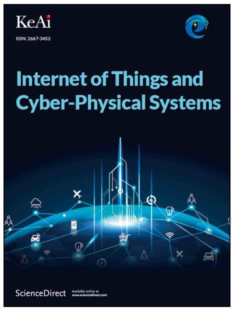
Journal Pre-proof



IoT: Communication protocols and security threats

Apostolos Gerodimos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, Ioanna Kantzavelou

PII: S2667-3452(22)00029-3

DOI: https://doi.org/10.1016/j.iotcps.2022.12.003

Reference: IOTCPS 27

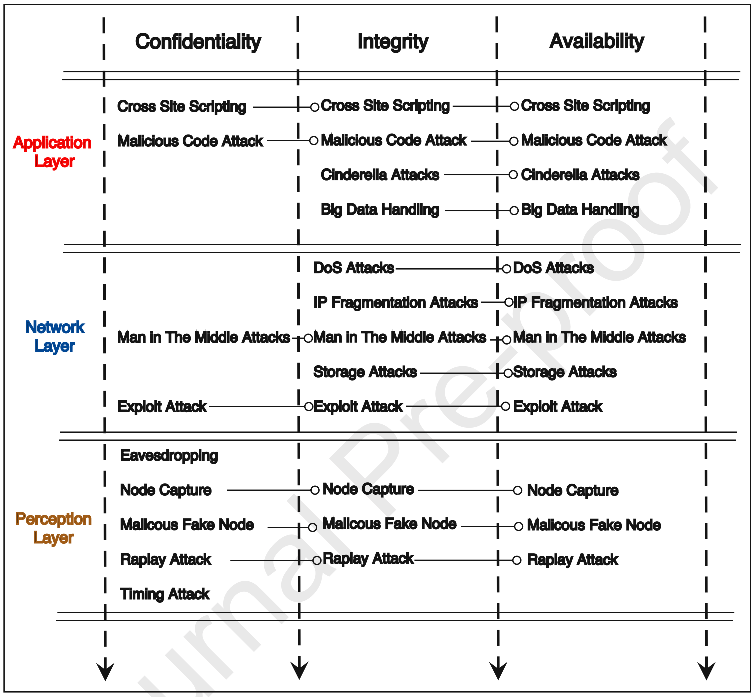
To appear in: *Internet of Things and Cyber–Physical Systems*

Received Date: 21 November 2022

Revised Date: 23 December 2022

Accepted Date: 25 December 2022

Please cite this article as: A. Gerodimos, L. Maglaras, M.A. Ferrag, N. Ayres, I. Kantzavelou, IoT: Communication protocols and security threats, *Internet of Things and Cyber–Physical Systems* (2023), doi: https://doi.org/10.1016/j.iotcps.2022.12.003.



Examines and describes a generic IoT architecture;

Presents the main communication protocols that are used in the application, transport, network and physical layer;

Identifies and describes current security threats in IoT;

Examines current challenges and discusses possible solutions and future directions.

IoT: Communication Protocols and Security Threats

Apostolos Gerodimos[a], Leandros Maglaras[b], Mohamed Amine Ferrag[c], Nick Ayres[d], Ioanna Kantzavelou[e]

[a]*School of Computer Science and Informatics, University of Thessaly, Lamia, Greece*
[b]*School of Computing at Edinburgh Napier University, Edinburgh, UK*
[c]*Technology Innovation Institute, Abu Dhabi, UAE*
[d]*School of Computer Science and Informatics, De Montfort University, Leicester, UK*
[e]*School of Engineering, Dept.of Informatics and Computer Engineering, University of West Attica, Athens, Greece*

Abstract

In this study, we review the fundamentals of IoT architecture and we thoroughly present the communication protocols that have been invented especially for IoT technology. Moreover, we analyze security threats, and general implementation problems, presenting several sectors that can benefit the most from IoT development. Discussion over the findings of this review reveals open issues and challenges and specifies the next steps required to expand and support IoT systems in a secure framework.

Keywords: IoT, Security, Protocols, Threats.

1. Introduction

Few decades earlier, the Internet revolutionized our world by connecting users across the globe simultaneously in real-time. Today, the Internet of Things, which is also known as the Internet of Everything or sometimes referred to as the Industrial Internet, is a paradigm of technology envisaged as a network, connecting machines, and devices globally and making them capable of interacting both with each other and the physical world autonomously within the existing Internet infrastructure.

By the term The Internet of Things, abbreviated to IoT, we refer to the innumerable tangible devices around the globe that can be connected to the internet. All of these devices collect and share data with each other while, simultaneously, eliminating the need for human-to-human or even human-to-computer communication. Thanks to the advent of computer chips at a remarkably low cost, the fact that wireless networks seem to be ubiquitous, and in addition, the advance of numerous technologies like machine – learning, big data analysis, smart sensors, and especially 5G, it has become plausible to convert anything, regardless of its size, to a part of the IoT, since the technology can be applied to anything, as minuscule as a pill, or even as huge as a tanker ship. Rayes and Salam (2017).

Although plenty of devices can connect to the Internet, we define IoT devices as those that would not normally be supposed to have Internet access, such as home appliances, health-monitoring devices, or any kind of equipment and that, at the same time, have the ability to interact with each other without human involvement. Subsequently, neither a laptop nor a smartphone is considered IoT devices, regardless of the fact that both carry sensors and communicate over the Internet. However, wearables, like smartwatches or fitness trackers could be regarded as ones. Nevertheless, it is possible for a PC or a smartphone to interact with an IoT network Lee and Lee (2015); Ferrag et al. (2019).

Connecting all these different objects, which are uniquely identifiable, and attaching sensors, transforms them into digitally intelligent devices, an attribute they would otherwise not possess. As a result, they are capable of communicating data in real-time, subsequently improving their efficiency, and accuracy and making the environment surrounding us more clever and quick to respond, accomplishing the fusion of the digital and the physical world. Khan et al. (2020).

This notion has multiplied the areas where it could be applied, which in turn, can improve the common welfare by making use of the means already available in ways never thought of before and it is considered to be one of the most crucial fields of future technology that is becoming popular with an extensive number of industries Wang et al. (2021). Except for efficiency and accuracy, the interconnection of IoT devices opens a number of security threats Ferrag et al. (2020a) to the users that can be connected to critical systems Maglaras et al. (2019). The authors in Mukherjee et al. (2020) have identified the major attacks on fog-based Internet of Things (IoT) applications.

The IoT technology forecast of connected devices is expected to increase by about 300% from 8.7 billion devices in 2020 to more than 25 billion IoT devices in 2030. In 2020, China was leading the IoT applications race with more than 3 billion devices in operation. The prevailing IoT devices are present in each industrial field and retail market. In particular, the retail market comprises around 60 percent of the total number of IoT devices in 2020. This allocation is predicted to remain unaltered in the next ten years. Al-Sarawi et al. (2020).

Security concerns must be prioritized in order to minimize the attack surface and prevent security issues, since IoT technology is intended to be used in numerous critical sectors, particularly the economy and national security, with varying industry standards and specifications. In addition to cyberattacks, the creation of large-scale heterogeneous networks made up of constrained nodes working in real-time should be based on an architecture that can handle factors like reliability Maglaras et al. (2022b), quality of service, modularity, semantic interoperability, privacy management, and compatibility between hardware and software. This article presents a generic IoT architecture, the communication protocols used in an IoT environment and the main threats against availability, integrity and confidentiality. These findings may help developers of Internet of Things (IoT) applications create secure IoT applications that protect their users and make it easier to deploy IoT applications.

The selection of the relevant literature for analysis in this article was based on a keyword search, namely, “IoT Architecture”, “IoT Communication Protocols”, “IoT Security Issues and Concerns”, and “IoT Applications”. Through searches of these specific keywords in various scientific repositories such as IEEE, Springer, Wiley, ACM, Web of Science, and Scopus, the first set of potentially relevant research sources were identified. The search procedure generated a considerable number of findings. In the first step, only the proposed security systems for IoT were selected for the collection. Then, each source collected was ranked based on the following metrics: 1) Reputation, 2) Suitability, 3) Importance of the source, 4) Publication date (between 2015 and 2022), and 5) Highly impactful articles in the field. The higher the global rating, the more the source has been classified in our list. Through the use of this scoring structure, we were able to prioritize the sources.

The contributions and novelty of this article are:

- Examines and describes a generic IoT architecture;
- Presents the main communication protocols that are used in the application, transport, network and physical layer;
- Identifies and describes current security threats in IoT;

- Examines current challenges and discusses possible solutions and future directions;

The rest of this paper is organized as follows: In section 2, we present the related surveys on the security of the IoT application In Section 3 we present the generic architecture of IoT and in Section 4 we give an overview of the communication protocols used. Section 5 discusses security issues and concerns and gives a thorough understanding of IoT security threats. In Section 6 we present the main IoT applications. In Section 7 we discuss open security issues and challenges. Finally, Section 8 collects and discusses all the conclusions we draw from the presented research work.

Study	IoT Architecture	Communication Protocols	Security Issues and Concerns	IoT Applications	Challenges
Alaba et al. (2017)	Partial	Partial	Yes	Partial	Yes
Ferrag et al. (2017)	No	No	Yes	Partial	Partial
Frustaci et al. (2017)	Yes	Partial	Partial	Partial	Yes
Vashi et al. (2017)	Partial	Partial	Partial	Partial	Partial
Ammar et al. (2018)	Partial	Partial	Yes	Partial	Yes
Hassija et al. (2019)	Partial	Partial	Yes	Partial	Yes
Chaabouni et al. (2019)	Partial	No	Partial	No	Partial
Ferrag et al. (2020b)	Yes	Partial	Partial	Partial	Partial
Da Xu et al. (2021)	Partial	Partial	Partial	No	Partial
Yang et al. (2022)	No	No	Partial	No	No
Derhab et al. (2022)	Yes	Partial	Yes	No	Yes
Our study	Yes	Yes	Yes	Yes	Yes

Table 1: Related Studies on Security of the Internet of Things Application

2. Related Surveys

Table 1 presents the related studies on security of IoT application. Alaba et al. (2017) concentrated on the advanced IoT security vulnerabilities and threats by performing an in-depth review of the existing research in the field of IoT safety. The research provides a comprehensive overview of the current security threats in the communication, architecture, and application contexts. This research also provides a comparison of potential security challenges in the IoT. In addition, the study provides a discussion of the current IoT based security environment as well as an overview of the potential threats. The remaining ongoing research problems and the security deployment challenges in IoT safety are also provided. Frustaci et al. (2017)

provided a taxonomy review from the view of the three major layers of importance in the IoT system framework: 1) application levels; 2) transport; and 3) perception. Vashi et al. (2017) gives an overview of the architecture of IoT with the help of Smart World. In the second phase of this paper, the authors discuss the security challenges in IoT followed by the security measures in IoT. Finally, these challenges, which are discussed in the paper, could be research direction for future work in security for IoT.

A comprehensive study of authentication technologies for IoT application is presented by Ferrag et al. (2017). In particular, more than forty authentication protocols implemented or deployed in the IoT environment are identified and reviewed in depth. The protocols are classified according to the specific IoT target setting: Internet of Sensors (IoS), Internet of Energy (IoE), Internet of Vehicles, and Machine to Machine Communications (M2M). In addition, this paper presents formal security verification techniques, countermeasures, and threat models used in authentication protocols for the IoT. Therefore, Ammar et al. (2018) studied the reliability of the major IoT platforms, a total of 8 platforms are reviewed. In each platform, they provide details on the proposed infrastructure, the essential elements of third-party smart application development, the supported equipment, and the required security functionalities. The comparison of the safety and security algorithms demonstrates that the identical norms are employed to ensure the security of the connectivity, while various specific methods are used to provide other safety and security characteristics of the IoT frameworks.

Hassija et al. (2019) presented a comprehensive overview of security issues and threat sources in IoT implementations. Following the discussions of security concerns, a variety of existing and newly available strategies that focus on obtaining a high level of reliability in IoT applications are reviewed and discussed. There are four various new technologies, namely, machine learning, edge computing, fog computing, and blockchain, to enhance the degree of trust in the IoT are described. Chaabouni et al. (2019) categorized the threats and IoT-related security issues for the IoT-enabled networks by reviewing the current defense mechanisms available. The study concentrates primarily on surveys of existing network intrusion detection systems deployment utilities and datasets as well as open and free software for network detection. In addition, it studies, discusses, and evaluates state-of-the-art network intrusion detection systems propositions in the IoT environment in its aspects of architecture, deployment detection methods, verification approaches, threats addressed, and deployment of algorithms.

Ferrag et al. (2020b) introduced the security and privacy research challenges in IoT-based green agriculture. The study begins by providing a four-level description of an IoT-based green agriculture architecture and summarizes available research surveys that address intelligent agriculture. Next, it proposes a categorization of attack models targeting IoT-based green agriculture into five types, including attacks against integrity, availability, confidentiality, authentication, and privacy properties. In addition, the study provides a side-by-side comparison and classification of state-of-the-art approaches to securing and maintaining privacy for IoT technologies. Da Xu et al. (2021) proposed a review paper that comprehensively investigates the current state of the art of blockchain-based IoT security, with a particular focus on the security functionalities, challenges, techniques, applications, and scenarios associated with blockchain-integrated IoT. The importance of blockchain and IoT integration and interoperability are presented.

Yang et al. (2022) presented a survey of physical safety and security of IoT devices to focus on emerging technology research opportunities in this field. Then, they provide a discussion of topics such as anti-theft and anti-vandalism designs as well as the design of hardware and software systems, supplemental detection equipment, the use of biometrics and behavioral intelligence, and monitoring methods, among other aspects. In addition, they synthesize the solutions of artificial intelligence for the safety and physical security of IoT devices. Derhab et al. (2022) provided a very detailed and complete internet of drones cybersecurity and physical security survey. Unlike many investigations that provide a classification of attacks/threats only, the authors also proposed three taxonomies that are associated with (1) countermeasures, (2) attacks, and (3) drone assets.

These available studies are either restricted in coverage or only provide partial coverage of the countermeasures for IoT security. To overcome these limitations, in this paper, we review the fundamentals of IoT with a general approach, by addressing the problems of standard architecture, vulnerabilities, and use cases of this promising technology.

3. A Generic IoT Architecture

In theory, the term IoT is commonly used to describe the design and implementation of a network that is successfully handling information data within the devices included in it. In practice though, since this network is the Internet, this is something challenging because all of the devices (Smart Sensors, Data Centers, etc.) that are participating must be able to communicate seamlessly with each other, either directly or indirectly (i.e. Gateways), in a secure way. As a result, making all the devices of the Internet compatible is something that requires specific protocols for communication, standard structure, application compatibility, advanced Data Processing capabilities, and many more. Despite their complexity in certain implementations, their elementary operation is quite simple Chaudhary et al. (2017).

A smart object transmits data collected by its sensors (physical world) to a data center, (either local or cloud-based), or even another smart object through an intermediate (gateway). The use of the gateway is not mandatory as the smart object can potentially work as a gateway too. Then, the data received "on the other side" are handled and multiple actions can be initiated. These actions are the ones that add complexity to the implementation because more interoperability is required to control or monitor an autonomous car, such as to turn on the heater at certain degrees.

Although the IoT technology applies to a vastly major number of fields and is not standardized in any way, we will address a simple approach by reviewing the basic architecture and the most common protocols invented for this technology Serpanos and Wolf (2018).

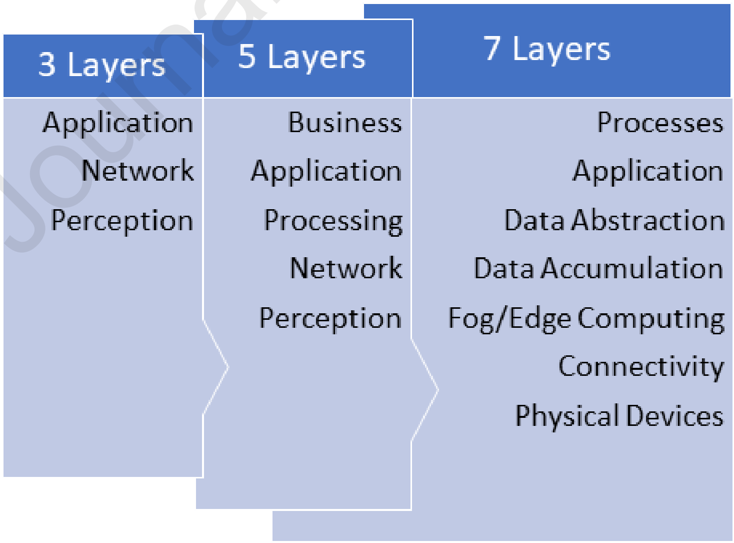


Figure 1: Elementary IoT Structure

To define a reference architecture that supports current features and future extensions scalability, interoperability, data distribution, computing power, and of course security, some fundamental factors must be considered regarding the architectural standardization, since several model architectures are described in the literature Gupta and Quamara (2020).

For example, in a systematic review of the Internet of Things architecture, examining more than 145 studies and their underlined architectures, we noticed that architectures in reference were mainly three-layer, four-layer or five-layer models, while in another survey the layer classification was applied in three-, four-, five-, six- or seven-layer models Santos et al. (2020) (See Figure 1).

To make things more complicated, international organizations and big tech companies, like the International Telecommunication Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), Cisco, Google, Amazon, and the European Telecommunications Standards Institute (ETSI), have presented different IoT frameworks based on application requirements, network topology, protocols, business, and service models, as it encompasses a variety of technologies. Pierleoni et al. (2019).

Since there's still no single standard reference architecture for IoT and not an easy blackprint that can be followed for all possible implementations, in our approach we chose the 3-layer model that consists of the Perception, Network/Transmission, and Application Layer, in which the layers, in any case, cannot be considered as sub-layers and can fully describe the elementary operations of an IoT implementation Lombardi et al. (2021).

3.1. Perception Layer

The Perception or Physical Layer consists of the physical devices, which are the cornerstone of IoT technology, whose purpose is to collect information, transform them into digital data and pass them to another layer so that actions can be done based on that information. Acting as a medium between the digital and real world, these physical devices can be Sensors (Temperature, Humidity, Light, etc.), Actuators (Electric, Mechanical, Hydraulic, etc.), RFID (RFID tags), Sparavigna (2008), Video Trackers (IP camera) or anything that can use data to interact with different devices through a network.

The difference between the traditional sensors and the smart sensors used in IoT however is that smart sensors include an integrated microprocessor (DMP), that can process the digitized data captured by the sensor. These data can be normalized, noise filtered, or transformed for the sake of signal conditioning before being forwarded to other devices throughout the network.

3.2. Transmission Layer

The Transmission Layer which can also be found in the literature as a Transportation or Network layer, is located between the perception and the application layer. In this layer, the data collected by smart sensors are transformed and forwarded to the Application Layer using suitable communication channels and protocols for further processing, like analysis, data mining, data aggregation, and data encoding, while providing network management functionality and not only a basic packet routing as the network layer of the ISO/OSI model does.

In IoT implementations, wireless protocols are more commonly used compared to wired ones, since wireless sensors can be installed even in places that lack the main requisites for wired sensors like power, communication cabling, etc. Moreover, in a wireless sensor network, it is easier for nodes to be added, removed, or relocated without reconsidering the structure of the entire network. The selection of protocols to be used can be based on several factors like hardware heterogeneity, power consumption, transmission speed, and the transmission distance needed in each application many others.

In other implementations, however, a wired sensor network is preferred since these networks are more reliable, more secure, and offer higher transmission data speeds. For example, in IoT implementations in a hospital, where reliability and speed are major factors for saving a patient's life, wired sensors are preferable and the requisites for their installation can be planned during the hospital's initial design (wiring, power delivery cables, etc.).

In general, smart sensors must be able to communicate with each other through the Internet to handle information and interact with the physical world, while being uniquely identified to prevent data conflicts. Depending on the specific applications, smart objects can be directly reachable without the need of an intermediary gateway, implement a UI making user interaction possible and many more.

3.3. Application layer

The Application Layer is present just above the Transmission Layer, it is based on the implementation, and can be organized in different ways. This layer, depending on the implementation, is responsible for analyzing and processing the information data that came from the below Layers (Perception and Transmission). More specifically, it handles these data to applications in order to be used for the desired actions (i.e., control actuators), acting like a bridge to transform and forward it to other nodes or hand it over to another application for further processing.

Moreover, this is the layer where the user interface is placed (if any), giving the choice of users to interact with the IoT system and perform various actions (for example if a piece of technical equipment needs servicing, the IoT will inform the technician through an interface that "structurally" is operating on the Application layer.

The Application layer, in contrast with the Transmission and Perception Layer, can vary a lot based on the implementation. Since it is designed with the desired application in mind, this layer is formed by its functionalities. For example, real-time monitoring and decision-making applications are in charge of taking actions based on the data collected from the perception layer, information digitization is responsible for collecting and transforming analog data into digital, analytics are used to process collected data and create an evaluation model, while hardware control for transforming data into physical actions Setetemela et al. (2019).

4. Communication Protocols

Many protocols contribute to an IoT implementation, but communication protocols are mandatory for IoT networks. Choosing the best IoT protocol means accurately weighing the criteria of desired application range, power consumption threshold, information bandwidth, and latency, and Quality of Service, all viewed through the prism of security. As mentioned earlier, IoT devices use network standards and protocols to enable communication between physical objects connected through the cloud. Network protocols and standards are policies that comprise certain rules that define the communication language between different network devices.

Every device generally is connected to the internet by using the Internet protocol (IP) but can also be connected locally via blacktooth, NFC (near-field communication), and others. Some of the differences between both types of connections are power, range, and CPU power used. IP connections are complex and require increased power and memory, but there are no range limitations. blacktooth connections, on the other hand, are simple and require less power and memory, but the range is limited.

Single devices like smartphones and personal computers use network protocols for communication, however, general protocols used by these devices might not meet specific requirements like bandwidth, latency, and cover distance of IoT-based solutions. Although IoT devices are easy to deploy, their communication protocols are the ones that must bridge the lack of processing power, range, and reliability with existing internet infrastructure. Since the existing protocols are not meeting the criteria for IoT implementation (Wi-Fi 802.11 a/b/g/n/ac, etc.), we will review some new IoT protocols created for IoT application requirements.

Since power consumption is an important factor when designing IoT networks, low-power wireless network technologies are preferable. These technologies generally fall into two groups:

- Low Power Wide Area Networking (LPWAN) that provides an extended range up to several kilometers, but with limited data rates for most (e.g., 6LoWPAN, LoRaWAN, Sigfox, NB-IoT, Wi-Fi HaLowTM);
- Wireless Personal Area Networking (WPAN) technologies, with a range of up to 100 meters and data rates up to 250 kbps for Zigbee and up to 3 Mbit/s for blacktooth Low Energy.

4.1. LPWAN

LPWANs (Low Power Wide Area Networks) are a category of protocols developed for short-range communications. Although "traditional" cellular networks are capable in supporting wide-area communication networks, their drawbacks, like complex infrastructure (Antennas, Amplifiers, etc.) and high-power consumption requirements, are making them a less favored solution when considering IoT applications. On the other hand, LPWAN protocols are to be used by simple, low-power, low CPU capabilities, allowing the deployment of sensors without investing in gateways, which are based on inexpensive batteries that last, making it a more favorable option in contrast to cellular networks.

With a low-requirement hardware capability in mind, LPWAN technology can operate in more than 10 km distance depending on the surroundings and obstacles and data transfer rates from 0.3 kbit/s to 50 kbit/s per channel. Moreover, while power consumption and data rate are big challenges for LPWANs, Quality of Service (QoS) and scalability are important factors when selecting an LPWAN protocol. The 6LoWPAN protocol is an LPWAN protocol example, which combines IPv6 and LoWPAN technologies, and has many advantages, like exceptional connectivity, compatibility with earlier architectures, low-energy consumption, and ad-hoc self-organization.

4.2. WPAN

WPAN is a local mesh network of devices organized in a mesh topology, in which, every device is connected directly (without a gateway) with the other devices of the network and transfers data between each other until it reaches the final recipient inside this network. This structure promotes network resilience, is simple to implement, and costs less to set it up than other networks, particularly over large areas due to the absence of extra equipment (i.e., gateways).

ZigBee is considered the most popular mesh protocol used in IoT. It has a short-range but consumes minimal power, which can extend communication over several IoT devices. In comparison with LPWAN protocols, ZigBee can deliver high data transfer rates at a single instance, but with more power efficiency due to its mesh topology. However, due to their short physical range, ZigBee and every other mesh protocol are best suited for small to medium-range implementations, like smart home networks de Almeida et al. (2019).

Communication in IoT technologies covers both wired and wireless connections. Depending on the connection type, communication protocols, in a 4-layer network, are described per layer in the sequel.

4.3. Application Layer

Five different protocols are described below for the application layer; the MQTT, the CoAP, the REST, the XMPP, and the AMQP. Inherent security-related features and problems are also discussed.

4.3.1. MQTT

The Message Queuing Telemetry Transport (MQTT) protocol is a messaging protocol for publishing and subscribing that works on the very simple client/server model, and runs over TCP/IP or other protocols. It is more suitable for constrained environments, such as in IoT, because it is open, lightweight, and easily implementable. Security requirements that should be fulfilled in MQTT implementations are authentication, authorization, and secure communication. In critical infrastructures and applications with sensitive information, MQTT can work and offer advanced security services with the use of specific recommended features.

4.3.2. CoAP

The Constrained Application Protocol (CoAP) is defined as a specialized web transfer protocol in RFC 7252. It is a lightweight protocol, with low transmission rate, proposed for use with constrained nodes and constrained networks, and its name is designated by this. The design is appropriate for machine-to-machine (M2M) applications such as supply chain management and smart meters for tracking energy consumption. It can interface with HTTP very well, which facilitates integration with the Web. But the CoAP is not a secure protocol, and this is a serious disadvantage. Security is achieved with the Datagram Transport Layer Security (DTLS), defined in Rescorla and Modadugu (2012), which unfortunately has no wide use in IoT.

4.3.3. REST

The Representational State Transfer (REST) is a hybrid architectural style for distributed hypermedia systems introduced by Fielding in Fielding (2000). It includes a set of rules that describe the software engineering guiding principles to build an application with certain constraints. It is used for the construction of web services, also called RESTful. REST includes a) the client-server constraint, b) the stateless constraint, which achieves visibility, reliability, and scalability, c) the cache constraint, which improves network efficiency, d) a set of four constraints for a uniform interface between components, e) layered system constraints, and f) the code-on-demand optional constraint.

4.3.4. XMPP

The Extensible Messaging and Presence Protocol (XMPP) is an open XML technology for real-time communication. It is used for instant messaging, presence, and collaboration. Presence specifies that an entity is ready for messaging. Messaging uses an efficient push mechanism that ensures real-time capability. The open design of XMPP facilitates changes and allows its extensible feature, which complies with an IoT implementation. A significant number of CVE codes have been recently added in NVD databases maintained by NIST, related to known vulnerabilities of XMPP that permit a series of attacks to take place.

4.3.5. AMQP

The Advanced Message Queuing Protocol (AMQP) is an open standard suitable for business messaging between applications, which operates asynchronously across different organizations and platforms. It is a wire-level protocol that allows reliable business messaging. Some of the main characteristics included in AMQP's design aim at ensuring security, reliability, and interoperability. It was approved for release as an ISO and IEC International Standard in 2014 and it comprises of several layers. The lowest level is for transporting messages between two processes, and the messaging layer defines the standard encoding format every message should have.

4.4. Transport Layer

A considerable number of protocols are commonly used at the transport layer, as described in the following paragraphs.

4.4.1. TCP

The Transmission Control Protocol (TCP) is a connection-oriented reliable protocol that operates in three phases. It belongs to the internet protocol suite and it is widely used for connections between devices. The great packet overhead generated ranks it in the heavyweight protocols category, with large power consumption.

4.4.2. UDP

The User Datagram Protocol (UDP) is a connectionless lightweight protocol, which can be used when packet loss is acceptable during data transmission. It is preferable for communication in Wireless Sensor Networks, but is not reliable. It is not required to establish a connection before transferring data.

4.4.3. DCCP

The Datagram Congestion Control Protocol (DCCP) is a transport protocol for bidirectional unicast connections. It is used for applications such as streaming media and VoIP, where TCP is not able to control time delays and commit reliable in-order delivery. On the other hand, UDP applications are able to control delays, but DCCP has an embedded congestion control mechanism to avoid them.

4.4.4. SCTP

The Stream Control Transmission Protocol (SCTP) is a reliable transport protocol for PSTN signaling of messages transmitted over IP. It has been designed to resist masquerade attacks and to avoid flooding attacks.

4.4.5. RSVP

The Resource Reservation Protocol (RSVP) is a protocol for specific QoS requests applied by hosts and delivered by rooters to nodes in order to ensure and provide the requested service. The result is resource reservation along the data stream paths.

4.4.6. TLS

Transport Layer Security (TLS) is a protocol used over the internet to provide secure communication between client/server applications. The use of cryptographic algorithms prevents data interception, forgery and message alterations. Version 1.3 is valid since 2018.

4.4.7. DTLS

The Datagram Transport Layer Security (DTLS) is based on the TLS protocol, which cannot be directly used in datagram environments because of packet loss and packet reordering problems. Thus, the DTLS is the TLS with the required alterations that fix these problems and enhance reliability.

4.4.8. RPL

The RPL is an IPv6 Routing Protocol designed for Low-Power and Lossy Networks (LLNs), a class of networks with memory, processing power, and energy constraints. It uses the Destination Oriented Directed Acyclic Graph (DODAG) for data routing, and because it is based on the IPv6 standard it is preferable for IoT applications.

4.4.9. CARP

The Channel-Aware Routing Protocol (CARP) is a distributed cross-layer protocol developed for underwater Wireless Sensor Networks for multi-hop delivery of data to the sink.

4.4.10. CORPL

The Cognitive RPL (CORPL) is an extension of RPL protocol for cognitive networks, which also uses DODAG adapted properly to cognitive networks.

4.4.11. QUIC

The Quick UDP Internet Connections (QUIC) is a connection-oriented protocol between two endpoints that exchange UDP datagrams. It provides low-latency connections and ensures confidentiality, integrity, and availability by incorporating security measures. This makes QUIC as secure as the TLS protocol.

4.4.12. uIP

The uIP TCP/IP stack achieves communications using the TCP/IP protocol suite on very small micro-controllers, even 8-bit small. It is a very small implementation of TCP/IP stack, written as simply as possible in the C programming language. The code requires a few KB and the RAM is extremely limited. Its design includes a minimal set of features required by a complete TCP/IP stack and contains the IP, the ICMP, the UDP, and the TCP protocols. The peers of uIP can also run a lightweight stack.

4.4.13. Aeron

Aeron is a protocol stack designed for UDP unicast and UDP multicast and used for streaming data. It is different from two main features, high throughput and low latency.

4.4.14. CCN

The Content-Centric Networking (CNN) or Information-Centric Networking (ICN) introduces a novel paradigm for communications. According to this architecture, requests of named content replace packet sending. Two ICN architectures are Named Data Networking (NDN) and Content-Centric Networking (CCNx).

4.4.15. NanoIP

NanoIP is a protocol suite specifically designed for tiny devices, such as sensors and embedded devices. A transport called NanoIP supports reliable connections, and another one, the nanoUDP supports connectionless communications. None of these refer directly to standard TCP and UDP, they rather refer to the functional equivalents.

4.4.16. TSMP

The Time Synchronized Mesh Protocol is a protocol stack for WSNs. It was developed to meet the requirements of reliability, security, timely delivery, and low power.

4.5. Network Layer

Five network protocols are presented for the application layer; WiFi, blacktooth, ZigBee, Z-Wave, and LoRaWAN, and security-related features and problems are also discussed.

4.5.1. WiFi

WiFi is the most commonly used and well-known communication technology based on the Institute of Electrical and Electronics Engineers (IEEE) wireless communication standard 802.11. It is going through continuous improvements that make it faster, with less latency, and appropriate for several different devices. Depending on the WiFi generation, security is enhanced to meet the requirements of authentication data privacy, and availability, securing WIFi connections. Devices are wirelessly connected by sending signals within a range of 100 meters, but in reality, this is quite shorter.

4.5.2. blacktooth

blacktooth Low Energy (LE) radio is preferable for IoT implementation because it is designed to operate at very low power. It is able to transmit data over a large number of channels, offering the necessary openness to be implemented in multiple different communication topologies, from point-to-point to broadcast and to mesh topologies, and next to large-scale wireless device networks. In addition, it provides device positioning services with high accuracy. It is widely used because it is perfect for the most modern mobile devices, such as wearables and smartphones, which have been spread worldwide.

4.5.3. ZigBee

ZigBee is a protocol with analogous significant usage as blacktooth in IoT infrastructures. It covers advanced security requirements, with low power consumption, low data range, and up to 200 meters communication range, which is double long compared to the corresponding blacktooth. Suitable for sensors and devices with several constraints, it facilitates the construction of large IoT models with numerous of nodes.

4.5.4. Z-Wave

Z-Wave is a wireless protocol designed for home automation. It operates on its own radio frequency range, which mitigates interference problems.

4.5.5. LoRaWAN

LoRaWAN is a Low Power, Wide Area (LPWA) networking protocol used to wirelessly connect battery-based devices in IoT implementations. It meets significant requirements of bi-directional communication and end-to-end security de Carvalho Silva et al. (2017).

4.6. Physical Layer

The IEEE 802.15.4 is a protocol designed for the physical layer and the MAC layer that enables the communication between devices with power constraints and certain requirements to provide services through sensors. Low-cost and short-range communication are supported, and devices cooperate to facilitate multi-hop routing and achieve range extension. It includes descriptions for Low-Rate Wireless Personal Area Networks (LR-WPANs).

Figure 2 illustrates the communication protocols that are mostly used in IoT implementations in a 4-layer ISO architecture. In Table 2 the main advantages and disadvantages of the main protocols are highlighted.

5. Security Issues and Concerns

Since IoT technology is designed to apply in many sectors that are crucial, especially for national security and the economy with different industry standards and specifications, security issues require primary attention to minimize the attack surface and prevent security issues Jasim et al. (2021). For example, in 29 of April 2021, Microsoft's IoT security research group, discovered critical memory allocation vulnerabilities in IoT devices that could potentially be used to bypass security controls and execute malicious code or cause a system crash Ahamed and Rajan (2016).

Besides cyber-attacks, the development of large-scale heterogeneous networks of constrained nodes engaging in real-time should be based on an architecture that is resilient to manage factors arising from Reliability, QoS, Modularity, Semantic Interoperability, Privacy Management, Hardware and Software Compatibility. Based on the 3-layer protocol, we will discuss in the following issues and concerns that address the security threats of each layer.

The most valuable information can derive by looking at each attack type and the corresponding major impact on confidentiality, integrity, and availability. Figure 3 illustrates in a per-layer picture the attacks described above and connects them to show those that affect two or even three of the security attitudes we have to preserve. We distinguish the majority of attacks that

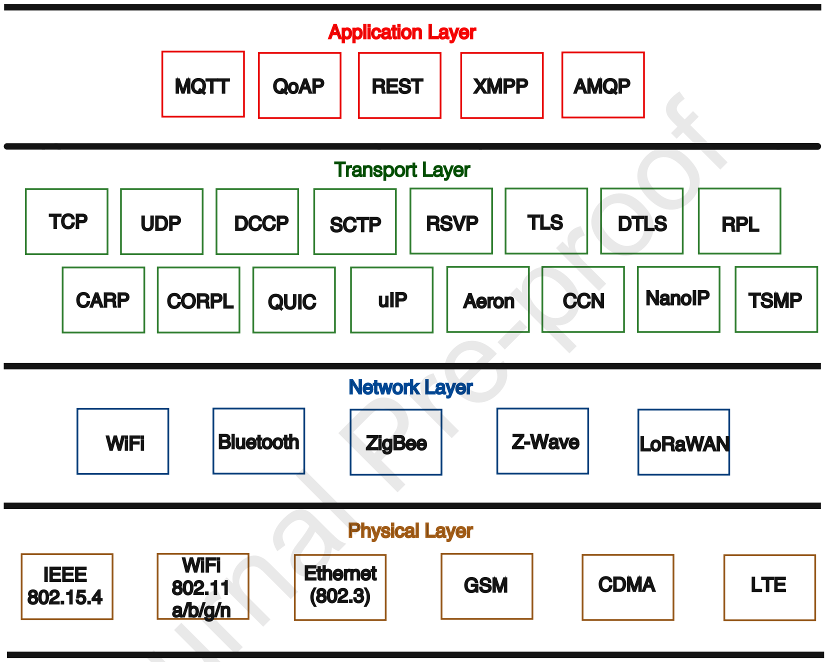


Figure 2: Communication Protocols for IoT in a 4-layer ISO architecture

have effects in all three security characteristics, a great number of them that affects only two, mainly the integrity and the availability, and only a few that have a serious impact on the confidentiality of data stored or transmitted. These findings might assist IoT developers to construct secure IoT implementations that would protect their users and facilitate IoT applications' deployment.

5.1. Perception Layer

The most important threats that endanger the Perception Layer have been selected and described in the sequel.

- Eavesdropping: IoT Devices are vulnerable to Eavesdropping Attacks because they lack the processing power for encryption techniques, in contrast to non-IoT network devices. Additionally, if the devices are operating in a remote location with minimum or no physical monitoring, eavesdropping attacks are easier to implement and more difficult to expose Aarika et al. (2020).

- Node Capture: Since there is a huge number of devices that can participate in an IoT network, the network's attack surface increases exponentially. An attacker can potentially gain control over a network's key node, such as a gateway, which in turn gives him access to all the information exchanged through the network Alohali et al. (2018).

- Malicious Fake Node: The IoT's advantage to easily creating a network can become a weakness. An adversary can always install a node to the network that inputs false data, an action could drain resources from the legitimate nodes, undermining the whole network's operation Pan and Yang (2018).

- Replay Attack: In the Replay Attack, an intruder eavesdrops on authentic information transferred over the communication line between the sender and a receiver and captures it. Then, he sends the same authenticated information to the victim that had already been received in his communication, by showing proof of her identity and authenticity. Since the message is encrypted, the receiver may treat it as a legitimate request and respond accordingly to the intruder Wara and Yu (2020).

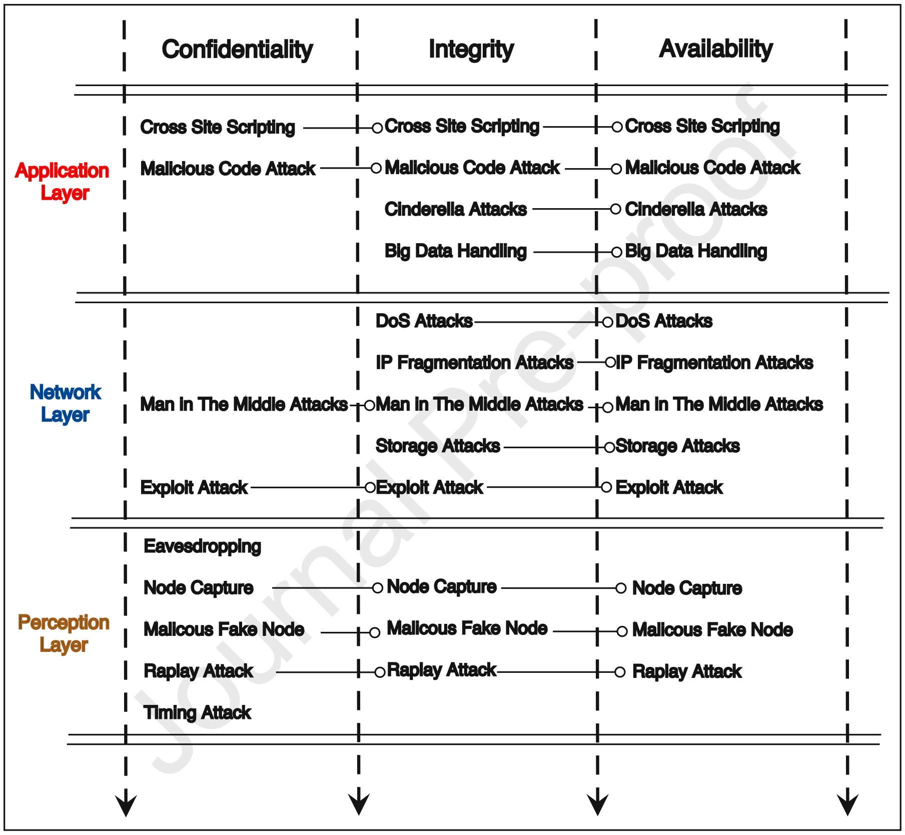


Figure 3: Attack Types that affect confidentiality, integrity, and availability in a 3-layer IoT architecture.

- Timing Attack: Timing Attack is more effective in devices with minimal computing capabilities. This attack enables an adversary to expose vulnerabilities and extract information maintained in the security of a system by timing how long it takes the system to respond to different queries, inputs, cryptographic algorithms, and others Takarabt et al. (2019).

Table 3 presents the attack types identified at the Perception Layer in IoT systems as the most significant. The targets of these attacks are the devices, a node, the whole network, or information transferred during an authentication procedure Alqarawi et al. (2022). The weaknesses of the devices, systems, or protocols that facilitate them are mainly located in the power limitations devices have, in inherent problematic issues in protocols or the IoT infrastructure and construction itself. The last column of the table proposes any countermeasures to prevent or detect such attacks, avoid the consequences and mitigate the damage spread.

5.2. Network Layer

The Network Layer is highly sensitive to attacks with security problems mainly to the integrity and availability of information exchanged throughout a network. Selected security threats of the Network Layer are summarized next.

- Denial of Service (DoS) Attacks: With a DoS attack, users are prevented from accessing devices or other network resources. This action is accomplished by flooding targeted devices or network resources with superfluous requests making it impossible or difficult for other users to communicate Salim et al. (2020).

- IP Fragmentation Attacks: It is a DoS category attack where the adversary exploits a network's Maximum Transmission Unit (MTU). When IP packets are reassembled after transmission, their size is larger than the maximum transmission unit the network can service, and therefore it collapses Salah and Amro (2022).

- Man in The Middle Attacks: In a MiTM attack, the attacker, while unobserved, intercepts and alters the communication data between two parties. Since they are both unaware of the interception, the attacker can control their communication, by changing messages according to his needs. It is considered a serious threat to the network's security because the attacker can capture and manipulate information in real-time, before being exposed Thankappan et al. (2022)

- Storage Attacks: Since all data is stored on storage devices (Locally or Cloud) they can be attacked by changing legitimate data to incorrect ones or even deleting them permanently. Therefore, if many groups of users have access to the storage, the more possible it is for these types of attacks even if the process is based on blockchain technology Dorri et al. (2022).

- Exploit Attacks: Exploit Attacks are attacks that take advantage of security vulnerabilities in applications, systems English et al. (2019), or hardware Zubair et al. (2019). Their goal is to gain partial or full control of a system and steal or alter the information stored. Although the system's admin can patch the security vulnerability, every single change in application or hardware can create new vulnerabilities for an attacker.

Table 4 presents the attack types identified at the Network Layer in IoT systems as the most significant. The targets of these attacks are the devices, the network resources, communication data, or data stored. The weaknesses are now located in the protocols, as well as in applications, or even the hardware. The last column of the table proposes some countermeasures to prevent or detect these attacks, and advance security.

5.3. Application Layer

The Application Layer is more prone to security issues compared to the other two layers, due to its diversity. The Application Layer consists of the applications and software built for IoT implementations and since these are countless, so are the applications built for them. For example, when IoT is used for Smart Home applications, the threats and vulnerabilities may come from every application with access to the hardware used either from the inside (control center or even our mobile app) or outside (remote applications).

Some of the most common security threats of the Application Layer in IoT are:

- Cross Site Scripting: In Cross Site Scripting attacks the adversary injects malicious code scripts, such as java scripts, in a trusted domain site viewed by many other users. With this action, the adversary can alter the contents of an application according to his purposes and use original information in a malicious way. Papaspirou et al. (2020).

- Malicious Code Attack: Every software is built with by code and so as malicious software. Either a Trojan, Virus, Worms, or Backdoors are malicious code intended to cause undesired effects to the system's operations Vignau et al. (2019). Usually, these types of attacks cannot be blocked or exposed with anti-virus software and can activate themselves either when certain criteria are met or after user interaction (i.e., opening a file).
- Cinderella Attacks: These attacks can occur when a malicious user, gains access to a system and changes the internal clock of the network. This action leads to false premature expiration of the security software (i.e., antivirus), making it useless thus increasing the network's vulnerabilities Nabiyev (2022).
- Big Data Handling: Large IoT networks with many devices interacting, create a massive amount of data. If the hardware used in the network cannot process the data according to to present or future requirements, it can lead to network disturbance and data losses Ferrag et al. (2020b).

Table 5 presents the attack types identified at the Application Layer in IoT systems as the most crucial. The targets of these attacks are the applications and the software in general. The weaknesses are located in applications and the system. The last column of the table that proposes some countermeasures are all towards the detection of these attacks, as prevention mechanisms have failed to stop them and thus they occur Sadhu et al. (2022).

5.4. Cross-layer attacks

Except for the aforementioned, cross-layer attacks are also a threat to IoT systems. As stated in Asati et al. (2018) a cross-layer attack that combines vulnerabilities across multiple network protocol layers can cause more damage as compared to a single-layer attack. Several scholars have investigated cross-layer attacks. Radosavac and Benammar introduced DoS (Denial of Service) attacks in wireless ad hoc networks that disseminate from MAC to the network layer, causing the interrupt in critical routes Radosavac et al.

(2004). Wang and Yan Wang et al. (2010) study coordinated attacks by reporting false sensed data attacks (RFSD) at the PHY layer. Recently Asati et al. (2018) proposed Rank Manipulation and Drop Delay (RMDD) cross-layer attack in loT, and looked into how a low-intensity attack on the routing protocol for low power lossy networks (RPL) reduces application throughput.

5.5. Countermeasures

In the previous section, we presented a plethora of attacks that can be materialized either in one or several layers affecting the proper operation of the applications supported by an IoT. These applications cover all critical and everyday aspects of the life of citizens in a modern city and demand cybersecurity solutions that can make these applications trustful, stable, and safe. Security solutions can be divided into three main categories: software, hardware, and organizational/procedural measures.

Every architecture that incorporates IoT solutions should start with the adoption of internationally accepted security standards within organizations, particularly those that deal with critical operations like health care or energy. The use of security tools for both prevention and investigation, such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and anti-virus and malware programs should also be included where needed. The implementation of measures for forensics, patching and upgrading, physical security, access control, and authentication are also important. Finally, the improvement of incident response capabilities should always be a priority for all modern digital systems.

Especially for IoT the solutions should include lightweight encryption Algorithms, distributed detection mechanisms, federated learning, adversarial learning methods, and advanced authentication of both devices and users (Papaspirou et al. (2021)). As stated in Rana et al. (2022) due to the heterogeneity, scalability, and dynamic nature of the Internet of Things, conventional cybersecurity cryptography such as AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), DES (Data Encryption Standard), Blowfish, and RC6 cannot be immediately utilized in these domains. Solutions like the ones proposed in Hedayati and Mostafavi (2022); Abutaha et al. (2022) are good examples of such solutions.

Regarding detection mechanisms that could be used for reporting abnormal operation of an IoT system several solutions were recently introduced. Friha et al. (2022) proposed a federated learning-based intrusion detection system for the protection of agricultural-IoT infrastructures called FELIDS that can both protect the privacy of IoT devices data and achieve high accuracy against several attacks. This model has not tested against adversarial attacks something that was extensively researched by Martins et al. (2020) using various adversarial attack strategies.

6. IoT Applications

As mentioned above, IoT systems could be deployed to support endless applications. Basically, "anything" can be turned into an IoT device that can interconnect with other devices on a network boosting productivity, safety, and cost reduction. However, we will address some of the areas that IoT would reinvent, providing unimaginable capabilities never thought of before.

6.1. Agricultural

IoT implementations can improve different parts of the agro-industrial industry, like soil state and environmental conditions evaluation (Oxygen, Hydration, temperature, CO2), biomass consistency, and more, but also to adjust variables during the production or transportation phase. Another implementation is to keep track of and predict a product's inventory on shelves or even inside refrigerators while processing valuable analytics. Moreover, it can provide reliable information to the end user about the originality and ingredients of the product and promote an informed, connected, developed, and adaptable rural community. In summary, IoT in Agriculture can literally reinvent the industry in the years to come affecting farmers, suppliers, technicians, distributors, businessmen, consumers, and government representatives Talavera et al. (2017).

6.2. Health Care

IoT, in conjunction with real-time connected objects, can play a significant role in preventing serious illnesses and reducing healthcare costs Rehman et al. (2020). Moreover, the implementation has a long-term impact on the health monitoring, administration, and clinical service to patients' physiological information. The basic concept consists of patients connected with sensors and the data are forwarded to the health-monitoring unit. Sometimes data are stored in the cloud, which helps to manage the amount of data with safety Kelli et al. (2021).

An IoT implementation coupled with machine learning can be used for the early detection of heart diseases Kumar and Gandhi (2018) or arthritis.

This type of implementation consists of wearable devices for collecting sensor data, a cloud center for storing the data, and a regression-based prediction model for heart diseases and arthritis.

Each year, millions of people over 65 years old fall. An IoT implementation with a simple detection algorithm can be used to detect people who fall into specific areas. These areas will contain RFID information and location identification data that can be used to provide alerts to hospitals and family members thus preventing a possible life loss Selvaraj and Sundaravaradhan (2020).

The IoT-based healthcare system can provide ways to collect data from cancer patients and monitor them on real-time for long periods while using a variety of sensors and communication protocols. The use of a network of sensors and suitable communication protocols allows us to have smart devices which can transmit data remotely through different servers from one end to the other. It can become quite easy for patients and the specialized medical staff, such as oncologists, to monitor and analyze the health condition of cancer patients, especially beneficial for those with deteriorating health situations.

During a pandemic, like COVID-19, IoT can be used to monitor quarantined and high-risk patients by using the internet and a smart sensor or a mobile phone Umair et al. (2021). Moreover, tracking the location of medical equipment in real-time can improve treatment process speed while providing procedure transparency.

6.3. Environmental Applications

As ESG (Environmental-Social-Governance) is a common tool worldwide for new technology evaluation, environmental IoT applications can be considered important. Real-time maps with air and water pollution, pandemic data, noise levels, temperature, and harmful radiation, can now become a reality with the use of smart sensors. Besides that, IoT is capable in collecting and storing environmental records, checking the compliance of environmental variables with local policies, triggering alerts, or sending recommendation messages to citizens and authorities. These data can be used by governments and organizations as inputs for predictive models to forecast environmental variables and track pollution sources over time and space, ultimately leading to faster and better decisions to ensure a safe and healthy environment for all citizens Talavera et al. (2017)

6.4. Maritime Industry

Ships and vessels are lacking many of the technologies that are used onshore, due to the open sea environment (absence of steady internet coverage, equipment more prone to defections, etc.). Since many on-board departments need to cooperate, real-time information on board is crucial. The maintenance department could monitor shipboard equipment in real time to deal proactively with maintenance, by monitoring shipboard equipment and machinery enhanced with IoT technology, to discover issues and prevent potential failures. In addition, since fuel represent about 55 percent of total ship operating costs, smart sensors and monitoring equipment on-board can track the ship's performance and report back to the headquarters on shore, which in turn can support the ship master and chief engineer with guidance when planning the most fuel-efficient route. Finally, identifying optimal speed, current, and upcoming weather conditions and engine configuration will potentially save significant amounts of fuel while minimizing CO2 emissions Plaza-Hernández et al. (2020).

6.5. Military

The capabilities of an IoT system besides wealth creation, productivity, and security can also be used in the Military. Many Countries worldwide are already trying to promote Military and Defense Applications through IoT implementations in order to overcome various warfare and battlefield challenges. In this case, we have the "Internet of Military Things" (IoMT) which is a class of IoT applications for Intelligent warfare and modern combat operations. By creating a miniature ecosystem of smart technology capable of distilling sensory information and autonomously governing multiple tasks at once, the IoMT is conceptually designed to offload much of the physical and mental burden that warfighters encounter in field combat. Use cases like real-time Health monitoring, Augmented reality training, superior Fleet management, Target recognition, and Battlefield awareness are only a few of the capabilities provided by an IoT implementation.

6.6. Smart Cities

IoT applications in a city are unimaginable and include everything from energy management, smart lighting, and intelligent traffic management to water treatment and wastewater management or evacuation guidelines in case of an emergency. In a machine-to-human approach, data from sensors in traffic lights can be used by the central authority to adjust traffic flow. In a machine-to-machine approach, intelligent traffic systems (i.e., smart traffic lights, traffic cameras, and a cloud data center) can monitor traffic and public transportation to calculate possible upcoming congestion with the use of A.I. and prevent them by adjusting traffic flow. IoT sensors in streetlights could also adjust not only power states (ON/OFF) but also brightness depending on real light conditions (i.e., from dusk till dawn). Considering the number of streetlights that can be found in a city, these few watts from every streetlight add up, making the savings and environmental impact worthy. Moreover, those same sensors can also alert if light needs servicing, reducing repair tickets and saving time to the service department Balandina et al. (2015).

A Smart Campus is a similar case, because we can assume it is a miniature of a Smart City with a more demanding framework that enables learning, social interaction, and creativity. Monitoring a smart campus with a robust surveillance system is essential to ensure its uninterruptible secure operation. Security-relevant findings for the construction of such monitoring systems are provided by the survey in Anagnostopoulos et al. (2021).

6.7. Transportation and Logistics

Transportation and logistics are industries that already reap the benefits of IO systems from a variety of applications. However, IoT could inform, in real-time, all kinds of fleets (cars, trucks, ships, trains, etc.) that carry goods, to reroute based on traffic, upcoming weather conditions, and vehicle or driver availability, thanks to IoT sensor data. The inventory itself could also be equipped with sensors for tracking and temperature-control monitoring, as many industries like food and beverage, flower, and pharmaceutical often carry temperature-sensitive products. In this case, alerts can be sent when temperatures change to a level that threatens the product. Furthermore, blockchain technologies can be used to ensure that the information about the transportation of goods has not been altered Rathee et al. (2022b)

6.8. Smart Grid

Always, energy grids were designed to deliver electricity from large power stations powered by coal, nuclear, etc. to a wide network of homes and businesses. Until now, the electric grid could not accept power contributions from houses and businesses that are harvesting power via renewable sources (solar panels, windmills, etc.). A smart grid though, is capable of accepting power from decentralized mini power stations like a house with solar panels while coupled with wireless smart meters, can monitor how much energy a net-positive establishment is generating and reimburse them accordingly. Besides smart meters, every piece of equipment can connect to the grid as well, enhancing its utilization. For example, data from weather stations could inform the grid that in upcoming cloudy weather the solar panels will stop contributing power, hence the grid should adapt to this parameter. Hassan et al. (2020)

7. Challenges

Nowadays, numerous IoT devices are interacting through networks to provide for the user, with the required information. However, when addressing IoT implementations it is not that easy, since besides security, many challenges arise, and in the next sessions we will briefly describe some of the key challenges Karie et al. (2020).

7.1. Standardization

As mentioned above, standardization is necessary because, without established regulations, precise guidelines, and worldwide standards, the industry will eventually face serious incompatibilities from unregulated IoT expansion which are more difficult to track and examine their impacts to different sectors. In addition, many IoT devices are handling unstructured data that are stored in various types of databases (NoSQL etc.) with different querying approaches, creating incompatibilities between systems. Since the number of end users keeps rising along with the extensive use of IoT devices in many sectors, a new attack vector arises. Similar attack methods have led to increased acceptance of the need for regulation, legislation, stronger protection measures, and more strict controls for devices that authenticate on the Internet Ferrag et al. (2019).

7.2. Integration

In communication networks, device integration is highly affected by the lack of effective standards and IoT is no exception. Since “traditional” communication interoperability is challenging due to the wide range of available technologies making it hard to communicate seamlessly between multi-vendor devices, IoT communication interoperability is more difficult to implement due to different programming languages and an enormous number of different components, utilized in the IoT hardware development. With these types of incompatibilities, the reliability of a network is dramatically decreased making communication unstable. These issues have led the market to propose certain solutions like standardization of protocols, but these solutions leave behind many incompatible hardware devices.

7.3. Privacy

Since connected devices around the world are increasing exponentially, adversaries now have many more potential entry points into a network. In simple terms, for every new IoT device connected to a network the attack surface increases because an adversary now has many more devices prone to hacking thus exposing the whole network's safety. Additionally, the ability to collect and distribute data and information to another device or network autonomously is also a disadvantage since the data could be sensitive but certainly will be vulnerable. For example, there are IoT devices that require users to agree to terms and conditions of service before interacting with them. These types of agreements can expose users' data making them vulnerable to attack. Therefore, strategies need to be developed to handle people's privacy options across a broad spectrum of expectations. Since ease of use and security are "enemies", the industry must figure out a solution that promotes technological innovation and services while avoiding putting sensitive private data and information in danger.

7.4. Regulation

Due to the diversity in the implementations of IoT technology and the legal scope that regulates IoT devices, there have been numerous dilemmas with reference to the regulations and laws that apply, complicating its users whether certain actions are prohibited or not in each jurisdiction Ploennigs et al. (2018). Some of the legal questions that have arisen with regard to the use of IoT devices include data retention and destruction policies, legal liability for unintended uses of IoT devices, security breaches or privacy lapses, to name just a few Derhab et al. (2019). Additionally, global regulation, for instance, rules, processes, protocols, audits, transparency, and continuity, is thus far absent in the IoT sphere, as a result of the nonexistent legislation applied in general in the IoT field. Such regulations in the industrial, national, and international spheres could be remarkably beneficial in assisting organizations to become more efficient and reliable as far as systems are concerned and contribute to the lessening of errors in the future Hanes et al. (2017).

7.5. Energy

IoT devices have to successfully resist a challenge to their own energy efficiency. Small or tiny ones base their operation and effectiveness usually on a battery's capacity and well-charging capabilities with the required periodical services. Software is responsible for controlling and checking the energy requirements, and for optimizing energy consumption as an ongoing task. But hardware does not make energy consumption visible by the software, and thus how software fails to serve certain checks properly. The device then might discontinue its operation due to energy exhaustion. Energy transparency between software development and hardware is a promising proposal in Georgiou et al. (2018). Transparency is achieved by creating a bridge between hardware and software, which will facilitate the interoperability between them and will ensure the energy consumption estimation for the continuous functioning of a device.

7.6. Hardware

The emerging technology of IoT hardware has many different challenging perspectives. Several types of sensors for temperature, light, or humidity, various smart wearables for head, arm, or feet, and standard devices, such as tablets and smartphones, each impose a set of requirements that need to be fulfilled, and all construct and assemble an IoT infrastructure. In addition, hardware-level security concerns Polychronou et al. (2021) were raised due to this diversity and the necessity to absorb it under the umbrella of a secure application.

7.7. Cost

It is hard to separate a challenge from the above list from the cost factor. Standardization suppresses incompatibilities, lack of device integration reduces network reliability, data privacy requires advanced security strategies, a global legislation framework will promote the reliability of IoT systems, energy exhaustion affects the operation, and hardware diversification all directly or indirectly influence and determine cost. Consequently, organizations with IoT infrastructures confront a sequence of challenges, including cost evaluation Pincheira et al. (2021), to ensure beneficial results when taking critical decisions.

8. Conclusions

With the advance of low-cost computing, cloud services, big data technologies, analytics, and mobile technologies, small-size physical devices forming a network, can collect and exchange data without human intervention. In this hyperconnected environment, every node can record, monitor, and adjust each interaction between connected things. This promising technology threatens users' privacy and security in the different environments under which is deployed. For this reason, solutions to threat detection, intrusion, compromise or misuse in the IoT domain should be developed and generally agreed-upon standards and security regulations are necessary for the industry to thrive. Since the advantages of the technology are not questionable, governments and engineers must unite their powers and overcome the challenges to make IoT networks be viewed as traditional networks making the term Internet of Everything valid.

Aarika, K., Bouhlal, M., Abdelouahid, R.A., Elfilali, S., Benlahmar, E., 2020. Perception layer security in the internet of things. Procedia Computer Science 175, 591–596.

Abutaha, M., Atawneh, B., Hammouri, L., Kaddoum, G., 2022. Secure lightweight cryptosystem for iot and pervasive computing. Scientific Reports 12, 1–15.

Ahamed, J., Rajan, A.V., 2016. Internet of things (iot): Application systems and security vulnerabilities, in: 2016 5th International conference on electronic devices, systems and applications (ICEDSA), IEEE. pp. 1–5.

Al-Sarawi, S., Anbar, M., Abdullah, R., Al Hawari, A.B., 2020. Internet of things market analysis forecasts, 2020–2030, in: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE. pp. 449–453.

Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of things security: A survey. Journal of Network and Computer Applications 88, 10–28.

de Almeida, I.B.F., Mendes, L.L., Rodrigues, J.J., da Cruz, M.A., 2019. 5g waveforms for iot applications. IEEE Communications Surveys & Tutorials 21, 2554–2567.

Alohali, B.A., Vassilakis, V.G., Moscholios, I.D., Logothetis, M.D., 2018. A secure scheme for group communication of wireless iot devices, in: 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), IEEE. pp. 1–6.

Alqarawi, G., Alkhalifah, B., Alharbi, N., El Khediri, S., 2022. Internet-of-things security and vulnerabilities: Case study. Journal of Applied Security Research , 1–17.

Ammar, M., Russello, G., Crispo, B., 2018. Internet of things: A survey on the security of iot frameworks. Journal of Information Security and Applications 38, 8–27.

Anagnostopoulos, T., Kostakos, P., Zaslavsky, A., Kantzavelou, I., Tsotsolas, N., Salmon, I., Morley, J., Harle, R., 2021. Challenges and solutions of surveillance systems in iot-enabled smart campus: A survey. IEEE Access 9, 131926–131954.

Asati, V.K., Pilli, E.S., Vipparthi, S.K., Garg, S., Singhal, S., Pancholi, S., 2018. Rmdd: Cross layer attack in internet of things, in: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE. pp. 172–178.

Balandina, E., Balandin, S., Koucheryavy, Y., Mouromtsev, D., 2015. Iot use cases in healthcare and tourism, in: 2015 IEEE 17th conference on business informatics, IEEE. pp. 37–44.

de Carvalho Silva, J., Rodrigues, J.J., Alberti, A.M., Solic, P., Aquino, A.L., 2017. Lorawan—a low power wan protocol for internet of things: A review and opportunities, in: 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), IEEE. pp. 1–6.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P., 2019. Network intrusion detection for iot security based on learning techniques. IEEE Communications Surveys & Tutorials 21, 2671–2701.

Chaudhary, A., Peddoju, S.K., Kadarla, K., 2017. Study of internet-of-things messaging protocols used for exchanging data with external sources, in: 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE. pp. 666–671.

Chaudhary, P., Gupta, B., Singh, A., 2022. Adaptive cross-site scripting attack detection framework for smart devices security using intelligent filters and attack ontology. Soft Computing , 1–16.

Cui, Z., Zhao, Y., Cao, Y., Cai, X., Zhang, W., Chen, J., 2021. Malicious code detection under 5g hetnets based on a multi-objective rbm model. IEEE Network 35, 82–87.

Da Xu, L., Lu, Y., Li, L., 2021. Embedding blockchain technology into iot for security: A survey. IEEE Internet of Things Journal 8, 10452–10473.

Derhab, A., Cheikhrouhou, O., Allouch, A., Koubaa, A., Qureshi, B., Ferrag, M.A., Maglaras, L., Khan, F.A., 2022. Internet of drones security: Taxonomies, open issues, and future directions. Vehicular Communications , 100552.

Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M.A., Mukherjee, M., Khan, F.A., 2019. Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security. Sensors 19, 3119.

Dorri, A., Mishra, S., Jurdak, R., 2022. Vericom: A verification and communication architecture for iot-based blockchain. Ad Hoc Networks 133, 102882.

English, K.V., Obaidat, I., Sridhar, M., 2019. Exploiting memory corruption vulnerabilities in connman for iot devices, in: 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE. pp. 247–255.

Ferrag, M.A., Maglaras, L., Ahmim, A., Derdour, M., Janicke, H., 2020a. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. Future internet 12, 44.

Ferrag, M.A., Maglaras, L., Derhab, A., 2019. Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends. Security and Communication Networks 2019.

Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks 2017.

Ferrag, M.A., Shu, L., Yang, X., Derhab, A., Maglaras, L., 2020b. Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges. IEEE access 8, 32031–32053.

Fielding, R.T., 2000. Rest: architectural styles and the design of network-based software architectures. Doctoral dissertation, University of California .

Friha, O., Ferrag, M.A., Shu, L., Maglaras, L., Choo, K.K.R., Nafaa, M., 2022. Felids: Federated learning-based intrusion detection system for agricultural internet of things. Journal of Parallel and Distributed Computing 165, 17–31.

Frustaci, M., Pace, P., Aloi, G., Fortino, G., 2017. Evaluating critical security issues of the iot world: Present and future challenges. IEEE Internet of things journal 5, 2483–2495.

Georgiou, K., Blackmore, C., Xavier-de Souza, S., Eder, K., 2018. Less is more: Exploiting the standard compiler optimization levels for better performance and energy consumption, in: Proceedings of the 21st International Workshop on Software and Compilers for Embedded Systems, pp. 35–42.

Guezzaz, A., Benkirane, S., Azrour, M., 2022. A novel anomaly network intrusion detection system for internet of things security, in: IoT and Smart Devices for Sustainable Environment. Springer, pp. 129–138.

Gupta, B.B., Quamara, M., 2020. An overview of internet of things (iot): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience 32, e4946.

Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., Henry, J., 2017. IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things. Cisco Press.

Hashemi, S., Zarei, M., 2021. Internet of things backdoors: resource management issues, security challenges, and detection methods. Transactions on Emerging Telecommunications Technologies 32, e4142.

Hassan, R., Qamar, F., Hasan, M.K., Aman, A.H.M., Ahmed, A.S., 2020. Internet of things and its applications: A comprehensive survey. Symmetry 12, 1674.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A survey on iot security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743.

Hedayati, R., Mostafavi, S., 2022. A lightweight image encryption algorithm for secure communications in multimedia internet of things. Wireless Personal Communications 123, 1121–1143.

Illy, P., Kaddoum, G., Kaur, K., Garg, S., 2022. Ml-based idps enhancement with complementary features for home iot networks. IEEE Transactions on Network and Service Management .

Jasim, K.F., Ismail, R.J., Al-Rabeeah, A.A.N., Solaimanzadeh, S., 2021. Analysis the structures of some symmetric cipher algorithms suitable for the security of iot devices. Cihan University-Erbil Scientific Journal 5, 13–19.

Karie, N.M., Sahri, N.M., Haskell-Dowland, P., 2020. Iot threat detection advances, challenges and future directions, in: 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), IEEE. pp. 22–29.

Kelli, V., Sarigiannidis, P., Argyriou, V., Lagkas, T., Vitsas, V., 2021. A cyber resilience framework for ng-iot healthcare using machine learning and blockchain, in: ICC 2021-IEEE International Conference on Communications, IEEE. pp. 1–6.

Khan, S., Shakil, K.A., Alam, M., 2020. Internet of Things (IoT): Concepts and Applications. Springer.

Kumar, P.M., Gandhi, U.D., 2018. A novel three-tier internet of things architecture with machine learning algorithm for early detection of heart diseases. Computers & Electrical Engineering 65, 222–235.

Lee, I., Lee, K., 2015. The internet of things (iot): Applications, investments, and challenges for enterprises. Business Horizons 58, 431–440.

Lombardi, M., Pascale, F., Santaniello, D., 2021. Internet of things: A general overview between architectures, protocols and applications. Information 12, 87.

Maglaras, L., Ayres, N., Moschoyiannis, S., Tassiulas, L., 2022a. The end of eavesdropping attacks through the use of advanced end to end encryption mechanisms, in: IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE. pp. 1–2.

Maglaras, L., Ferrag, M.A., Derhab, A., Mukherjee, M., Janicke, H., Rallis, S., 2019. Threats, protection and attribution of cyber attacks on critical infrastructures. arXiv preprint arXiv:1901.03899 .

Maglaras, L.A., Ferrag, M.A., Janicke, H., Ayres, N., Tassiulas, L., 2022b. Reliability, security, and privacy in power grids. Computer 55, 85–88.

Martins, N., Cruz, J.M., Cruz, T., Abreu, P.H., 2020. Adversarial machine learning applied to intrusion and malware scenarios: a systematic review. IEEE Access 8, 35403–35419.

Mukherjee, M., Ferrag, M.A., Maglaras, L., Derhab, A., Aazam, M., 2020. Security and privacy issues and solutions for fog. Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics , 353–374.

Nabiyev, B.R., 2022. Investigation of computer incidents for cyber-physical infrastructures in industrial control systems, in: Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems. IOS Press, pp. 125–130.

Pan, J., Yang, Z., 2018. Cybersecurity challenges and opportunities in the new" edge computing+ iot" world, in: Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, pp. 29–32.

Papaspirou, V., Maglaras, L., Ferrag, M.A., 2020. A tutorial on cross site scripting attack-defense .

Papaspirou, V., Maglaras, L., Ferrag, M.A., Kantzavelou, I., Janicke, H., Douligeris, C., 2021. A novel two-factor honeytoken authentication mechanism, in: 2021 International Conference on Computer Communications and Networks (ICCCN), IEEE. pp. 1–7.

Pierleoni, P., Concetti, R., Belli, A., Palma, L., 2019. Amazon, google and microsoft solutions for iot: architectures and a performance comparison. IEEE access 8, 5455–5470.

Pincheira, M., Vecchio, M., Giaffreda, R., Kanhere, S.S., 2021. Cost-effective iot devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. Computers and Electronics in Agriculture 180, 105889.

Plaza-Hernández, M., Gil-González, A.B., Rodríguez-González, S., Prieto-Tejedor, J., Corchado-Rodríguez, J.M., 2020. Integration of iot technologies in the maritime industry, in: International Symposium on Distributed Computing and Artificial Intelligence, Springer. pp. 107–115.

Ploennigs, J., Cohn, J., Stanford-Clark, A., 2018. The future of iot. IEEE Internet of Things Magazine 1, 28–33.

Polychronou, N.F., Thevenon, P.H., Puys, M., Beroulle, V., 2021. A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in iot/iiot devices, and their detection mechanisms. ACM Transactions on Design Automation of Electronic Systems (TODAES) 27, 1–35.

Radosavac, S., Benammar, N., Baras, J.S., 2004. Cross-layer attacks in wireless ad hoc networks, in: Conference on Information Sciences and Systems.

Rana, M., Mamun, Q., Islam, R., 2022. Lightweight cryptography in iot networks: A survey. Future Generation Computer Systems 129, 77–89.

Rathee, G., Kerrache, C.A., Calafate, C.T., 2022a. An ambient intelligence approach to provide secure and trusted pub/sub messaging systems in iot environments. Computer Networks 218, 109401.

Rathee, G., Kerrache, C.A., Ferrag, M.A., 2022b. A blockchain-based intrusion detection system using viterbi algorithm and indirect trust for iiot systems. Journal of Sensor and Actuator Networks 11, 71.

Rathee, G., Kerrache, C.A., Lahby, M., 2022c. Trustblksys: A trusted and blockchained cybersecure system for iiot. IEEE Transactions on Industrial Informatics .

Rayes, A., Salam, S., 2017. Internet of things from hype to reality. Springer .

Rehman, O., Farrukh, Z., Al-Busaidi, A.M., Cha, K., Park, S.J., Rahman, I.M., 2020. Iot powered cancer observation system .

Rescorla, E., Modadugu, N., 2012. Rfc 6347: Datagram transport layer security version 1.2. Internet Engineering Task Force (IETF) , 2070–1721.

Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A., 2022. Internet of things: Security and solutions survey. Sensors 22, 7433.

Salah, S., Amro, B.M., 2022. Big picture: analysis of ddos attacks map-systems and network, cloud computing, scada systems, and iot. International Journal of Internet Technology and Secured Transactions 12, 543–565.

Salim, M.M., Rathore, S., Park, J.H., 2020. Distributed denial of service attacks and its defenses in iot: a survey. The Journal of Supercomputing 76, 5320–5363.

Santos, M.G.d., Ameyed, D., Petrillo, F., Jaafar, F., Cheriet, M., 2020. Internet of things architectures: A comparative study. arXiv preprint arXiv:2004.12936 .

Selvaraj, S., Sundaravaradhan, S., 2020. Challenges and opportunities in iot healthcare systems: a systematic review. SN Applied Sciences 2, 1–8.

Serpanos, D., Wolf, M., 2018. The iot landscape, in: Internet-of-Things (IoT) Systems. Springer, pp. 1–6.

Setetemela, K., Keta, K., Nkhabu, M., Winberg, S., 2019. Python-based fpga implementation of aes using migen for internet of things security, in: 2019 IEEE 10th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT), IEEE. pp. 194–198.

Singh, S., Rathore, S., Alfarraj, O., Tolba, A., Yoon, B., 2022. A framework for privacy-preservation of iot healthcare data using federated learning and blockchain technology. Future Generation Computer Systems 129, 380–388.

Sparavigna, A., 2008. Labels discover physics: the development of new labelling methods as a promising research field for applied physics. arXiv preprint arXiv:0801.2700 .

Takarabt, S., Schaub, A., Facon, A., Guilley, S., Sauvage, L., Souissi, Y., Mathieu, Y., 2019. Cache-timing attacks still threaten iot devices, in: International Conference on Codes, Cryptology, and Information Security, Springer. pp. 13–30.

Talavera, J.M., Tobón, L.E., Gómez, J.A., Culman, M.A., Aranda, J.M., Parra, D.T., Quiroz, L.A., Hoyos, A., Garreta, L.E., 2017. Review of iot applications in agro-industrial and environmental fields. Computers and Electronics in Agriculture 142, 283–297.

Thankappan, M., Rifà-Pous, H., Garrigues, C., 2022. Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review. arXiv preprint arXiv:2203.00579 .

Umair, M., Cheema, M., Cheema, O., Li, H., Lu, H., 2021. Impact of covid-19 on iot adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial iot. Sensors .

Vashi, S., Ram, J., Modi, J., Verma, S., Prakash, C., 2017. Internet of things (iot): A vision, architectural elements, and security issues, in: 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE. pp. 492–496.

Vignau, B., Khoury, R., Hallé, S., 2019. 10 years of iot malware: A feature-based taxonomy, in: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), IEEE. pp. 458–465.

Wang, J., Lim, M.K., Wang, C., Tseng, M.L., 2021. The evolution of the internet of things (iot) over the past 20 years. Computers & Industrial Engineering 155, 107174.

Wang, W., Sun, Y., Li, H., Han, Z., 2010. Cross-layer attack and defense in cognitive radio networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, IEEE. pp. 1–6.

Wara, M.S., Yu, Q., 2020. New replay attacks on zigbee devices for internet-of-things (iot) applications, in: 2020 IEEE International Conference on Embedded Software and Systems (ICESS), IEEE. pp. 1–6.

Yang, X., Shu, L., Liu, Y., Hancke, G.P., Ferrag, M.A., Huang, K., 2022. Physical security and safety of iot equipment: A survey of recent advances and opportunities. IEEE Transactions on Industrial Informatics 18, 4319–4330.

Zubair, M., Unal, D., Al-Ali, A., Shikfa, A., 2019. Exploiting bluetooth vulnerabilities in e-health iot devices, in: Proceedings of the 3rd international conference on future networks and distributed systems, pp. 1–7.

Protocol	Advantages	Disadvantages
AMQP	Reliability Security, Extendibility with minimal effort	Heavy memory requirements, Slow data transmission
MQTT	Low power consumption Low bandwidth usage	Limited interoperability, Inherent security constraints, Poor extendibility
Zigbee	Highly secure, Low power consumption, long range of communication	prone to interference, expensive
Z-Wave	Low latency, Low power consumption, Reasonable coverage	Low data transfer rate, Premium prices
Wi-Fi	Convenient and easy to instal, High data transfer rate	High power consumption, Hard to scale
LoRaWAN	Scalability, Large are coverage, Low power consumption	Low data transfer rate, Custom LoRa gateway

Table 2: Communication Protocols for IoT in a 4-layer ISO architecture: Pros and Cons

Attack	Target	Weakness	Countermeasure
Eavesdropping	Devices	Low Power (no encryption), no monitoring.	Encryption Maglaras et al. (2022a)
Node Capture	Network's Key Node	Vulnerable Protocols.	Detection Mechanisms
Malicious Fake Node	Network	IoT's easiness to create networks.	Detection Mechanisms Guezzaz et al. (2022), Trust services Rathee et al. (2022a)
Replay Attack	Authentication Information	Vulnerable Protocols.	Session Keys, blockchain Rathee et al. (2022c), Detection Mechanisms Rathee et al. (2022b)
Timing Attack	Devices with limited capabilities	Device unique behavior and response time.	Privacy Protection Mechanisms Singh et al. (2022)

Table 3: Attack Surface at the Perception Layer in IoT Systems

Attack	**Target**	**Weakness**	**Countermeasure**
DoS Attack	Devices or Network Resources	Vulnerable Protocols.	Detection Mechanisms Friha et al. (2022)
IP Fragmentation Attacks	Network's MTU	Vulnerable Protocols.	Detection Mechanisms Illy et al. (2022)
Man in The Middle Attacks	Communication Data	Vulnerable Protocols.	E2E encryption Maglaras et al. (2022a)
Storage Attacks	Data Stored on Storage Devices	No Encryption.	Lightweight Encryption Algorithms Abutaha et al. (2022)
Exploit Attacks	System and Information Stored	Application, System, and Hardware Vulnerabilities.	Application and System Upgrade, Hardware Replacement Hashemi and Zarei (2021)

Table 4: Attack Surface at the Network Layer in IoT Systems

Attack	**Target**	**Weakness**	**Countermeasure**
Cross Site Scripting	Application	Application and System Vulnerabilities.	Detection Mechanisms Chaudhary et al. (2022)
Malicious Code Attack	Application and System	Application and System Vulnerabilities.	Detection Mechanisms Cui et al. (2021)
Cinderella Attacks	Security Software	System Vulnerabilities.	Detection Mechanisms Friha et al. (2022)
Big Data Handling	System	System Vulnerabilities.	Detection Mechanisms Friha et al. (2022)

Table 5: Attack Surface at the Application Layer in IoT Systems

Declaration of interests

☒ 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.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: