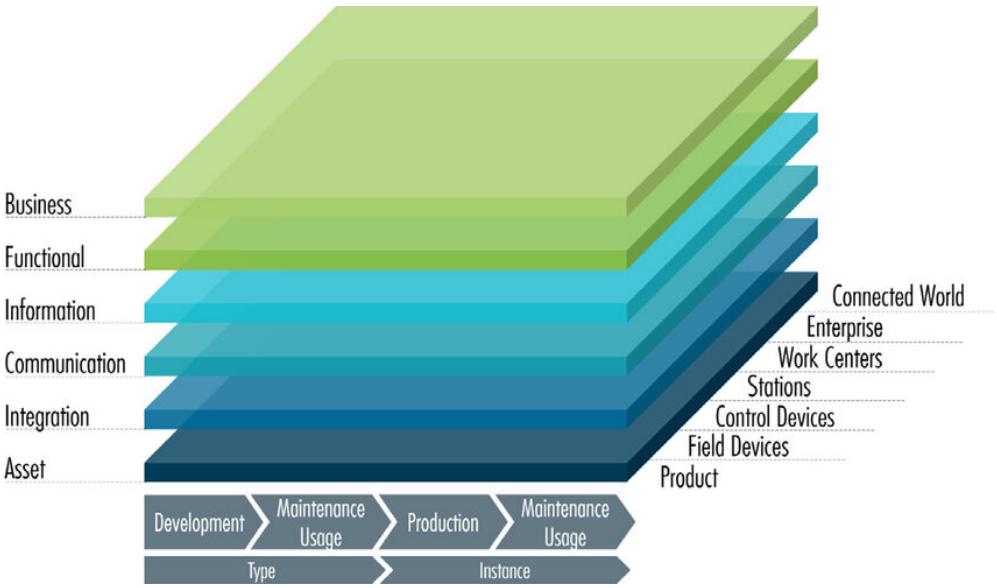


Fig. 3 RAMI 4.0 Reference Model according to [30]

products or protocols. They also distinguish between physical end devices, the necessary communication, subsequent information processing, and the applications built on top of them. Security is comprehensively addressed in all reference models, thereby taking into account the EU Cyber Resilience Act [11].

However, each reference model has its own specific strengths and weaknesses. The ITU-T reference model can be applied to many IoT domains and therefore defines a general IoT vocabulary. However, it is quite coarse-grained and does not model lifecycles. The IIRA is suitable for many industrial sectors and takes into account the respective business objectives. However, it does not describe a concrete technical reference architecture and leaves a great deal of room for interpretation, which quickly makes it too complex for simple use cases. RAMI 4.0 provides a very detailed representation of industrial plants and supports digital twins, but it focuses on manufacturing processes and is difficult for non-industrial users due to its high complexity. All models lack extensions toward Artificial Intelligence (AI) and an in-depth consideration of the cloud-edge continuum.

Our generic reference model presented in the next section attempts to reduce the complexity identified in the existing reference models in order to create an easy-to-use reference model that focuses primarily on the components of the IoT system, their communication with one another, and thus on the cloud-edge continuum. Therefore, it provides a communication-based modeling framework for IoT systems that can describe them across various use cases. As a result, it is also well-suited for university-level teaching.

3 Our Proposal for a Generic IoT Reference Model

This new proposal of a generic IoT reference model is depicted in Figure 4. The model contains the essential parts of an IoT system and illustrates the relationships between them.

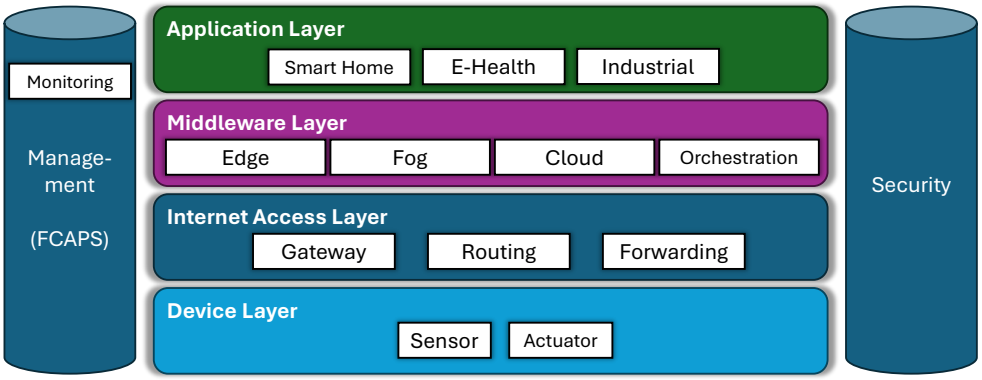


Fig. 4 Overview on the generic IoT reference model.

3.1 Device Layer

In the Device Layer, all the end devices are gathered that either offer information about the environment (e. g., sensor nodes), that can analyze the gathered information, or that can react to certain commands in response to the received information

(e. g., actuators controlling the heating). The devices are connected with each other through cables or radio. They can autonomously exchange information without the need of human interaction. Usually, these devices run on batteries, making energy efficiency an important factor [26]. This is also the reason for the reduced complexity of these devices, not allowing them to execute the Internet protocols directly, but rather running specific IoT protocols. Each of these devices plays a crucial role in the IoT ecosystem by enabling the collection of large amounts of data in real time. This data can then be used to increase efficiency, improve decision-making processes and gain new insights into the respective application areas.

3.2 Internet Access Layer

In a layered architecture, the Internet Access Layer plays a critical role in the establishment of connections in IoT networks. It consists of gateways providing connectivity and managing channel access between the IoT devices and border network segments, such as edge and cloud servers, or user applications. It acts as an interface between the Device Layer, where data are generated through sensors, and the Middleware Layer, which saves, processes, and analyzes the data. The Internet Access Layer ensures reliable and secure data flow from edge devices to fog nodes or cloud platforms [7].

The following key functions are provided by the Internet Access Layer:

- **Connectivity Management:** It focuses on providing connectivity, control and management information to transport specific IoT data information [23]. It supports various communication technologies to establish and maintain communication links such as Wi-Fi, Zigbee and Bluetooth, which are used for short-range applications, as well as long-range applications such as Long Range Wide Area Network (LoRaWAN), NarrowBand Internet of Things (NB-IoT), while traditional Ethernet has been utilized for wired networks.

- **Routing and Forwarding:** This function determines the transport of the data through the network. Routing identifies the optimal route from the source to the destination that accommodates the mobility of the device, constrained resources, and dynamic topology. On the other hand, forwarding refers to the processing of transferring the data along the previously selected path [24].
- **Error Detection and Correction:** This functionality supports different mechanisms for collision detection and avoidance to ensure reliable communication links, such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in Wi-Fi, and error detection schemes such as Cyclic Redundancy Check (CRC) [33].

Essentially, the Internet Access Layer bridges the gap between the physical hardware of IoT devices and the upper layers that handle data processing and application functionalities, acting as a gateway between IoT-specific communication technologies and the Internet.

3.3 Middleware Layer

The Middleware Layer acts as the central component in an IoT system. It receives the data from the Internet Access Layer, stores and pre-processes these, and lets higher-level applications and services access them in a uniform manner.

Therefore, different nodes provide edge, fog, and cloud functionality. Edge nodes are usually provided by public network providers and located at the edge of the network. They can process data in a real-time environment. Fog services are offered by other network nodes that provide additional resources to other nodes. Finally, cloud services are available in the center of the network. There, the highest processing power and the biggest data storage volume is available, but latency is also very high compared to edge or fog computing due to the distance between the data producing nodes and the cloud servers.

Nevertheless, the Middleware Layer hides the complexity of different hardware types, communication methods, and data formats. By doing this, it gives developers a standard and easier environment to build reliable and scalable IoT solutions. Without middleware, developers would need to deal directly with each device's technical details, making IoT systems much harder to build and maintain [8]. The main responsibilities of the Middleware Layer include:

- **Resource Abstraction:** IoT devices are often made by different manufacturers and use different protocols. The Middleware Layer offers a unified interface to interact with these devices, so developers do not need to know how each one works internally. This makes the system easier to scale and reduces development time.
- **Data Management:** Since IoT devices constantly produce large amounts of data, this layer helps by filtering, summarizing, and storing the data temporarily. It also prepares the data for real-time processing. Middleware provides Application Programming Interfaces (APIs) for configuration, telemetry, and firmware updates, which support system monitoring and control [28].
- **Service Discovery and Orchestration:** In many IoT environments, devices and services often change – new ones join, and others leave. Middleware helps automatically detect these changes and allows the system to adjust by combining services dynamically using technologies like Web Services Description Language (WSDL) or Constrained RESTful Environment (CoRE) Link Format.
- **Interoperability:** IoT systems use various communication protocols such as Message Queueing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), HyperText Transfer Protocol (HTTP), and eXtensible Messaging and Presence Protocol (XMPP). Middleware helps different devices "talk" to each other by translating between these protocols, even if they were not designed to be compatible [2].

The Middleware Layer plays a key role in simplifying IoT system design. It helps manage devices and data, ensures secure communication, and supports system growth by enabling interoperability and dynamic services.

3.4 Application Layer

In the Application Layer, applications for different IoT use cases offer their services and enriched information to the users. In Figure 4, we illustrated three use cases "Smart Home", "E-Health" and "Industrial", which we explain in section 4, but these are only placeholders for any other IoT applications.

3.5 Cross-Layer Security

Security and privacy are among the most critical challenges in the development of the IoT. The presence of attackers on the Internet poses a serious threat, as they can steal or modify sensitive information transferred from the devices.

In our proposed IoT reference model, the Security Layer is designed as a cross-cutting layer that is not isolated to a single layer of the architecture. Instead, it interacts with and provides protection services to all layers, ensuring that security requirements are met throughout the data lifecycle. This design allows the security mechanisms to work in parallel with functional processes at every stage, rather than being confined to a specific point in the system. At each layer, the following security goals will be supported by different functions:

- **Authentication and Integrity**: Verifying the identity of entities and ensuring data has not been altered during transmission.
- **Access Control**: Restricting resource usage and functions to authorized entities only.
- **Confidentiality**: Protecting the content of the data from unauthorized access.

Previous research [4] has focused on end-to-end security with hierarchical key-based control that involves intermediary devices. In contrast, our work presents a cross-layer security framework that enforces authentication, access control, and confidentiality through layer-specific protocols across IoT layers. Although centralized security models may introduce vulnerabilities, our approach integrates security as a cross-cutting layer, providing comprehensive protection throughout the architecture. Another research [34] also uses a cross-layer approach to secure IoT by focusing on the device, network, and service layers. Their framework is effective in addressing security at multiple points, making the system more resilient. However, our research extends this by adding a management layer that coordinates security across all layers, ensuring better integration and consistent enforcement of security policies throughout the IoT system.

Privacy is an equally critical concern in the IoT. It requires that user information be handled securely and accessed only by authorized individuals. In this context, privacy goes even further than security: it ensures that data remain in the control of its rightful owner and are not exposed to unauthorized access. Therefore, both security and privacy must be ensured by preventing unauthorized identification and access and ensuring that user data remain under their control.

In the proposed IoT reference model, each layer cooperates with the Security Layer by implementing the required functions for authentication and data integrity, access control, and confidentiality using specific protocols and interfaces, while facing distinct security threats.

Finally, continuous deployment and management of IoT security require integrated approaches that combine modeling, deployment, and operational feedback to address evolving security and privacy challenges efficiently, underscoring the importance of adaptive and automated security frameworks in maintaining resilience across the IoT system lifecycle [12, 27].

3.6 Cross-Layer Management

As IoT solutions generally embrace a wide variety of heterogeneous hardware and software components and technologies, especially in the case of complex systems, a natural challenge arises with respect to the management of the elements and the overall solution. [20] and [36] define a system management model and divide it into four main aspects: information, functional, communication, and organizational aspects. Within the functional aspect, [22] further specifies five functional areas of management: Fault, Configuration, Accounting, Performance, and Security management (FCAPS). Although they were initially thought of for network management, their use spreads also to monitoring resources and services, like the ones involved in systems such as IoT systems. In this sense, monitoring should not be seen as a separate functionality, but as an intrinsic task to achieve efficient and effective management [10, 31]. In this section, we explore the management dimension in more detail.

Traditional Management Solutions

A typical management solution is based on three elements: a manager, managed items, and agents. The manager is the entity used to handle a group of managed items. The items expose parameters like CPU utilization, interface status, addressing information, etc. that are of interest to the manager. The agent is the software running on the managed items whose tasks are to collect the parameters and transmit them to the manager [1]. Although the role of these three components is expected to remain the same, it is worth noticing some points when considering complex IoT systems.

- **Silos Monitoring**: Traditionally, monitoring activities are performed on the basis of subsystems. Every subsystem that is part of a complex system is independently monitored. Examples of such subsystems are computing, storage, and networking facilities. From the perspective of an IoT solution, it might be hard to determine

the correlation of events that influence the performance of the solution. That calls for a holistic monitoring approach.

- **Independent Management Tools**: Similarly to the monitoring case, the current management tools are usually independent of each other. That has worked well until now through a considerable coordination effort of support and maintenance engineers once an event triggers a troubleshooting campaign. Examples of such management tools include device, application, security, and resource management.
- **Protocols and frameworks**: In [29, 31] the authors provide a comprehensive overview of management protocols, frameworks, and management approaches for IoT low power networks. Among the classical management protocols are: Lightweight Machine to Machine Protocol (LwM2M), CoAP Management Interface (CoMI), Simple Network Management Protocol for IPv6-enabled Low-power Wireless Personal Area Network (6LoWPAN-SNMP) and Network Configuration Protocol (NETCONF) light. In terms of frameworks we encounter Cloud-based, Software-Defined Networking (SDN)-based, Semantic-based, and machine learning-based examples [1]. The emphasis lies primarily on monitoring the IoT design criteria defined, namely: scalability, fault tolerance, quality of service, energy efficiency, security, and self-configuration. Nevertheless, very little effort has been made to monitor holistically the service performance provided by the overall IoT system.
- **Challenges**: The silo strategy yields an increase complexity when the businesses require to become agile, either by reacting to demands or recovering from failure scenarios. The coordination among subsystem specialists makes it difficult to pinpoint an end-to-end strategy. As a result, the dependability of the system may be compromised.

Toward Unified Management Solutions

Research may experience a trend towards unified management solutions [31]. In Figure 4, we see that the management function is transversal, thus it might result

natural to think of exploiting this particularity to provide a holistic view over the resources and services of IoT systems tailored to specific use cases. [21] defines a layer architecture for the Telecommunications Management Network (TMN). Particularly important is the Service Management Layer, where specific monitoring activities can be allocated.

The increasing adoption of IoT systems, especially in critical scenarios like e-Health, smart grid, and industrial production, advocates for such a sophisticated management strategy. New technologies like cloud computing and artificial intelligence enable the development of a holistic approach in which inferences can be made based on the combined analysis of the individual Key Performance Indicators (KPIs) being monitored. Automatic reconfiguration of the subsystems could be triggered based on these inferences. This allows operators to react agilely in terms of business cases instead of subsystems.

- **Protocols and Frameworks**: To facilitate such unified management strategy, we can foresee the development of cross-layer protocols like [29]. Cross-layer protocols collect bits of information from different layers to support decision-making activities. They could be useful for specific IoT use cases where very low performance degradation may be tolerable, for instance, in the context of smart grids and industrial processes relying on real-time management.
- **Challenges**: Due to the heterogeneity of the IoT ecosystem, the adoption of standardized communication protocols and interfaces becomes imperative. A cross-layer approach should be able to consume data and provide instructions to the different elements involved through standardized methods. However, standardization is an ongoing effort by many actors. Another challenging vector concerns delegation of responsibility. For example, in the case where parameter values obtained via unified management serve as inputs for automatic corrective maintenance, the different actors may not know how to behave and might neglect responsibility.

4 Application of the Generic Reference Model

A reference model should be applicable to many different use cases without constraints or expressive problems fullfilling its generic purpose. Therefore, the reference model introduced in this paper is applied to three quite different IoT use cases, namely E-Health, Smart Home, and Industrial IoT.

4.1 E-Health: Individual Health Management

Whether our proposal for a generally valid IoT reference model can correlate with actual requirements in practice will be shown using an example. This is currently still largely to be regarded as fictitious. However, the development of information technology in the healthcare sector is actually moving towards such holistic models. For example look at the German digital patient file ([14]) or the Fast Healthcare Interoperability Resources (FHIR) standard ([16]).

4.1.1 System Components

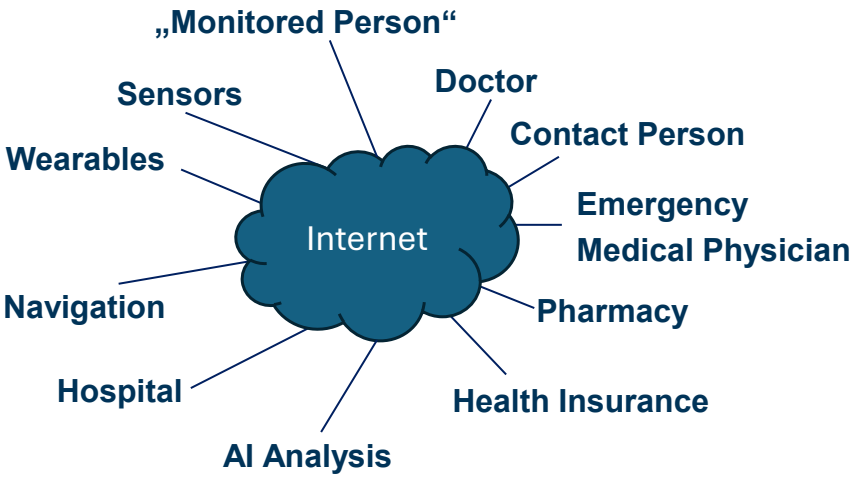


Fig. 5 Overview of the system components

The system we have assumed consists of the components shown in Figure 5, which are all linked to each other via the Internet. This includes the connection to the family doctor, who can access a person's medical data. It also includes a trusted contact person who is informed in the event of an emergency or can make decisions if the person is no longer able to make them on their own. An emergency medical physician can be contacted or called automatically in urgent cases. Necessary data can be used by a hospital, for example, to make appropriate preparations for rapid assistance when the person arrives, thus saving valuable time. A pharmacy is also involved, which is able to purchase the required medication at an early stage and receive prescriptions directly from the doctor. The planned connection to a navigation application serves to guide the person seeking help to the nearest hospital, pharmacy or similar. However, the emergency doctor can also be directed to them in cases where the person is no longer able to give his location. Sensors, wearables, etc. collect relevant data on the person's (health) status and provide additional information on the person's surrounding context (e.g. weather). The connection to the health insurance company is used, among other things, for direct billing of costs incurred. Finally, an AI analysis is provided to help the system and partners involved to make decisions efficiently and in the best interests of the person concerned and to forecast. The history of previous incidents, the person's own medical history, current vital signs and the overall context can all be taken into account.

4.1.2 An Example Scenario

While the components shown in the previous section actually exist in reality, the following scenario is fictitious in order to give an insight into the power of such a system.

We consider a person who has just been cycling and fell off the bike. The person is unconscious and also suffers from diabetes. She is equipped with wearables and sensors that record her vital signs as well as track current Global Positioning System (GPS)

data. The system we have assumed would have noticed the fall and would immediately initiate various emergency measures with the help of AI analysis.

Firstly, an emergency medical physician would be informed. This person can usually be reached via an emergency center, which is also immediately informed by the system of the location of the injured person and receives a recommendation on how best to care for the injured person based on the AI analysis. The emergency medical physician, who is also already informed about the person's diabetes, then decides that the person must be transported by helicopter as quickly as possible. At the same time, the nearest suitable hospital is informed of the incident and the estimated time of arrival of the casualty. The hospital can now make all preparations for admission and treatment. Additional information is provided by the emergency medical physician after the initial treatment.

At the same time, a message is sent to the contact person about the event informing about the status of the casualty, current assistance measures and the destination hospital. During the entire rescue mission, the system continues to monitor the vital signs and passes on information about blood sugar, blood pressure, body temperature, etc. in real time to the emergency medical physician and hospital, who can then adapt and take targeted actions.

4.1.3 Specification with Our Proposed IoT Reference Model

The following section describes how the system fits into our proposed IoT reference model and shows that this is suitable in principle for all IoT scenarios. The individual layers are considered and it is shown which functions, services and protocols they contain.

- **Device Layer:** This includes the end devices (e.g. sensor nodes, wearables, input devices, hardware connection of the emergency medical physician, etc.) that are used to collect or access data.

- **Internet Access Layer:** This layer mainly covers communication via Internet Protocol (IP). It also includes underlying functions, services and physical connections. These would be, for example, the connection via Ethernet and WiFi, including the protocols used there.
- **Middleware Layer:** This includes the communication between medical practice software, pharmacy software, and the services in the telematics infrastructure. These are provided via special protocols and standards that link the applications with each other. In our scenario, this could include FHIR. This is responsible for data exchange and uses JavaScript Object Notation (JSON) or eXtensible Markup Language (XML), for example, to represent the data.
- **Application Layer:** This concerns the software applications with which the human interactors work and thus access the system. It includes the tools that are available to the emergency medical physician, the hospital, the contact person, etc.
- **Security:** Security must be guaranteed across all horizontal layers in our data protection-sensitive system. For the Device Layer, this includes access control of the end devices, password protection if necessary, but also the spatial separation of servers that require protection and on which sensitive personal data is stored. One measure that belongs to the Internet Access Layer would be encrypted via Wi-Fi Protected Access version 3 (WPA3) in WiFi, for example. In the middleware, we find end-to-end encryption, e.g., using Transport Layer Security (TLS) and authorization of access via Open Authorization, Version 2 (OAuth2), as described in the FHIR standard. At application level, security is provided via authentication mechanisms. Two-way authentication or, even better, PassKeys should be used for login.
- **Management:** Management also covers all horizontal layers. This enables the system to carry out holistic monitoring of all layers and thus all components involved. For an efficient evaluation of the data, KPIs must be defined, as described in section

3.6, which can be responded to accordingly. In our scenario, this could be the vital signs, for example.

4.2 Smart Home

Many IoT reference models have been proposed to provide a structured framework to standardize and organize the interaction between data, devices, and services in a smart home environment. The smart home is a living environment system that allows all home appliances or household devices to be connected and controlled remotely to improve the customer's comfort, security, and energy efficiency. Therefore, the application of an IoT reference model ensures scalability, reliability, and data security across all devices and platforms [3, 13].

4.2.1 Smart Home Energy Management System (SHEMS)

Recently, many researchers in both industry and academia have focused on various techniques to enhance the health living environment and minimize unnecessary energy consumption for green smart cities. Smart Home Energy Management Systems (SHEMSs) are among these techniques, which integrate multiple smart home devices, such as lights, power meters, sensors, and solar inverters, into a systemized IoT architecture [5].

Several sensors and actuators are installed throughout the home to measure real-time environmental conditions, including voltage, temperature, light, and other data. These data serve as the primary data source for the SHEMS, which is collected and processed for further analysis. The IoT gateway collects data, processes and performs critical tasks such as data cleaning. The Energy Management System (EMS) extracts relevant patterns related to user behavior, which can be fed into a machine learning infrastructure to optimize opportunities and make decisions. The user interface provides homeowners with information on energy consumption patterns, giving them options to adjust settings and meet their energy management goals. [15]

4.2.2 Specification with Our Proposed IoT Reference Model

- **Device Layer** In this layer, several sensors and actuators continuously collect environmental and operating data. Smart thermostats measure indoor temperature and humidity, while smart plugs and power meters monitor energy consumption at the appliance level. Motion sensors detect the presence of occupants, while window sensors evaluate the availability of natural light. These data inputs are the system's base; they translate physical conditions into digital signals that higher layers can examine.

- **Internet Access Layer** The Internet Access Layer connects smart devices, home gateways, and external cloud servers. In this application scenario, Zigbee links low-power devices (lights, sensors), while Wi-Fi supports high-data-rate devices (cameras and speakers). A smart home gateway collects the data, translates them (for example, Zigbee-to-IP), and sends them to cloud or edge servers using secure protocols like MQTT or CoAP [3]. This connectivity layer ensures that the data flow smoothly while maintaining network security and quality of service.

- **Middleware Layer** This layer is responsible for data aggregation, storage, and analysis. Real time analysis and AI decision are applied via edge computing or cloud based data processing. Edge computing might perform time critical tasks, while cloud computing analyzes historical data to predict peak times and set an energy scheduling optimization. For example, when there is no motion in the room, it automatically turns off the lights and reduces the heating power [25].

- **Application Layer** This layer converts the middleware processed data into a meaningful user-facing service interface through dashboards and mobile apps to enable automation and energy consumption insights. Users can manage devices, monitor real-time energy consumption, or receive energy-saving recommendations. The user service interface applies automation rules, such as turning the lights on and off,

and automatically adjusting the heating based on the number of audience and the outside temperature.

- **Vertical Layers: Management and Security** Security and management span over all four layers and function as cross-layer vertical planes to ensure that all four layers are operating reliably. Management ensures that the system remains reliable and capable of long-term operations without human intervention. However, security ensures integrity, secure access control, and confidentiality for all elements of the IoT system.

4.3 Industrial Internet of Things (IIoT)

In this section, we introduce the differentiation between two terms that are usually used as synonyms: Industry 4.0 and Industrial Internet of Things (IIoT). Industry 4.0 refers to an umbrella term for all functional areas of a company, namely product development, sales, and after sales that, pursuing efficiency, follow a transformation impulsed by digitization, automation, and cognitive processing of the digitized information. Here, the focus lies on the core processes of a company. On the other hand, IIoT refers to the interconnection of a set of technologies to achieve a particular functionality that contributes to increasing productivity on the Shopfloor. In this sense, there may be several IIoT developments supporting a specific task within a company. We may also find the term "*Industry*" being applied in different economic sectors such as energy, health, transportation, and manufacturing. Similarly, we hear about smart grids, e-health, smart transportation, and smart manufacturing respectively, where the term smart alludes to the result of applying a digital transformation of processes [17]. In this section, for explanatory purposes, we will refer only to the smart manufacturing sector to contrast our proposed IoT reference model with.

4.3.1 Smart Manufacturing

In this context, [6] elaborates on an automation pyramid for manufacturing processes. The pyramid is made up of six levels. The top levels embrace activities related to the Enterprise Resource Planning (ERP) strategy; followed by the Manufacturing Execution System (MES). At the middle level are the HMI and Supervisory Control and Data Acquisition (SCADA) and Programmable Logic Controller (PLC) systems. The base of the pyramid relates to field devices such as sensors, actuators, and Radio Frequency Identification (RFID) readers. [17] presents a comprehensive ecosystem that may cover the most needs in smart manufacturing environments. The building blocks of this ecosystem overlap with the pyramid elements mentioned above, but elaborate on concepts such as Machine Learning, Digital Twins, Blockchain, Predictive Quality Management, Autonomous Transport Units, and Sustainability.

4.3.2 Use Case: Autonomous Mobile Robots

To evaluate our generic model, we selected the use case of Autonomous Mobile Robots (AMRs) being employed to transport heavy parts between work stations in an assembly line. The AMRs are mobile units in a fleet management strategy inside the factory. They are equipped with proximity sensors (Device Layer), and communicate their position and status in real-time to anchor points located at strategic positions (Internet Access and Management Layer), the fleet manager software may react based on this information and external events, modifying the route that the AMRs follow (Application and Middleware Layer). Software updates and security measurements may be communicated as needed to the AMRs (Security and Management Layer). This simple, but contemporary example shows how a "*Thing*" – the robot – equipped with sensor and communication capabilities supports a business process to contribute to the business efficiency.

4.3.3 Specification with Our Proposed IoT Reference Model

In this section, we relate the activities described above to the corresponding layers in our proposed reference model.

- **Device Layer:** Here we find the elements of the AMR that help in the navigation task. These are the proximity sensors, usually a combination of Simultaneous Localization and Mapping (SLAM) navigation, Light Detection and Ranging (LiDAR) and Quick-Response Code (QR Code) technology.
- **Internet Access Layer:** Here we are concerned with the elements of the IoT solution that help the system determine the real-time location of the AMRs on the shopfloor. The AMRs communicate their current position and status via anchor points. To achieve high precision, this location is usually based on Ultra-Wideband (UWB) communication.
- **Middleware Layer:** The fleet management software, with its orchestration capability among heterogeneous AMRs supports the final IoT application and therefore may be assigned to the Middleware Layer. The continuous access to relevant operative variables such as material flow, external orders and AMR location information, which may need to be processed in cloud, edge or fog also concern this layer.
- **Application Layer:** The fleet management software with its route updates is at the top of this particular IoT use case, therefore it is assigned to this layer. Its tasks is to update in real time the route information that the AMRs need to follow.
- **Security Layer:** It is paramount to secure all possible aspects of the scenario under evaluation. A production line usually has to comply with strict quality and safety standards. Improperly securing the different elements and processes that form the IoT support will introduce a very high risk in the production line that may have serious consequences.
- **Management layer:** The supervision task of the float by the fleet management software is assigned to this layer. This software oversees the status of the AMRs and

the other elements necessary to enable its functionality. The real-time predictive analytic activities concern this layer, too.

4.4 Applicability of the Introduced Reference Model

The three application examples showed that our simplified reference model can comprehensively describe each of them. It is very flexible and generic without oversimplifying relevant aspects. Admittedly, we concentrated on the technical features and contexts and thus somewhat disregarded the business aspects.

5 Conclusion

This paper introduces a generic IoT reference model comprising all the layers and functionalities required to describe different IoT use cases. Based on several published and even standardized IoT reference models, we concentrated on the relevant features for modeling IoT systems, stripping off the parts related to business aspects, to life cycles, and to value streams. If these aspects should be considered, more complex reference models like RAMI 4.0 or IIRA should be used. Our model is appropriate for describing the different components of an IoT system and how these components communicate and interact with each other. The model was specifically developed to be used in study courses on the Internet of Things (IoT).

In the future, we will apply this model to more and different IoT use cases to prove its validity and to refine it. Furthermore, several PhD students in our group will use this model in their work and thereby extend it and make it more precise.

Abbreviations

6LoWPAN-SNMP Simple Network Management Protocol for IPv6-enabled Low-power Wireless Personal Area Network

AI Artificial Intelligence

AMR Autonomous Mobile Robot

API Application Programming Interface

CoAP Constrained Application Protocol

CoMI CoAP Management Interface

CoRE Constrained RESTful Environment

CRC Cyclic Redundancy Check

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

EMS Energy Management System

ERP Enterprise Resource Planning

FC Fundamental Characteristics

FCAPS Fault, Configuration, Accounting, Performance, and Security management

FHIR Fast Healthcare Interoperability Resources

GPS Global Positioning System

HLR High Level Requirements

HMI Human-Machine-Interface

HTTP HyperText Transfer Protocol

IEC International Electrotechnical Commission

IIC Industrial Internet Consortium

IIoT Industrial Internet of Things

IIRA Industrial Internet Reference Architecture

IoT Internet of Things

IP Internet Protocol

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

JSON JavaScript Object Notation

KPI Key Performance Indicator

LiDAR Light Detection and Ranging

LoRaWAN Long Range Wide Area Network

LwM2M Lightweight Machine to Machine Protocol

MES Manufacturing Execution System

MQTT Message Queueing Telemetry Transport

NB-IoT NarrowBand Internet of Things

NETCONF Network Configuration Protocol

OAuth2 Open Authorization, Version 2

PLC Programmable Logic Controller

QR Code Quick-Response Code

RAMI 4.0 Reference Architectural Model for Industry 4.0

RFID Radio Frequency Identification

SCADA Supervisory Control and Data Acquisition

SDN Software-Defined Networking

SHEMS Smart Home Energy Management System

SLAM Simultaneous Localization and Mapping

TLS Transport Layer Security

TMN Telecommunications Management Network

UWB Ultra-Wideband

WPA3 Wi-Fi Protected Access version 3

WSDL Web Services Description Language

XML eXtensible Markup Language

XMPP eXtensible Messaging and Presence Protocol

References

[1] Aboubakar M, Kellil M, Roux P (2022) A Review of IoT Network Management: Current Status and Perspectives. Journal of King Saud University – Computer and Information Sciences 34(7):4163–4176. https://doi.org/https://doi.org/10.1016/j.jksuci.2021.03.006

[2] Al-Fuqaha A, Guizani M, Mohammadi M, et al (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials 17(4):2347–2376

[3] Al-Fuqaha A, Guizani M, Mohammadi M, et al (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials 17(4):2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[4] Alhamedi AH, Snasel V, Aldosari HM, et al (2014) Internet of Things Communication Reference Model. In: 6th International Conference on Computational Aspects of Social Networks. IEEE, pp 61–66, https://doi.org/10.1109/cason.2014.6920423

[5] Aliero MS, Qureshi KN, Pasha MF, et al (2021) Smart home energy management systems in internet of things networks for green cities demands and services. Environmental Technology & Innovation 22:101443

[6] Armin R (2016) Industrie 4.0 Einführung und Umsetzung von Industrie 4.0 - Grundlagen, Vorgehensmodell und Use Cases ausder Praxis. Springer Gabler, Berlin Heidelberg, https://doi.org/10.1007/978-3-662-48504-7, URL https://doi.org/10.1007/978-3-662-48504-7

[7] Bauer M, Bui N, De Loof J, et al (2013) IoT Reference Model. In: Bassi A, Bauer M, Fiedler M, et al (eds) Enabling Things to Talk. Springer, Berlin; Heidelberg, chap 7, p 113–162, https://doi.org/10.1007/978-3-642-40403-0_7

[8] Delicato FC, Pires PF, Batista T (2013) Middleware Solutions for the Internet of Things. Springer Briefs in Computer Science, Springer, London, https://doi.org/ https://doi.org/10.1007/978-1-4471-5481-5

[9] DIN Deutsches Institut für Normung e. V. (2016) Reference Architecture Model Industrie 4.0 (RAMI 4.0). DIN SPEC 91345, Deutsches Institut für Normung e. V., Berlin, Germany, URL https://www.dinmedia.de/de/technische-regel/

din-spec-91345/250940128

[10] Ersue M, Romascanu D, Schönwälder J, et al (2015) Management of Networks with Constrained Devices: Problem Statement and Requirements. RFC 7547, https://doi.org/10.17487/RFC7547, URL https://www.rfc-editor.org/info/rfc7547

[11] European Union (2024) The Cyber Resilience Act. Regulation (EU) 2024/2847, European Union, URL https://www.cyberresilienceact.eu/regulation.html

[12] Ferry N, Nguyen PH (2019) Towards Model-Based Continuous Deployment of Secure IoT Systems. In: ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C). IEEE, https://doi.org/10.1109/models-c.2019.00093

[13] Gaikwad PP, Gabhane JP, Golait SS (2015) A survey based on smart homes system using internet-of-things. In: 2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp 0330–0335, https://doi.org/10.1109/ICCPEIC.2015.7259486

[14] gematik GmbH (2025) epa für alle. Website, gematik GmbH, URL https://www.gematik.de/anwendungen/epa-fuer-alle, last access: 19.11.2025

[15] Griet K, Ediga P, S. A, et al (2024) Smart energy management: real-time prediction and optimization for iot-enabled smart homes. Cogent Engineering 11(1):2390674. https://doi.org/10.1080/23311916.2024.2390674

[16] HL7 International (2023) Fhir release. Trial use 5.0.0, Health Level 7 (HL7), URL https://hl7.org/fhir/directory.html, last access: 19.11.2025

[17] Huber W (2024) Industrie 4.0 kompakt – wie Technologien unsere Wirtschaft und unsere Unternehmen verändern: Transformation und Veränderung des gesamten Unternehmens, 2nd edn. Springer Vieweg, Wiesbaden, https://doi.org/10.1007/978-3-658-44783-0, URL https://doi.org/10.1007/978-3-658-44783-0

[18] Industry IoT Consortium (2022) Industrial internet reference architecture, version 1.10. Tech. rep., Industry IoT Consortium, URL https://www.iiconsortium.org/wp-content/uploads/sites/2/2022/11/IIRA-v1.10.pdf, foundational document

[19] International Electrotechnical Commission (2003) Enterprise-Control System Integration -– Part 1: Models and Terminology. International Standard IEC 62264-1:2003(E), IEC/ISO, URL https://cdn.standards.iteh.ai/samples/35480/106d6c212cc9472bbc89d6a1450ffd7d/IEC-62264-1-2003.pdf, first edition

[20] ITU-T (1997) Information Technology – Open Systems Interconnection – Systems Management Overview. Recommendation X.701, International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

[21] ITU-T (2000) Principles for a Telecommunication Management Network. Recommendation M.3010, International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

[22] ITU-T (2000) TMN Management Functions. Recommendation M.3400, International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)

[23] ITU-T (2012) Overview of the Internet of Things. Recommendation Y.2060, International Telecommunication Union – Telecommunication Standardization Sector (ITU-T), URL https://www.itu.int/rec/T-REC-Y.2060-201206-I, accessed: 2025-08-13

[24] Johnson M, Mohan BC (2020) A Review on Routing in Internet of Things. Wireless Personal Communications 111(1):209–233. https://doi.org/10.1007/s11277-019-06853-6

[25] N AM, N K, G SK, et al (2025) Iot-based smart home energy management system (shems) using networking and automation. 2025 International Conference on Data Science and Business Systems (ICDSBS) pp 1–8. URL https://api.semanticscholar.org/CorpusID:279454267

[26] Ojo MO, Giordano S, Procissi G, et al (2018) A Review of Low-End, Middle-End, and High-End Iot Devices. IEEE Access 6:70528–70554. https://doi.org/10.1109/ACCESS.2018.2879615

[27] Punia A, Gupta D, Jaiswal S (2017) A Perspective on Available Security Techniques in IoT. In: 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, pp 1553–1559, https://doi.org/10.1109/rteict.2017.8256859

[28] Razzaque MA, Milojevic-Jevric M, Palade A, et al (2015) Middleware for internet of things: a survey. IEEE Internet of Things Journal 3(1):70–95

[29] Resner D, Medeiros de Araujo G, Fröhlich AA (2018) Design and Implementation of a Cross-layer IoT Protocol. Science of Computer Programming 165:24–37. https://doi.org/https://doi.org/10.1016/j.scico.2017.08.008, special issue on VI Brazilian Symposium on Computing Systems Engineering

[30] Sapel P, Hopmann C (2023) Towards an ontology-based dictionary for production planning and control in the domain of injection molding as a basis for standardized asset administration shells. Journal of Industrial Information Integration 35:100488. https://doi.org/10.1016/j.jii.2023.100488

[31] Sinche S, Raposo D, Armando N, et al (2020) A survey of iot management protocols and frameworks. IEEE Communications Surveys & Tutorials 22(2):1168–1190. https://doi.org/10.1109/COMST.2019.2943087

[32] Sisinni E, Saifullah A, Han S, et al (2018) Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics 14(11):4724–4734. https://doi.org/10.1109/TII.2018.2852491

[33] Tomlinson M, Tjhai CJ, Ambroze MA, et al (2017) Error-correction Coding and Decoding. Springer, Cham, https://doi.org/https://doi.org/10.1007/978-3-319-51103-0

[34] Wang A, Mohaisen A, Chen S (2019) XLF: A Cross-layer Framework to Secure the Internet of Things (IoT). In: IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, pp 1830–1839, https://doi.org/10.1109/icdcs.2019.00181

[35] Weiser M (1991) The Computer for the 21st Century. Scientific American 265(3):94–104. URL https://www.jstor.org/stable/24938718

[36] Yemini Y (1993) The OSI Network Management Model. IEEE Communications Magazine 31(5):20–29. https://doi.org/10.1109/35.212418

Declarations

Ethics, Consent to Participate, and Consent to Publish declarations: not applicable

Funding: not applicable

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.