Suleyman Demirel University
Faculty of Engineering and Natural Sciences
Department of Computer Science

Dean of Faculty

Associate Professor

PhD Zhamanov A.

«06» 06 2023

Topic of the thesis:

Ontology for the Internet of Things

Thesis submitted as part of the requirements for the award of the MSc in "7M06102 - Computer Science" SDU, 2021-2023

Head of Department _____ Assistant Professor, PhD Mukash Zh.

Academic Supervisor _____ Associate Professor Tulemissova G.

Master student _____ Rakhmetolla D.

Kaskelen 2023

Ministry of Science and Higher Education of the Republic of Kazakhstan

Suleyman Demirel University

Dauren Rakhmetolla

Ontology for the Internet of Things

THESIS

Presented in Partial Fulfilment for the

Master of Technical Sciences Degree in Computer Science

(degree code: 7M06102)

Department of Computer Science

Faculty of Engineering and Natural Sciences

Supervisor: **Associate Professor Gulfarida Tulemissova**

Kaskelen 2023

Suleyman Demirel University
Faculty of Engineering and Natural Sciences
Department of Computer Science

Dean of Faculty

Associate Professor

PhD Zhamanov A.

_____

« _____ »_____ 2023

Topic of the thesis:

Ontology for the Internet of Things

Thesis submitted as part of the requirements for the award of the MSc in "7M06102 - Computer Science" SDU, 2021-2023

Head of Department _____ Assistant Professor, PhD Mukash Zh.

Academic Supervisor _____ Associate Professor Tulemissova G.

Master student _____ Rakhmetolla D.

Kaskelen 2023

Declaration

I, Dauren Rakhmetolla, declare that the thesis work submitted, titled "Ontology for the Internet of Things", is my personal work and is the result of my own research based on prior work in the field. No materials or ideas taken from other sources have been used in the work, except for those that are explicitly indicated and documented in the list of references. All citations and references to other studies are correctly identified and cited accordingly. I also certify that this dissertation has not been previously presented as a dissertation in any other educational institution or organization. All sources of information, quotations and materials of other authors that were used in the work are clearly identified and appropriately attributed. This dissertation is presented in accordance with the requirements and standards established by SDU and is fully consistent with academic integrity and research ethics.

Dauren Rakhmetolla

2023

Acknowledgements

First of all, I want to thank my supervisor, Gulfarida Tulemissova, for her valuable knowledge, guidance and support throughout the study. Her expert guidance and valuable advice proved invaluable to the success of the job. I also express my gratitude to the university for providing all the conditions. Special thanks go to my colleagues and friends who supported me during this research. Your support, motivation and constructive discussions have been instrumental in achieving my goals.

Thanks to all of you, my dissertation work has become a reality. Your support and contributions have made a huge contribution to my professional development. I am deeply grateful to you for all your efforts and cooperation.

Dedication

I dedicate this dissertation to my parents, who have always supported me in all my endeavors and inspired me to achieve high goals. Your invaluable love, wisdom and support have been my pillars throughout this journey. Your professional guidance, expertise and motivation have been indispensable to this success. I also express my gratitude to my colleagues and friends who supported and inspired me throughout the study. Your discussions, ideas and feedback have been valuable in developing my research and professional skills. Your faith in me and in my abilities has always been a source of strength and inspiration. Finally, I express my gratitude to all those who have contributed to my field of research and technology, which became the basis for this dissertation. Your work as researchers, scientists and practitioners has been an important foundation for the development of my ideas and concepts. My work would never have been possible without the support and contributions of each and every one of you.

Abstract

This MSc thesis is devoted to the creation of a common ontology for the Internet of things (IoT) in order to clarify the general principles of building the IoT architecture in various industries and assess their variability over time. The paper reviews the literature, including studies, articles and publications related to the architecture and principles of building IoT. A comparative analysis of the most popular IoT platforms was carried out, their common features and differences were identified. Based on a literature review and comparative analysis, a general ontology for IoT has been developed, taking into account various aspects, such as devices, communication protocols, network infrastructure and security. A common ontology allows for a unified and structured approach to the IoT architecture, ensuring compatibility and interoperability between different systems and devices.

Аңдатпа

Диссертация әртүрлі салаларда IoT архитектурасын құрудың жалпы принциптерін анықтау және уақыт өте келе олардың өзгергіштігін бағалау мақсатында Заттар интернеті (IoT) үшін жалпы онтологияны құруға бағытталған. Жұмыста IoT құрылысының архитектурасы мен принциптеріне байланысты әдебиеттерге шолу жасалды. Ең танымал IoT платформаларына салыстырмалы талдау жүргізілді, олардың жалпы белгілері мен айырмашылықтары анықталды. Әдебиеттерді шолу және салыстырмалы талдау негізінде құрылғылар, байланыс протоколдары, желілік инфрақұрылым және қауіпсіздік сияқты әртүрлі аспектілерді ескере отырып, IoT үшін жалпы онтология әзірленді. Жалпы онтология әртүрлі жүйелер мен құрылғылар арасындағы үйлесімділік пен өзара әрекеттесуді қамтамасыз ете отырып, IoT архитектурасына біртұтас және құрылымдық тәсіл жасауға мүмкіндік береді.

Аннотация

Диссертация посвящена созданию общей онтологии для Интернета вещей (IoT) с целью выяснения общих принципов построения архитектуры IoT в различных отраслях и оценки их изменчивости со временем. В работе проведен обзор литературы, связанный с архитектурой и принципами построения IoT. Был проведен сравнительный анализ самых популярных платформ IoT, выявлены их общие черты и различия. На основе обзора литературы и сравнительного анализа разработана общая онтология для IoT, учитывающая различные аспекты, такие как устройства, протоколы связи, сетевая инфраструктура и безопасность. Общая онтология позволяет создать единый и структурированный подход к архитектуре IoT, обеспечивая совместимость и взаимодействие между различными системами и устройствами.

Abbreviations

IoT Internet of Things

WoT Web of Things

IIoT Industrial Internet of Things

SSN Semantic Sensor Network

HTTP HyperText Transfer Protocol

MQTT Message Queuing Telemetry Transport

TCP Transmission Control Protocol

AMQP Advanced Message Queuing Protocol

XMPP Extensible Messaging and Presence Protocol

UDP User Datagram Protocol

BLE Bluetooth Low Energy

LoRaWAN Long Range wide-area networks

OWL Web Ontology Language

RDF Resource Description Framework

CoAP Constrained Application Protocol

NFC Near Field Communication

RFID Radio Frequency IDentification

Table of Contents

Chapter 1

Background and motivations

1.1 Introduction

The IoT enables interaction, data sharing, and cooperation across various things and networks, resulting in intelligent and intelligent surroundings by connecting physical devices, sensors, and systems. However, the variety of IoT platforms, gadgets, and protocols now in use results in restrictions regarding compatibility, interoperability, and data sharing.

Ontology for the Internet of Things is the subject of the dissertation. The subject itself has a vague quality, thus it was first essential to define the scope of the research before formulating the formulation of the research problem. In order to address this, the study question was defined as follows: Are the fundamental guidelines for developing IoT architecture unique to each industry and evolving over time?

An overview of research on the Internet of Things (IoT) is given in this section. Works that significantly advance our understanding of IoT technology are taken into consideration. The examination uncovered the following areas of research and outcomes.

A portion of the research focuses on the semantic model of the Internet of Things, including methods for incorporating and evaluating sensor data in IoT systems. Other study focuses on IoT architecture, examining various strategies

and solutions as well as emphasizing the problems and difficulties involved in creating IoT systems. Some research explores the possibilities and uses of Linked Data in the context of IoT in a variety of scenarios[1]. The use of IoT technology for aid in daily living, such as Ambient Assisted Living (AAL), is another significant area of research. Additionally, research on the use of ontologies in IoT were undertaken, and the benefits and future possibilities for their application in the context of IoT systems were recognized. The advancement and development of IoT technology will benefit greatly from all of these research. They offer insightful data and a framework for further studies in this field.

Significance of the work: With the IoT developing quickly and the requirement for integration between many platforms and devices, it is crucial to have consistent architectural principles. By establishing consistency and uniformity in the structure, modeling, and data interchange inside the IoT, these principles can help systems operate more effectively and steadily.

Modern results on the topic: To date, significant results have already been achieved in the field of building IoT and developing ontologies related to this topic. However, most of these studies focus on specific aspects of the IoT and do not offer general principles that could be applied to a wide range of devices and platforms.

Research gap: The absence of consistent building IoT principles in this setting creates a research gap. There are yet no unified guidelines and standards that might enable communication and data sharing across different Internet of Things devices.

Problem statement, research questions, and research goals: The objective of this dissertation is to provide a standard ontology for the Internet of Things, which would give consistent construction guidelines for IoT. To do this, the following issues must be resolved:

- Identify the key ideas and traits that should be considered when creating a generic IoT ontology.
- Create a technique and procedure for creating such an ontology, taking into

consideration the variety of IoT platforms and devices.

- Comparatively analyze current IoT systems to see how well they adhere to the established guidelines and ontologies.

Creation of an Internet of Things (IoT) common ontology based on the many IoT tenets and traits. The process of developing a methodology and ontology will take into consideration the variety of IoT platforms and devices. 20 of the most well-known IoT systems are compared in terms of their adherence to the established guidelines and ontologies. Summary of the following chapters: The dissertation's next chapters will include a study of the literature, an examination and comparison of IoT platforms, the creation of a generic ontology of IoT, and an analysis of the findings. The last chapter will concentrate on recommendations for more study and conclusions.

Chapter 2

Overview of the IoT: Definition, principles and ontologies

2.1 Definition and basic principles of the IoT

The Internet of Things (IoT) is a theory that describes how physical things, systems, and devices may communicate and share data via a network to create intelligent and smart surroundings.[2]. Each physical thing in the IoT becomes an individually identified device that can generate, collect, and send data as well as communicate with other objects or systems(see Figure 2.1).

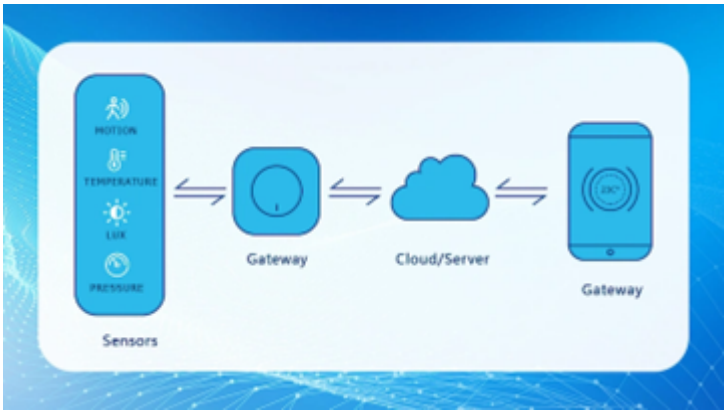

Figure 2.1: Communication of sensors with the gateway [3].

The main principles that determine the operation and functionality of the IoT are:

- Sensors are essential elements of the Internet of Things (IoT) that let you gather environmental data. They may gather data from other devices and measure physical parameters like temperature, humidity, and illumination.
- Wireless: The IoT's capacity to wirelessly transport data between devices is a key characteristic. IoT devices may communicate and interact without a direct physical connection by utilizing a variety of wireless protocols and standards.
- Cloud Computing: The enormous volume of data that IoT devices collect is processed and stored using cloud computing. To store, process, and analyze IoT data, cloud platforms offer scalable infrastructure and services.
- Data analytics: Collected IoT data may be examined to get insightful and useful information. Pattern recognition, event prediction, and automated decision-making are all possible with the help of analytical techniques like machine learning and artificial intelligence.
- Security: Security is crucial given the size and complexity of the IoT. The four major components of IoT security are data protection, device identification, authentication, and encryption[4].

The impact of network technologies, particularly those that intrude private and public space, should not only be passively safe but also preventively safe because people's lives and health depend on it[5]. If consumer or industrial systems are not adequately protected from risk, if all precautions are not taken to ensure their safe operation, and if there are no ways to reduce or completely eliminate the effects of adverse events, it is impossible to allow the spread of technologies that have the potential to have significant negative or even catastrophic effects on them(see Figure 2.2).

It has not been and will not be feasible to completely rule out the possibility of dangerous circumstances occurring in technically complicated systems, especially those incorporating several distinct devices, algorithms, and pieces of

information. Not to mention quite plausible, the infamous "human factor" is also a possibility. A system of defense against several risks, including those that are technological, methodological, informational, market-related, event-related, resource-related, and many more, must be developed[6][7].

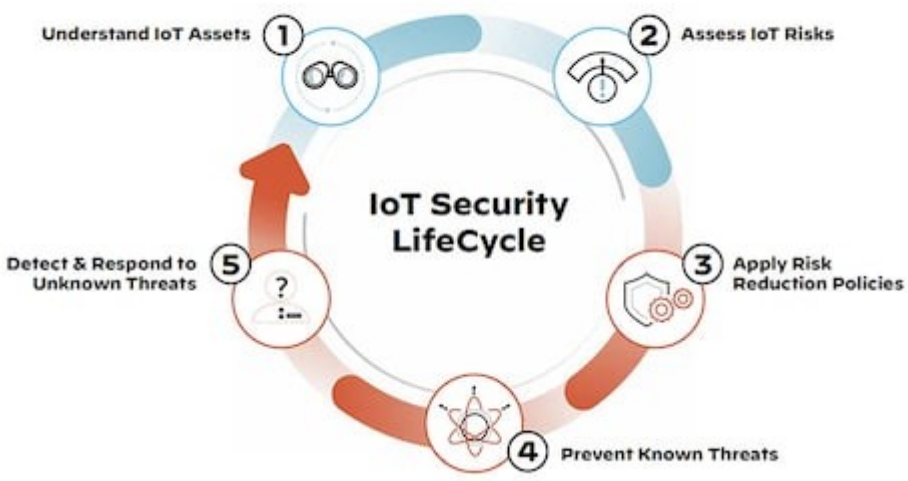

Figure 2.2: IoT security lifecycle [8].

On the other hand, full quality protection against unfavorable occurrences, their eradication, and compensation for their effects can only be offered by an autonomous, specialized firm that is growing systematically and instrumentally. Legally, it may be a stand-alone individual or a different division of a big corporation.

As a result, it will be required to establish specialized, highly skilled risk management centers in order for the Internet of Things to expand actively and safely:

- analyze and predict risks
- to prevent risky events
- to manage the course of risky events
- to eliminate the consequences of adverse events
- to restore the normal state after risky events

It is not sufficient to create "magic" protocols and algorithms for compliance and security control in systems deployed using IoT technology. To keep track of

occurrences in the Internet of Things sectors and manage risks, including those related to their technological sustainability, information security, and independence and viability economically[9].

IoT involves not only mobile and stationary devices, not only physical things and algorithms, but also ordinary people, social groups, industries, and businesses[10]. A failure in the chain of transactions at any stage and on any subject can lead to unexpected consequences(see Figure 2.3).Therefore, a special type and informational level of risk management is required.

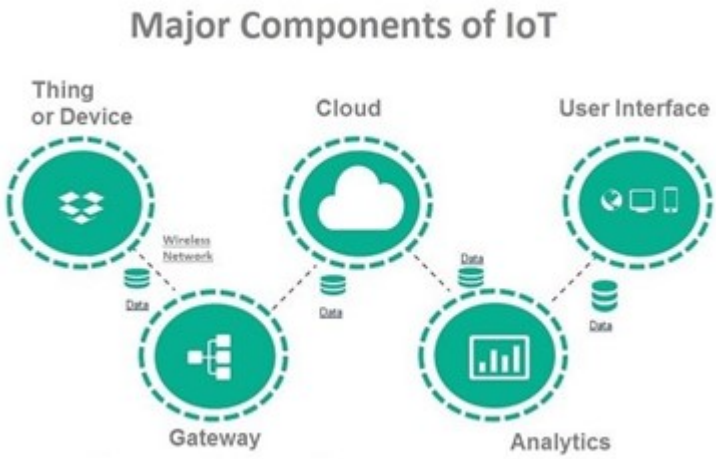

Figure 2.3: Major components of IoT [11].

IoT relies heavily on wireless technologies since they enable device communication without a physical connection. Communication protocols allow people to build wireless networks and communicate with one another. To safeguard the confidentiality and integrity of data, encryption and authentication procedures are required given the numerous devices and different network connections.

The utilization of cloud computing for data processing and analysis is a significant component of IoT. For storing and processing IoT data, cloud platforms offer computing resources and services. They also let you grow the infrastructure based on the system's requirements.

In order to further protect IoT devices from prospective attackers, cloud computing is used. Access is only given to trustworthy individuals when utilizing cloud authentication, and all data is secured. This guarantees that private information is kept secure(see Figure 2.4).

Figure 2.4: The IoT chain and cloud computing [12].

IoT devices may be patched and updated via cloud computing. Companies can simply and rapidly upgrade their IoT devices via the cloud. This keeps devices up to speed with the most recent security updates and makes it simpler to repair security problems.

The use of cloud computing allows for the monitoring of IoT device activities. Businesses may learn more about how their gadgets are being used by using the cloud. As a result, they are able to identify any suspicious or harmful activities and take appropriate measures to stop any possible security breaches.

2.2 Key Uses for the IoT

IoT opens up new possibilities for the app of technology across a range of human endeavors. With a network of interconnected devices capable of collecting, processing and transmitting data, the IoT opens the door to automating, monitoring and improving processes across industries. Thanks to this technology, physical objects such as smart devices, cars, industrial equipment and even home appliances can become part of a global network, interacting with each other and with people[13]. Applications for the Internet of Things (IoT) span a wide range of

fields and sectors where devices may connect to a network and share data to boost productivity and automate procedures.

Wearable devices. Perhaps the most noticeable kind of IoT gadget for the common person is wearable technology. These consist of virtual reality headsets, smart glasses, fitness trackers, smart watches, and more.

Smart Homes. Appliances from the home include the smart home system. The smart home has a variety of IoT gadgets, such as wireless kitchen appliances, smart lighting systems, mood music systems, electric shutters, automated windows and doors, and smart utility meters.

Smart cities. Smart cities use IoT devices such as sensors and meters to collect and analyze data(see Figure 2.5).

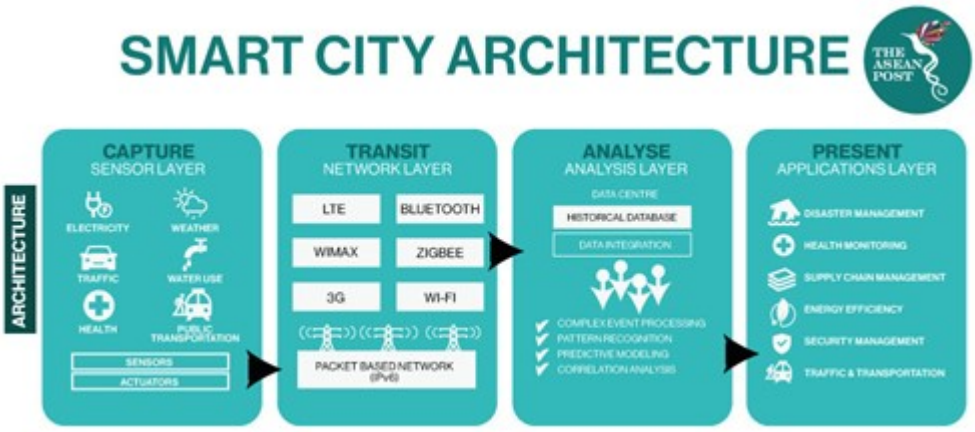

Figure 2.5: Smart city architecture [14].

This data can then be used to improve infrastructure, utilities and other services.

Self-driving cars. IoT-based technology is generally used in self-driving cars to communicate data about the vehicle and the road it is traveling on. To allow autonomous vehicle movement, the car's computer systems acquire and assess data on navigation, traffic, the outside environment, and other issues.

Retail. Retail is using IoT more and more. It enables you to deploy automated checkouts and smart shelves (which alert the seller when inventories are running short), robotize workplaces, and improve supply chain management in addition

to offering customized discounts. The Amazon retail network, which is based on the idea of automated shopping, includes elements of both traditional and online businesses. This is an example of the Internet of Things.

Healthcare Healthcare involves the use of computer and telecommunication technologies to provide medical services. The IoT is an important aspect of Healthcare (IoT is sometimes used to refer to the Internet of Medical Things) (see Figure 2.6).

Healthcare IoT provides the chance to manage medical resources, streamline processes, and improve the effectiveness and accessibility of medical care. The Internet of Things (IoT) in healthcare may be used to collect, examine, and distribute patient data as well as to oversee and control medical apparatus and equipment. Medical equipment with sensors may continuously detect health indicators like heart rate, blood pressure, oxygen levels, and others, and this information can be transferred in real time to a monitoring system.

The application of IoT in healthcare also raises a number of challenges and issues, including worries about data security and privacy, the necessity to standardize and make systems and devices interoperable, and the obligation to train medical personnel in the use of cutting-edge technology. In general, IoT in healthcare offers a wide range of potential to improve the efficiency and standard of medical care.

Smart farming. Utilizing digital technology to streamline agricultural activities is known as smart agriculture. Farmers may obtain general agricultural data using linked sensors, cameras, and other equipment, and then modify their operations to increase yields. (see Figure 2.7).

This list is not all-inclusive because the Internet of Things is altering how we live and work in many different sectors. Smart mobile phones, smart refrigerators, smart watches, fitness trackers, smart door locks, smart bikes, medical sensors, smart security systems, and virtual assistants like Alexa and Google Home are a few examples of IoT products. And the list keeps going.

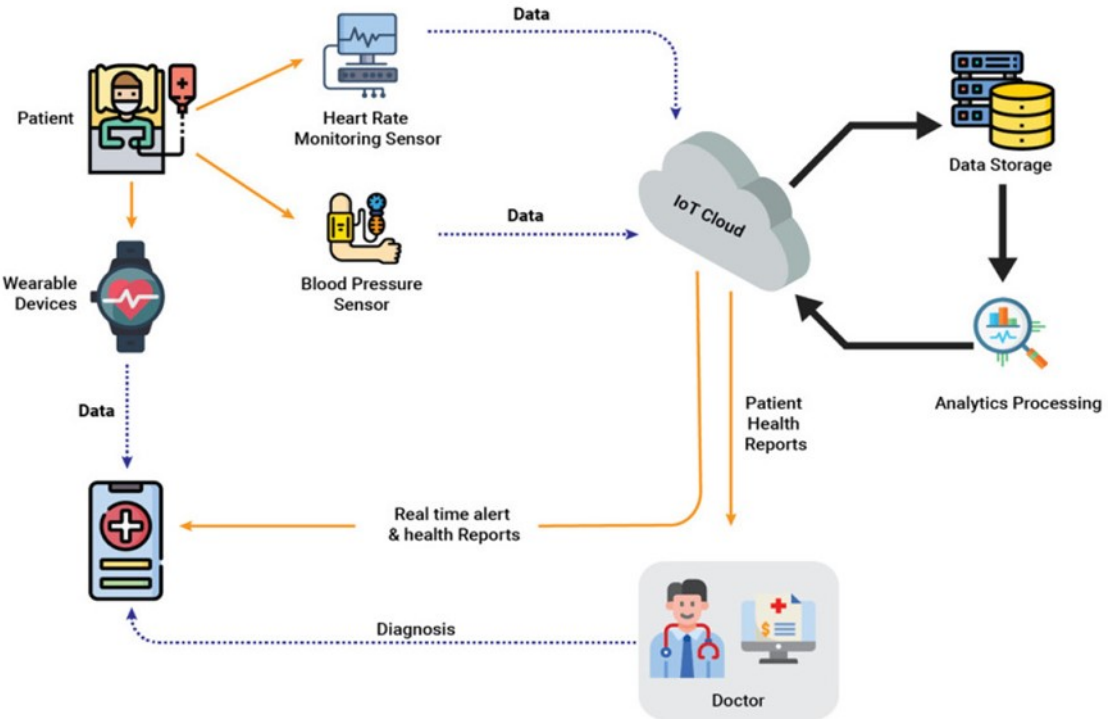

Figure 2.6: IoT Healthcare [15].

2.3 An examination of existing IoT construction methods and their driving principles

The study's analysis of existing IoT construction methods and their guiding principles is crucial since it gives you a thorough view of the range of methods and tactics employed in different IoT systems.

A centralized design, in which all data is gathered and processed in a single hub or cloud, is one of the most popular methods for developing IoT. This method offers simple administration and system scalability, but may have drawbacks in terms of communication speed and dependability, as well as a higher sensitivity to errors.

An IoT central hub or cloud platform would be used in a centralized design, where all data gathered from various IoT devices would be transported and processed there. This method uses IoT devices as data sources, while a central hub handles data collection, management, and analysis. IoT devices connected to centralized hubs and clouds surpassed 7 billion in number in 2020, and this number

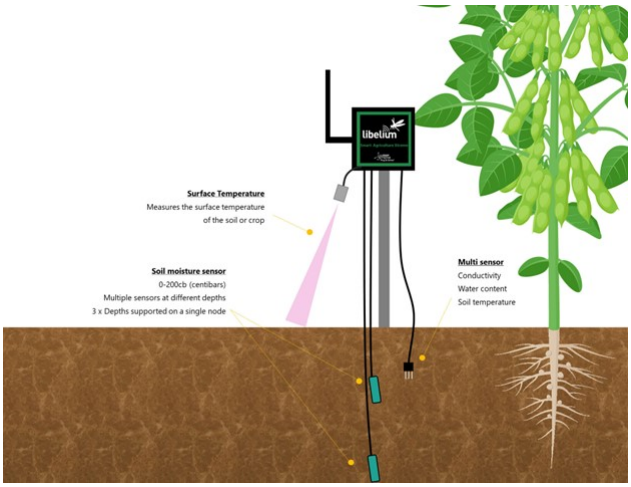

Figure 2.7: IoT soil sensor [16].

is anticipated to increase to 25 billion by 2025. Large amounts of data can be sent to a single hub for processing in centralized IoT systems. For instance, a self-driving car produces about 4 terabytes of data each day.[17][18][19].

One of the benefits of a centralized IoT architecture is its ease of management and scalability. When using a central hub, devices can be easily added or removed from the system, and data processing can be centrally configured and managed. This facilitates the administration and management of the IoT system, especially in the case of a large number of devices. Centralized IoT systems are widely used in smart cities, where hundreds of thousands of devices can be connected to central control systems, monitoring and controlling various aspects of the city's infrastructure.

There are some drawbacks to the centralized architecture. First, network capacity may be an issue when transferring data from IoT devices to a central hub. Delays and network congestion may happen if a lot of devices are transmitting data at once. This is crucial when it comes to large-scale IoT systems that contain a lot of devices.

Data analysis techniques and machine learning may be used in centralized IoT systems to analyse data, allowing you to find patterns, forecast occurrences, and base management choices on the gathered data. A central server or platform makes administration simpler and offers consistent management by enabling you to monitor and control all linked devices from a single location (see Figure 8).

The capacity to centrally store and handle data is another benefit of a centralized design. It is simple to assess and make choices using this data because it is all gathered and kept in one location.

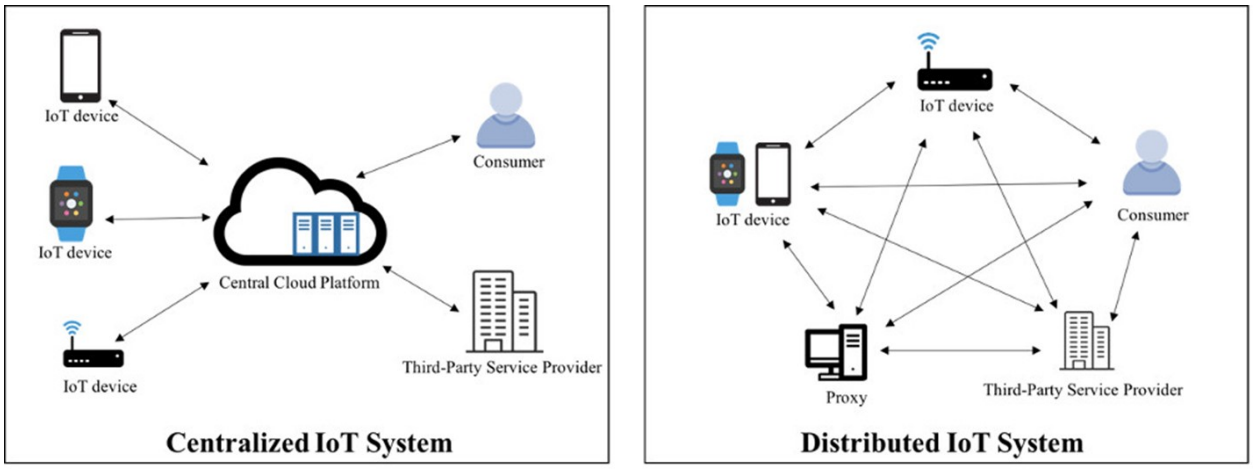

Figure 2.8: Centralized and distributed IoT systems[20].

The centralized IoT architecture is nevertheless widely employed in many sectors, such as smart homes, business, healthcare, and transportation, in spite of these drawbacks. Many companies find it to be an attractive option due to its ease and scalability. However, because to the rising number of devices, alternative solutions such as decentralized systems and edge computing (cloud computing at the network edge) are becoming more and more well-liked.

These methods enable data processing to take place nearer to the data source, lowering latency and enhancing system resilience. Additionally, they offer more adaptability and flexibility, which is crucial for IoT systems functioning in a dynamic environment.

As opposed to a centralized control system, the IoT's decentralized design distributes data processing and decision-making among numerous IoT nodes and devices. With this strategy, each IoT device has some autonomy and decides for itself depending on the data gathered.

Increasing the IoT system's resilience and dependability is one of the key benefits of a decentralized design. The failure of a single node or device does not result in a total loss of system functionality since choices are taken at the device level (cite 21). The remaining nodes can instead carry on independently. Data is

processed in real time at the point of collection in decentralized IoT systems.

The more effective use of network capacity is another benefit of a decentralized design. IoT devices share data processing among themselves, reducing needless network traffic and allowing for the transmission of only the essential data. This lessens network traffic and delay. In the industrial sector, decentralized IoT systems are often employed, allowing IoT devices on production lines to make choices on their own to improve workflows and avoid problems. As a result, manufacturing efficiency is increased and downtime is decreased.

Data privacy also rises in IoT systems with decentralized control. Sensitive information can stay more safe and not be transferred over the network since each device makes its own judgments and analyzes data locally. Devices can employ blockchain technology in decentralized IoT networks to guarantee data security and integrity. For instance, IoT devices may autonomously execute and verify the conditions of contracts in blockchain-based smart contract systems without having to rely on a central participant.

IoT devices must have the capacity to analyze data and make choices, which can call for increased processing power and resources. In order to guarantee the coordination and consistency of the operations of numerous devices, it is also important to establish the proper algorithms and protocols.

The fundamentals of communication in IoT systems are just as crucial as architecture. Numerous communication protocols, including as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, etc., can be utilized depending on the system's needs.

Security is among the most often discussed subjects in the IoT industry. Security concerns are crucial as IoT systems' components analyze and collect a lot of data. The challenges of authentication, encryption, access control, and data protection need to receive extra consideration while analyzing various IoT construction methods(see Figure 2.9).

A crucial component of IoT systems is data management. To yield useful insights, the data must be effectively processed, stored, and evaluated. The usage of databases, cloud platforms, data analysis methods, and machine learning are

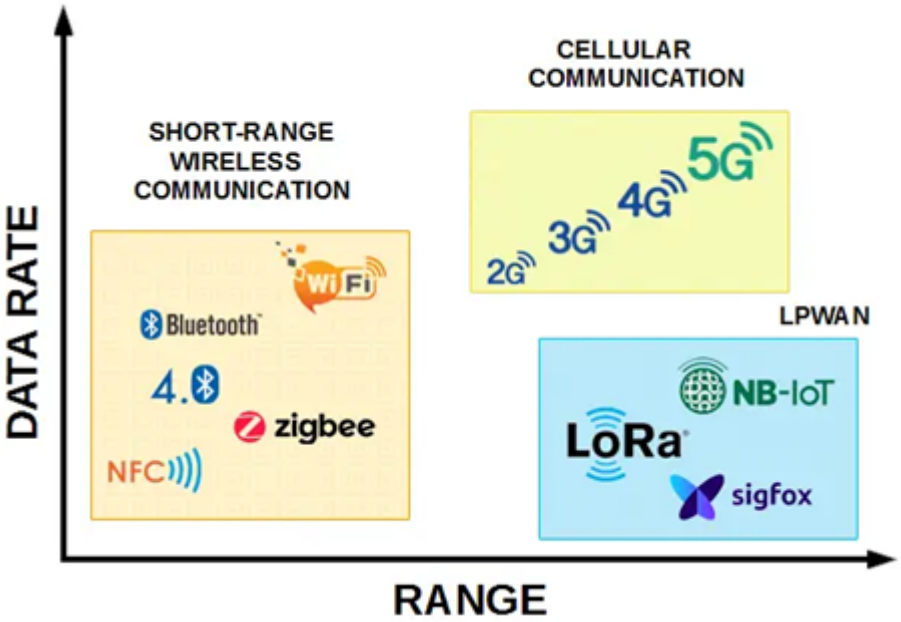

Figure 2.9: Comparing of various wireless connection protocols in IoT [21]

.

just a few examples of data management techniques.

We can detect and assess many areas of design, communication, security, and data management in IoT systems by analyzing existing techniques to developing IoT and their underlying concepts. This offers a foundation for creating a standard IoT ontology and aids in gaining a fundamental knowledge of the guiding concepts behind the IoT.

2.4 Overview of Existing Ontologies

An essential step toward standardization and consistency of interaction amongst IoT devices is the review of current ontologies in the field. In order to successfully share and utilise data between various systems, ontologies provide formal models and semantic descriptions of ideas and connections in the Internet of Things (IoT). The WoT (Web of Things) ontology is another significant IoT ontology. WoT creates a single semantic network out of both real-world items and digital entities.

The goal of WoT is to offer a unified interface for communication between web applications and IoT devices utilizing industry-standard protocols and technolo-

gies like HTTP and REST. To make it simpler to create apps and integrate devices into existing web infrastructure, WoT aims to provide a standardized method of accessing and controlling IoT devices using web interfaces.

To further simplify the integration and exchange of data across devices and services, WoT principles also call for the use of semantic models and ontologies to characterize devices and their capabilities[22]. International standards bodies like the W3C (World Wide Web Consortium) are actively supporting and developing WoT, which helps this idea expand throughout the IoT market.(see Figure 2.10). Smart homes, where diverse equipment like lights, thermostats, and security can be connected and managed by web interfaces and applications, are one of the practical uses of WoT. Industry, which uses IoT devices like sensors, is another sector where WoT is being used.

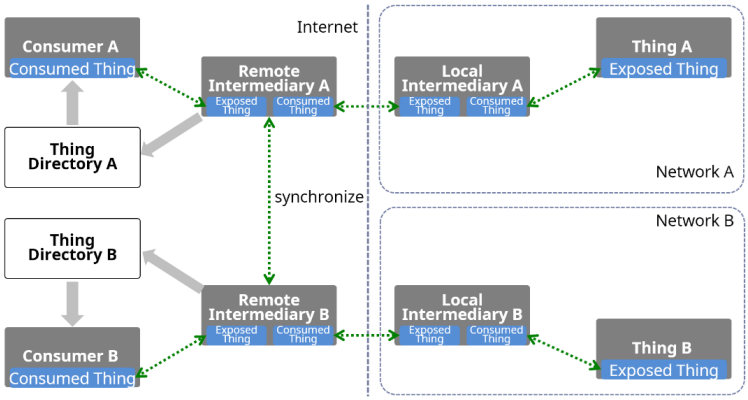

Figure 2.10: WoT architecture[23].

It explains the interfaces and services that are offered, the functioning of the devices, and the relationships between them. WoT offers a single language for controlling and interacting with IoT devices, as well as simplifying their creation and integration. IoT-Lite, among other ontologies, offers a more comprehensive approach for representing abstractions and interactions in IoT(see Figure 2.11).

IoT-Lite defines classes of devices, events, services, and attributes as well as the relationships between them. As a result, standardized data models and communication protocols for the Internet of Things may be created. There are also specific ontologies for certain IoT vertical sectors, such as the Manufacturing Ontology for the manufacturing industry and the Smart Home Ontology for smart

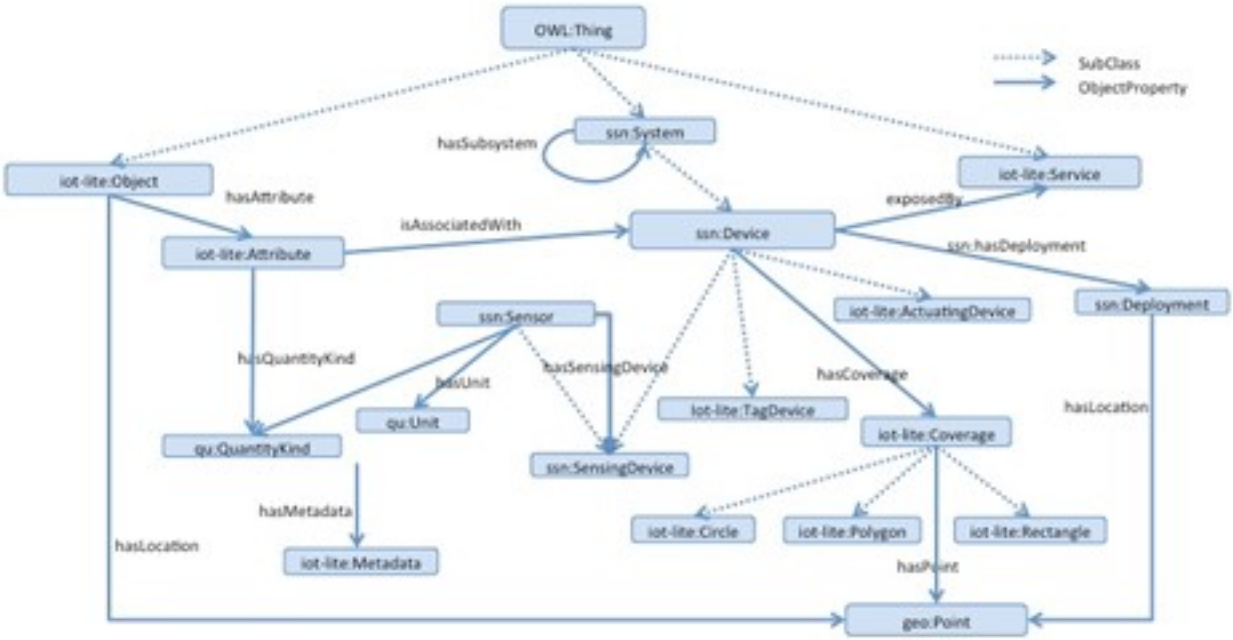

Figure 2.11: IoT-Lite[24].

houses. These ontologies include special classes and relationships that match the characteristics and requirements of specific enterprises.

It aims to provide a simplified and resource-efficient approach to presenting and managing IoT devices, data, and services. The IoT-Lite model focuses on core IoT concepts while minimizing complexity and overhead. One of the key features of IoT-Lite is its emphasis on semantic interoperability. In order to facilitate meaningful and consistent data sharing across various IoT devices and platforms, it makes use of semantic technologies like RDF and ontologies.

It is important to note that there are standard languages and formats for representing ontologies, such as RDF and OWL, which provide interoperability and data exchange between different systems(see Figure 2.12).

Ontology Description Language (OWL-DL) is the foundation of OWL, a formal language that offers features for formalizing and describing complicated domain knowledge. OWL's primary objectives are to give a semantic interpretation of data and to enable automatic knowledge processing by computers(see Figure 2.13).

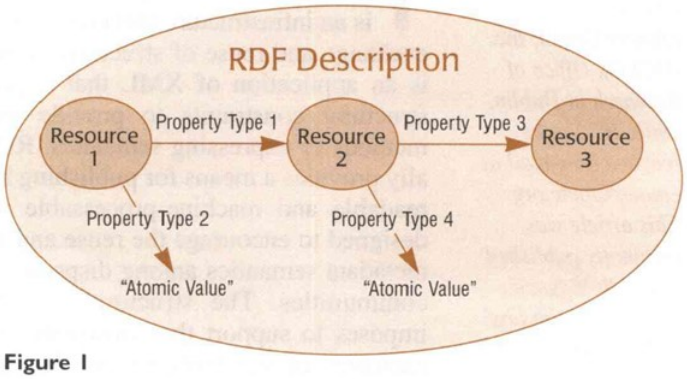

Figure 2.12: RDF description[25].

After reviewing the ontologies used in the IoT space, it can be said that they are crucial for standardizing and coordinating how IoT systems and devices interact. Ontologies offer a shared understanding of the ideas and connections in the Internet of Things, which makes it easier to integrate and communicate data between various apps and devices[27].

RDF is a network model that enables you to specify resources, their attributes, and the connections between them. Through the use of subject, predicate, and object triples, it offers a straightforward and adaptable method to describe knowledge. Links between IoT objects, occasions, and other elements may be established using RDF. On the other hand, OWL is a formal top-level language for ontologies.(see Figure 2.14).

Achieving interoperability and semantic compatibility across various devices and apps is made possible by the usage of OWL and RDF in IoT systems. IoT ideas, connections, and processes may be described and standardized using ontologies supplied in OWL format. The flexibility and extensibility of RDF, in turn, makes it possible to describe and exchange data in the IoT. You may build sophisticated semantic models that let you automatically analyse and combine data from many sources using OWL and RDF. This enhances the interoperability of IoT systems between operators and across platforms. OWL and RDF are widely used in a variety of industries, including smart cities, healthcare, transportation, and manufacturing, where data sharing and interchange across multiple IoT systems and devices is necessary. The development of ontological models for

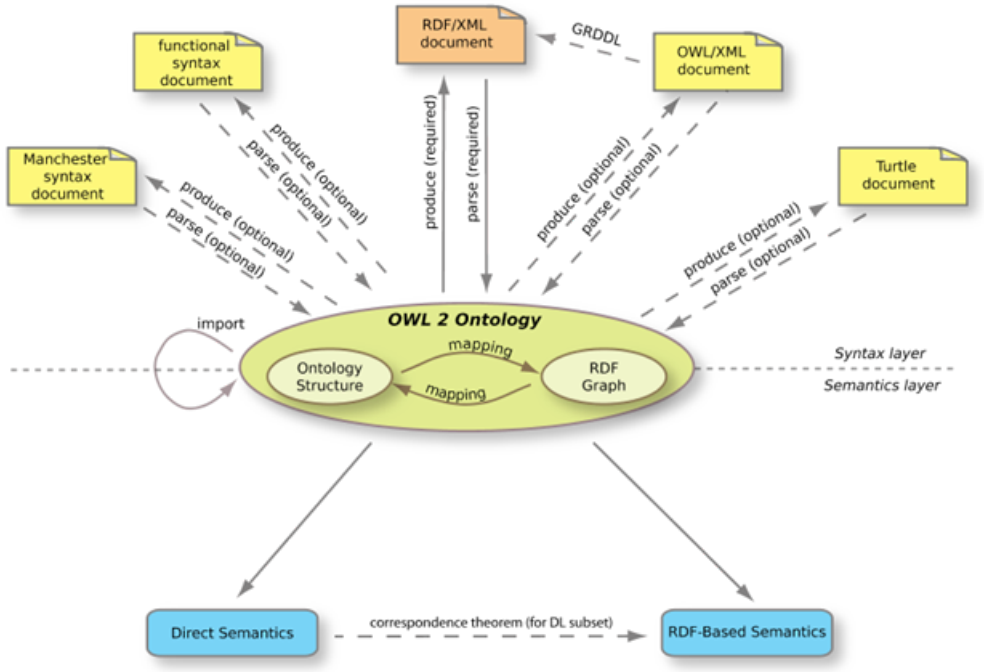

Figure 2.13: OWL ontology[26].

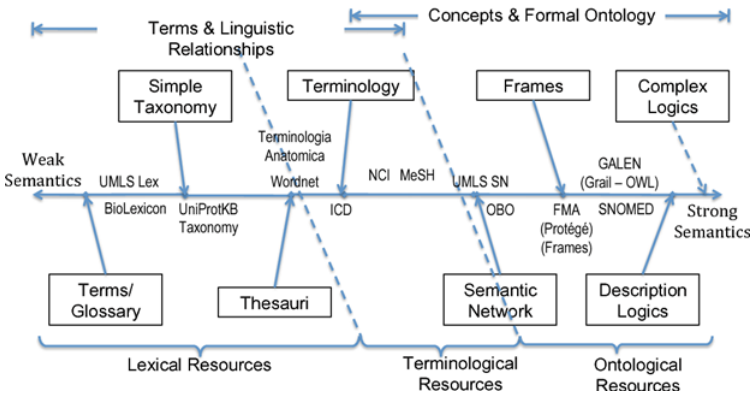

Figure 2.14: Transforming ontologies in the OWL[28].

controlling smart houses is one instance of how OWL and RDF are utilized in IoT. Lights, thermostats, and sensors are just a few examples of the types of devices that may be defined using OWL. With RDF, you can generate triplets that describe particular devices and their states.

Chapter 3

Technologies and tools in the IoT

3.1 Technologies for wireless communication in the IoT

The Internet of Things (IoT) relies heavily on wireless technology to transport data between devices and network infrastructure without the use of traditional connections. Wi-Fi is one of the most widely used wireless communication methods in the Internet of Things. Wi-Fi is perfect for home and business settings with many of devices since it offers fast data transfer rates and extensive coverage.

IoT devices may join existing wireless networks, such as private and public hotspots in homes and offices, thanks to Wi-Fi. Wi-Fi further provides security measures including encryption, allowing safe communication between Internet of Things devices and network infrastructure. (see Figure 3.1).

For IoT devices, this offers extensive coverage and flexible communication. Wi-Fi's high bandwidth is one of its benefits for IoT. This makes it possible to send massive volumes of data, which is crucial for programs that send video, audio, or other media files. To safeguard privacy and stop unwanted access to information, this is crucial. Another benefit of IoT is Wi-Fi's extensive support for standards

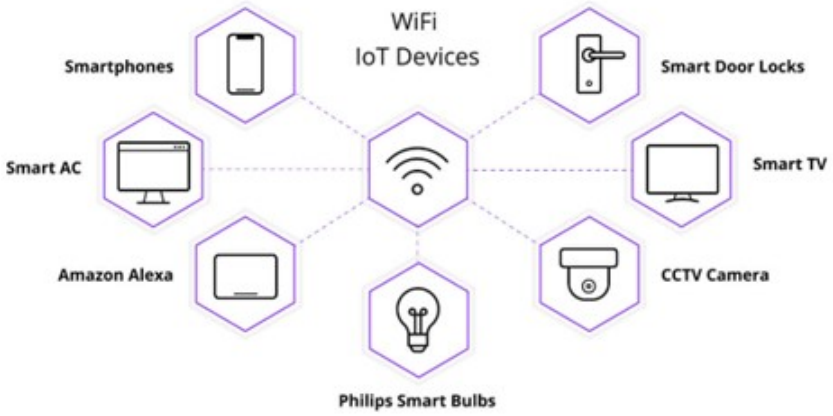

Figure 3.1: An illustration of WiFi use in IoT [29].

and protocols, which enables it to work with most systems and gadgets. Wi-Fi also enables easy configuration and management of connected devices. Wi-Fi 6 delivers improved power efficiency, lower latency, and faster data transmission rates, for example. But there are other limitations to Wi-Fi.

Bluetooth's low power consumption is one of its primary benefits for IoT. IoT devices may run on batteries for a very long period thanks to a specific Bluetooth variation called Bluetooth Low Energy (BLE; see Figure reffig:16). As a result, it is perfect for energy-constrained devices like wearables, sensors, and other low-power IoT gadgets. Additionally, Bluetooth makes it simple and quick to connect gadgets. Users can simply install and manage IoT devices on their network because of this [30].

Support for a number of profiles and services that specify how devices may connect with one another and what functions they can carry out is a key feature of Bluetooth in the Internet of Things.

The device may act as a card in the card emulation mode, enabling access authorisation or payment. Mobile payments are one of the most widely used NFC applications in the IoT. NFC enables contactless payments from mobile devices by merely touching the reader. Users benefit from a quicker and more convenient payment procedure as a result. In smart homes, where it may be used to automate different operations like turning on lights, opening doors, or adjusting

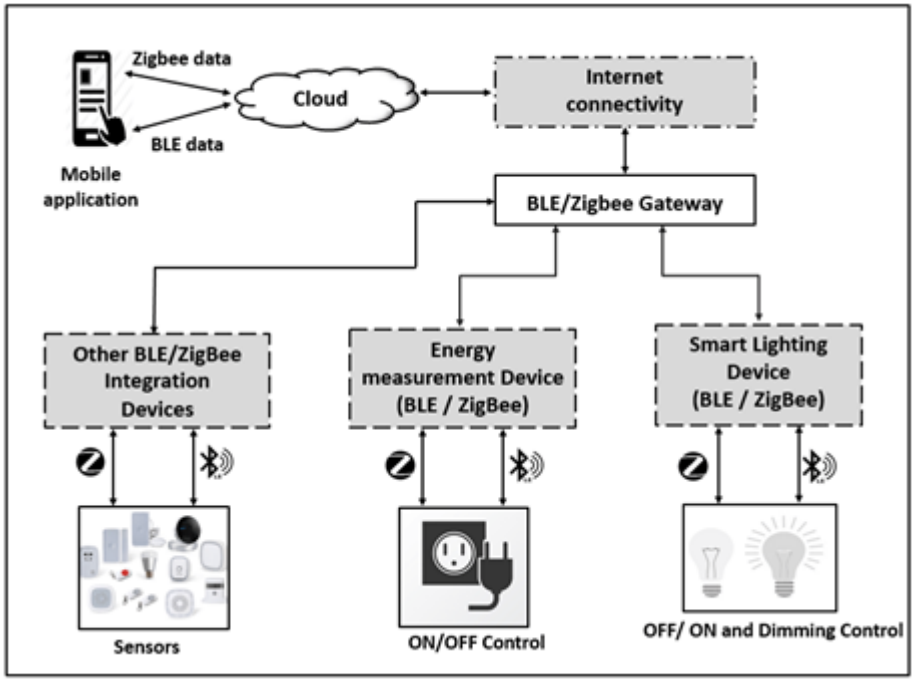

Figure 3.2: Zigbee and BLE embedded IoT technology[31].

the temperature, NFC is also in use.

Technology called LoRaWAN is crucial to the Internet of Things (IoT). It offers the potential to link several IoT devices on the same network and is built to send data over great distances with little power usage. The ISM (Industrial, Scientific and Medical) radio frequency band, which has a communication range of up to several kilometers in urban areas and up to several tens of kilometers in rural regions, is the foundational element of LoRaWAN.

Another significant wireless technology utilized in the Internet of Things (IoT) is Sigfox. It is made to send little quantities of data over vast distances while consuming little power. The distinctive structure and frequency spectrum of Sigfox are incomparable to those of other wireless communication technologies. The Sigfox network's architecture is based on the idea of nodes (nodes) and base stations (base stations). Nodes are Internet of Things (IoT) devices that collect data and transmit it across base stations to a central server or the cloud.

Examples of wireless technologies that operate across local area networks include Wi-Fi, Bluetooth, and Zigbee. On the other hand, devices may communicate over far longer distances via a public communications infrastructure thanks

to cellular standards and LoRaWAN. A specific wireless technology should be chosen for an IoT application based on characteristics including data rate, range, power consumption, and cost.

3.2 IoT sensors and devices

Devices and sensors play a crucial role in IoT systems by gathering data from the physical world and sending it to centralized systems for analysis and decision-making. These gadgets and sensors have various traits and capabilities, and their variety enables you to address a variety of issues. The numerous smart devices used in IoT systems include those used in smart homes, smart cities, industrial systems, medical devices, and more. They are able to communicate with other devices and centralized servers over the internet. Smartphones, tablets, smart watches, smart sensors, smart locks, and smart energy metering sensors are a few examples of such gadgets. (see Figure 3.3).

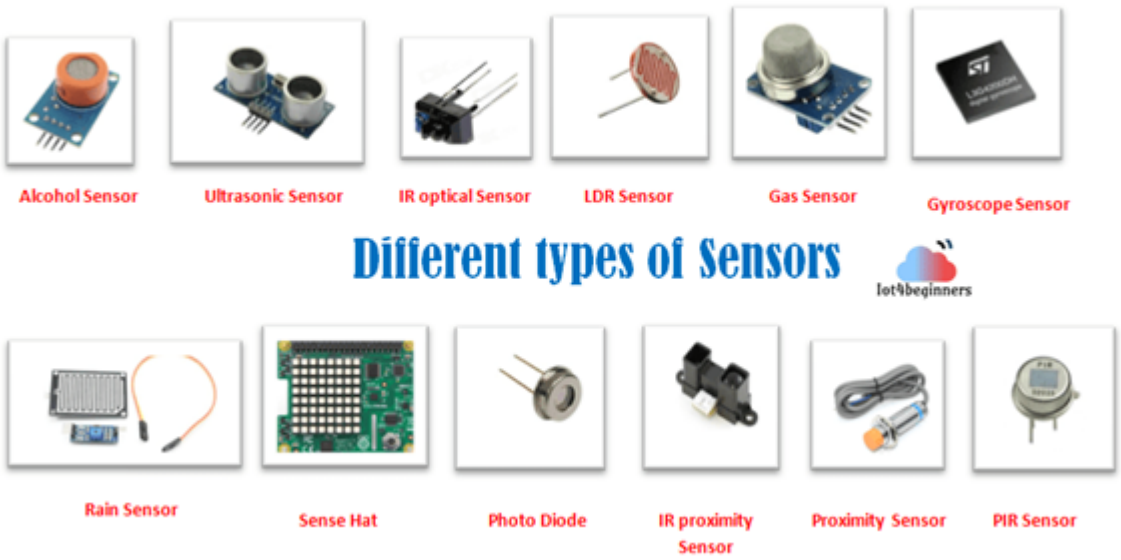

Figure 3.3: Different types of sensors [32].

Sensors are key components of IoT systems as they allow the collection of data about the physical environment. Sensors can measure various parameters such as temperature, humidity, illumination, movement, pressure and others. They can be integrated into devices or installed as separate devices.

Different types of sensors are used by Internet of Things (IoT) systems, which are crucial for gathering information about the real world and diverse items. Then, for use in different IoT applications or for decision-making, this data may be sent and analyzed. Here are a few of the most common sensor types utilized in the Internet of Things:

- Temperature sensors: Determine the environment's or an object's temperature. used in applications where temperature control is crucial, such as smart homes, climate systems, industrial operations, and others.
- Measure the air or soil humidity with humidity sensors. widely applied in climate control, environmental protection, and agriculture.
- Light Sensors: Detect the ambient light level. They are used in smart lighting, security and home automation systems.
- Motion sensors: These devices track the movement or shifting of things. Used frequently in traffic control, smart homes, retail, and security systems.
- Measure the pressure of gases, liquids, or forces with pressure sensors. They are used in the manufacturing of automobiles, meteorology, medical equipment, and other industries.
- Gas sensors: Recognize the presence and level of specific gases in the surrounding atmosphere. used in security, industrial, and air quality control systems.
- Sound sensors: Capture noise and sound waves. They are employed in a variety of applications, including smart homes, medical equipment, and video surveillance systems.
- Sensors that measure acceleration and motion may track the movement of objects. utilized in a variety of applications, including wearable technology, sports trackers, and auto security.
- GPS sensors: Use satellite navigation to find items. They are employed in several sectors, including geolocation, logistics, and auto navigation.
- Measure air quality parameters including pollutant content and pollution

levels using air quality sensors. used extensively in environmental

IoT systems make use of a variety of gadgets that are essential for gathering, processing, and delivering data. To analyze data and carry out specific duties, these devices interact with the environment and objects, gather information, and connect with the network. Here are some of the most common IoT device categories:

- Mobile phones, tablets, laptops, smart watches, and other electronic devices with Internet connectivity are referred to as "smart devices." For managing other IoT devices, smart devices frequently serve as both a central controller and user interface.
- Actuators: Actuators are used to move items or carry out certain tasks. These could include actuators, valves, and other electromechanical devices, as well as LEDs, speakers, and other things that can make sound, light, or movement.
- Small computers or microcontrollers that are integrated into other products or items are known as embedded systems. Specialized tasks are carried out by embedded systems, which also offer access to the network or to other IoT devices.
- Webcams and camcorders are tools used for security, remote monitoring, video surveillance, and other uses. They can feed live video or capture it for subsequent processing and analysis.
- Devices that control different IoT system activities and processes are known as automation devices. It might be, among other things, a transportation management system, a smart home system, or an automated building management system.
- Smart meters and meters are used to measure and track resource use, including that of energy, water, gas, and other resources. They gather information to assess resource efficiency and take the necessary action.
- Robots and autonomous devices are utilized in the Internet of Things (IoT) to automate and complete a variety of activities. They have the ability to

communicate with other devices, interact with the environment, and carry out actions according to data and instructions.

These are only a few of the several kinds of equipment found in IoT systems. The introduction of new devices and the extension of IoT systems' capabilities are both driven by technological advancements and research in this field.

3.3 IoT protocols and standards

IoT networks employ a variety of protocols and standards to make it possible for devices to connect and communicate with one another. The guidelines and formats for data transfer, communications, and device control are set out in these protocols and standards. We'll examine some of the most important IoT protocols and standards in this part.

A protocol called CoAP was created particularly for Internet of Things (IoT) networks and restricted devices. It offers a quick and effective approach for IoT devices to communicate with each other by utilizing UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). CoAP is comparable to the HTTP protocol since it is based on the RESTful architectural philosophy.

The minimal overhead of CoAP, which enables its implementation on devices with limited resources like sensors or microcontrollers, is one of its important characteristics. The protocol is appropriate for IoT devices since it is designed for minimal latency and limited bandwidth. Flow control and dependable message delivery techniques are also supported by CoAP.

The Internet's most popular data transport protocol, HTTP (Hypertext transport Protocol), is also utilized in Internet of Things (IoT) devices. It is possible to send different kinds of data and carry out a number of tasks thanks to HTTP, which enables connection between clients and servers. A request-response protocol is HTTP.

AMQP is a messaging protocol that may be used in Internet of Things (IoT) systems to facilitate asynchronous message processing and communication between devices. AMQP uses message-based protocols to offer efficient and dependable

message passing.

Message delivery acknowledgment, queue management, message flow control, and error handling are just a few of the features that AMQP enables. Since dependability and delivery certainty are crucial needs in complex IoT systems, it is a viable protocol for messaging in those systems.

Extensible communications and Presence Protocol (XMPP) is an open standard for controlling presence and real-time communications. It may be utilized in Internet of Things (IoT) systems as well as chat and instant messaging (IM) systems.

The scalability and dispersion capabilities of the XMPP protocol make it advantageous for IoT. It enables a client-server architecture where devices may act as both clients and servers, processing and delivering messages, respectively.

To offer security in accordance with the demands of a certain system, the protocol allows a range of authentication procedures, including easy passwords, digital certificates, and other techniques. The usage of XMPP in IoT does, however, have certain restrictions. The protocol is not the most resource-efficient, and it could be difficult to implement in devices with limited processing power.

Chapter 4

Analysis and comparison of IoT platforms

4.1 Description of IoT platforms

The Internet of Things (IoT), which enables data exchange and communication between networks and devices, is an essential part of many contemporary industries, from manufacturing to home automation. The significance of IoT is determined by several different factors.

Using IoT platforms is essential in the current information age. Because of this, businesses and organizations are able to create systems that are smarter, more efficient, make the best possible use of their resources, raise production and product quality, and improve user safety and comfort.

More study and development in the IoT field is required due to the need to safeguard data security and privacy, problems with compatibility and interoperability between various systems and devices, and the need to develop standards and protocols that can ensure efficient communication and interaction between devices. Internet of Things (IoT) platform comparison and analysis are required for a number of reasons.

This section examines the twenty most widely used and well-known Internet of

Things (IoT) platforms in the modern information society. When evaluating the platform, a number of aspects are taken into account, such as functionality, performance, scalability, security, adaptability, and cost-effectiveness. The objective of this review is to provide a comprehensive and unbiased assessment of each platform, including all of its features and capabilities. With the help of this research, the reader will be able to get a broad grasp of the various IoT platforms and make an informed choice that suits the requirements of their project or business. The following platforms will be considered throughout the study:

- AWS IoT
- Microsoft Azure IoT
- Google Cloud IoT
- IBM Watson IoT
- Siemens MindSphere
- PTC ThingWorx
- Bosch IoT Suite
- Oracle IoT
- Cisco IoT Cloud Connect
- SAP Leonardo IoT
- GE Predix
- Altair SmartWorks
- Particle IoT
- Ubidots IoT
- Zebra Savanna
- Kaa IoT
- Afero IoT
- Axonize IoT

- Hologram IoT
- Losant IoT

An overview of each platform will be given, along with details on its key traits, potential, architecture, supported protocols, and other crucial elements.

The best platform for creating and overseeing Internet of Things projects is AWS IoT (Amazon Web Services Internet of Things). It provides a vast array of tools and services to help developers create scalable and secure IoT applications.

Advantages:

- Strong IoT data analysis and processing skills.
- Infrastructure for device management and communication that is adaptable and scalable.
- End-to-end IoT solutions are provided through integration with other AWS services.

Disadvantages:

- Using some platform services comes at a considerable expense.
- The requirement for expertise in particular AWS tools and technologies.

Protocols used:

- MQTT
- HTTP
- AMQP

AWS IoT Core, AWS IoT Device Management, AWS IoT Analytics, as well as other platform services, are the programs used.

Applications include those in business, medicine, home automation, and many other fields where it is necessary to gather, manage, and analyze data from Internet of Things (IoT) devices.

A strong platform for creating, delivering, and managing IoT projects is Microsoft Azure IoT. It offers a wide range of tools and services to facilitate the development of creative and scalable IoT applications.

Advantages:

- High level of compatibility and development ease with other Microsoft services and products.
- Strong capabilities for IoT data collection, storage, and analysis.
- Infrastructure for device management and communication that is adaptable and scalable.

Disadvantages:

- Some IoT devices and protocols only receive limited support.
- Integration issues with other cloud platforms.

Protocols used:

- MQTT
- HTTP
- AMQP

Azure IoT Hub, Azure IoT Central, Azure IoT Edge, and other platform services were used as the software.

Industry, healthcare, smart cities, transportation, agriculture, and other sectors where managing and keeping an eye on IoT devices is necessary are application areas.

A platform from Google Cloud called Google Cloud IoT is available for creating and overseeing IoT projects. It offers a range of tools and services for gathering, managing, and processing IoT data.

Advantages:

- High platform flexibility and scalability to handle plenty of IoT data.

- Incorporating other Google Cloud services offers comprehensive functionality and capabilities for creating IoT applications.
- Secure and reliable mechanisms for device management and communication in the IoT network.

Disadvantages:

- Some IoT devices and protocols only receive limited support.
- The platform can only be used to its greatest potential if you completely grasp and master the Google Cloud environment.

Protocols used:

- MQTT
- HTTP

Google Cloud IoT Core, Google Cloud Functions, Google Cloud Pub/Sub, and other Google Cloud services were used.

Industry, smart cities, energy, healthcare, retail, and other sectors where IoT data collection, analysis, and administration are necessary are application areas.

The IBM Watson IoT platform blends the strength of analytics and artificial intelligence (AI) with IoT technologies. The platform offers resources and services for creating and maintaining IoT applications as well as for gathering, processing, and analyzing IoT data.

Advantages:

- Integration with the Watson AI system enables you to use machine learning and data analytics to extract insightful knowledge from the gathered IoT data. A large range of features for collecting, storing, and visualizing data, as well as for managing devices and security, are available for creating and administering IoT applications.
- To enable compatibility and integration with a range of systems and devices, support for numerous protocols and IoT standards is required.

Disadvantages:

- High technical skill level required due to the platform's complexity in setting up and usage.
- Restrictions on flexibility and scalability, particularly when handling significant amounts of IoT data.

Protocols used:

- MQTT
- HTTP
- CoAP
- Other protocols, depending on the specific needs of the project.

IBM Watson IoT Platform, IBM Watson Studio, IBM Watson Machine Learning, as well as additional services and tools made available by IBM, were used as software.

Application areas: Industries such as industry, healthcare, transportation, energy, smart cities, and others where the use of IoT and AI can improve procedures and lead to better decisions.

The open cloud-based IoT platform Siemens MindSphere was created by Siemens. The platform offers resources and assistance for gathering, processing, and utilizing IoT data as well as for creating and deploying applications that rely on it.

Advantages:

- A platform with a focus on industry was created with the demands of industrial businesses and the IIoT (Industrial Internet of Things) sector in mind.
- flexibility and scalability to support many device kinds and protocols while handling massive amounts of IoT data.
- IoT data can be analyzed with rich capability, including capabilities for

machine learning and artificial intelligence.

Disadvantages:

- A certain level of technical competence is required for the platform's setup and configuration because of its complexity.
- Dependence on the cloud computing infrastructure, which may have an impact on the system's availability and dependability when the network is down or the cloud infrastructure has issues.

Protocols used:

- MQTT
- OPC UA
- Other protocols, depending on the specific needs of the project.

IBM Watson IoT Platform, IBM Watson Studio, IBM Watson Machine Learning, as well as additional services and tools made available by IBM, were used as software.

Application areas: Industries such as industry, healthcare, transportation, energy, smart cities, and others where the use of IoT and AI can improve procedures and lead to better decisions.

PTC PTC created the IoT platform called ThingWorx. It offers resources and services for creating, implementing, and maintaining IoT applications. Organizations can use ThingWorx to gather data, analyze it, and then use the results to improve operations and make management choices.

Advantages:

- Easy to use and quick program launch thanks to graphical user interface and pre-built function blocks.
- Powerful data analytics abilities, such as machine learning, predictive analytics, and data visualization.
- Adaptable architecture that enables you to scale the solution to meet chang-

ing needs and incorporate other devices and systems.

Disadvantages:

- Possible functional and scalability restrictions in comparison to some other IoT platforms.
- For intricate and particular use cases, there is some complexity in setup and configuration.

Protocols used:

- MQTT
- HTTP
- OPC UA
- Other protocols, based on the particular requirements of the project.

Software used: ThingWorx Composer, ThingWorx Foundation, ThingWorx Analytics, ThingWorx Industrial Connectivity

Industry, manufacturing, energy, healthcare, smart cities, and other sectors where the use of IoT can improve operations, resource optimization, and efficiency are application areas.

The IoT platform Bosch IoT was created by Bosch. It offers resources and assistance for creating, implementing, and maintaining IoT applications. In order to develop solutions for a number of industries and use cases, Bosch IoT offers a wide range of features and integrations.

Advantages:

- Bosch products are known for their high reliability and safety thanks to a significant focus on these two factors.
- The platform's scalability and adaptability to various needs and project sizes.
- A wide range of functions and resources, including event management, device administration, data collection, and analysis.

- Integration with other Bosch services and products makes it simpler to utilize and manage different systems and devices.

Disadvantages:

- Compared to some other IoT systems, limited flexibility and extension.
- A preference for Bosch goods and solutions, which could restrict the selection and integration of hardware and software from other manufacturers.
- For some users, setup and setting may be challenging.

Protocols used:

- MQTT
- HTTP
- OSGi
- Other protocols, depending on the specific needs of the project.

Bosch IoT Suite, Bosch IoT Gateway Software, Bosch IoT Insights, Bosch IoT Things, and Bosch IoT Remote Manager are among the applications used.

Application areas include those in industry, transportation, energy, healthcare, and other sectors where IoT implementation can boost productivity and streamline procedures.

An IoT platform created by Oracle is called Oracle IoT. It offers resources and assistance for creating, implementing, and monitoring IoT applications.

Advantages:

- Oracle Cloud infrastructure provides scalability and flexibility.
- Advanced analytics for IoT data
- Support for open standards and protocols to facilitate simple system integration

Disadvantages:

- High implementation and usage costs

- Limited compatibility with some devices and protocols
- Dependence on Oracle Cloud infrastructure.

Protocols used:

- MQTT
- HTTP
- CoAP
- Other protocols, depending on the specific needs of the project.

Oracle IoT develops and manages IoT applications using its own software suite, which also includes Oracle IoT Cloud Service and Oracle IoT Applications.

Application areas: It can be utilized to enhance performance, maximize resources, and develop cutting-edge IoT solutions in a variety of industries, including manufacturing, energy, healthcare, and transportation.

Cisco offers an IoT platform called Cisco IoT Cloud Connect. It is intended to link and control IoT devices through the cloud.

Advantages:

- High scalability and flexibility provided by using the Cisco Cloud cloud infrastructure
- Advanced IoT data analytics
- Wide range of analytical tools and machine learning capabilities.

Disadvantages:

- Limited compatibility with some devices and protocols
- Dependence on Cisco Cloud infrastructure.

Protocols used:

- MQTT
- HTTP

- CoAP
- Other protocols, depending on the specific needs of the project.

Software used: Based on Cisco's own creation, Cisco IoT Cloud Connect offers IoT device administration, data analytics, visualization tools, and more.

Industries, such as manufacturing, transportation, energy, and smart cities, are among the application sectors.

A platform for IoT that SAP offers is called SAP Leonardo IoT. It is intended for the development and integration of IoT solutions, data analysis, and the creation of novel applications.

Advantages:

- High scalability and flexibility
- Advanced IoT data analytics
- Wide range of analytical tools and machine learning capabilities.

Disadvantages:

- Limited compatibility with some devices and protocols
- The need for specialized knowledge and skills to work with the SAP Leonardo IoT platform.

Protocols used:

- MQTT
- HTTP
- CoAP
- Other protocols, depending on the specific needs of the project.

Used software includes SAP HANA for data analysis and SAP Cloud Platform for creating and deploying Internet of Things applications. SAP Leonardo IoT is built on these SAP software solutions.

Application areas: It can be used to increase performance, streamline operations, and create new value with IoT data in a variety of industries, including manufacturing, transportation, energy, healthcare, and smart cities.

An IoT platform called GE Predix was created by General Electric. It offers resources and assistance for creating, implementing, and monitoring IoT applications.

Advantages:

- High scalability and flexibility
- Advanced IoT data analytics
- Wide range of analytical tools and machine learning capabilities.

Disadvantages:

- Limited compatibility with some devices and protocols
- High entry threshold for some users due to the complexity of setting up and configuring the platform.

Protocols used:

- MQTT
- HTTP
- Other protocols, depending on the specific needs of the project.

Software used: GE Predix uses tools and services created by the firm for data processing, analytics, device management, and other features. It is built on GE cloud technology.

Industries such as energy, industry, transportation, and healthcare are among the application sectors. It can be used to streamline production procedures, keep an eye on and maintain machinery, analyze data, and base decisions on IoT data.

An IoT platform called Particle IoT offers resources for creating and overseeing IoT gadgets.

Advantages:

- Ease of use and configuration, scalability, cloud integration and management of IoT devices
- Ready-made libraries and templates for application development.

Disadvantages:

- Limited analytical capabilities
- Possible limitations in customization and extensibility.

Protocols used:

- MQTT
- HTTP (Hypertext Transfer Protocol)
- Other protocols, depending on the specific needs of the project.

Software used: To assist developers in creating applications for IoT devices, Particle IoT offers a range of development tools, including online IDEs, libraries, SDKs, and APIs.

Application areas: Sectors where IoT devices are used to monitor, control, and gather data, such as agriculture, healthcare, smart homes, and others.

IoT platform Ubidots IoT offers tools for gathering, viewing, and analyzing data from IoT devices. Advantages:

- IoT device administration, scalability, cloud integration, and ease of use and configuration
- Flexible and customizable interface

Disadvantages:

- Limited analytical capabilities
- Possible limitations in customization and extensibility.

Protocols used:

- MQTT
- HTTP
- TCP
- Other protocols, depending on the specific needs of the project.

Software used: To assist developers in integrating and interacting with the platform, Ubidots IoT offers a set of development tools, including APIs, SDKs, and libraries.

The Ubidots IoT platform is utilized in a variety of sectors, including industrial, energy, agriculture, smart cities, and others, where IoT devices are used to monitor, regulate, and improve processes.

An IoT platform called Zebra Savanna was created by Zebra Technologies. It offers services and solutions for gathering, processing, and utilising data from IoT devices.

Advantages:

- Integration with Zebra devices, wide range of functions for data collection and analysis
- Scalability and flexibility

Disadvantages:

- Limited analytical capabilities
- Possible limitations in integration with third-party systems

Protocols used:

- MQTT
- HTTP
- Other protocols, depending on the specific needs of the project.

Software used: A selection of development and analytics tools, such as APIs and SDKs, are available through the Zebra Savanna Platform.

Zebra Savanna has applications across a range of sectors, including retail, logistics, manufacturing, healthcare, and others that employ IoT devices to track, monitor, and improve business operations.

IoT application development and management can be done using the open and adaptable Kaa IoT Platform. Advantages:

- A wide range of functionality, flexibility and customization, support for various communication protocols
- The ability to develop in various programming languages.

Disadvantages:

- Limited analytical capabilities
- Possible limitations in integration with third-party systems

Protocols used:

- MQTT
- HTTP
- Other protocols, depending on the specific needs of the project.

Software used: The Kaa platform makes it simple to construct and maintain IoT applications by providing a variety of modules and development tools like SDKs, APIs, databases, and analytics tools.

Applications: Kaa is used in a wide range of sectors, such as manufacturing, energy, healthcare, transportation, and other ones that call for the creation and administration of sophisticated IoT solutions.

Afero provides a cutting-edge platform called the Afero IoT Platform. It offers businesses and developers all the capabilities they need to build and manage IoT applications. integrating user-friendliness, dependability, and support for a variety of communication protocols.

Advantages:

- A wide range of functionality, flexibility and customization, support for various communication protocols
- The ability to develop in various programming languages.

Disadvantages:

- Limited analytical capabilities
- Possible limitations in integration with third-party systems

Protocols used:

- MQTT
- HTTP
- Other protocols, depending on the specific needs of the project.

Software used: For creating and overseeing IoT applications, the Afero platform provides development tools, data analytics, device management, and cloud infrastructure.

Afero has uses in a range of sectors, including smart homes, retail, healthcare, automation, and others that call for the development and administration of connected devices and sensors.

In order to determine the features, functionality, and application of 20 IoT platforms in different industries, an analysis and comparison of these platforms was done as part of this dissertation. The analysis' findings are displayed as tables that include a great deal of information about each platform. The tables containing comparative statistics on IoT platforms have been relocated to the appendix of this dissertation due to the volume of data and the space needed for their presentation (see Appendix A). This choice was made to maintain the logical flow of the primary content and to guarantee its reading and comprehension. The reader can find complete tables with thorough information about each of the investigated platforms in the dissertation's appendix.

Chapter 5

Building a common ontology of the IoT

5.1 Description of the developed general ontology and its structure

The generic ontology that has been created and is used as the foundation for semantic modeling and data interpretation in the context of the Internet of Things (IoT) is described in this section. In order to organize knowledge and create connections between diverse ideas in IoT systems, an ontology was established.

Creating a formal model that offers a uniform representation and consistency of ideas and connections inside the IoT is the aim of building a common ontology. You may group together and categorize IoT platforms, devices, protocols, data formats, and services into a single category using ontology.

The ontology given comprises a number of classes and subclasses that correspond to the fundamental IoT concepts. The iot:Sensor, iot:Actuator, and iot:Gateway classes, for instance, represent several IoT device kinds. The iot:Networkin and iot:CommunicationProtocolIoT communication and networking protocols are defined by protocol classes.

The classes iot:DataSchema, iot:DataModel, and iot:DataFormat, which deal

with the description and structure of data gathered and communicated by IoT devices, are also defined in the ontology. The many kinds of IoT services that may be offered within a particular scope are represented by the iot:WebOfThings and iot:IoTApplication classes.

The iot:IoTPlatform class, a broad category for IoT platforms, is also included in the ontology. It provides an overview of the resources and infrastructure available for creating, deploying, and administering IoT applications. Each class and subclass will be thoroughly discussed in this section, along with its attributes and connections. This will make it possible to comprehend the ontology's structure and organization as well as how it applies to different IoT systems.

There are several benefits to using a standard IoT ontology. First, it encourages consistent idea representation across various IoT systems, which makes it easier for them to integrate and communicate. Second, by offering formal models and organized data schemas, it makes IoT application development and data management simpler. Thirdly, it aids in the comprehension and sharing of information in the IoT sector, helping to standardize vocabulary and ideas.

It's important to recognize some of this generic ontology's limits. It might not account for all the unique characteristics and specifics of various IoT systems and objects. Additionally, the right categorization and arrangement of concepts, which calls for suitable analysis and modeling, may determine its efficacy and application.

The ontology's classes and subclasses will be described in depth later on in the section, along with examples of how they might be used in various IoT situations. This will make it possible to portray the created generic IoT ontology's structure and capabilities in a way that is more thorough and accurate. Classes and subclasses that explain the key ideas and connections in the context of the Internet of Things (IoT) are included in the created generic ontology. Below is a description of this ontology's structure.

Classes of IoT devices:

- iot:IoTDevice: Describes a generic class for all IoT devices.

- iot:Sensor: A subclass of iot:IoTDevice that represents sensor devices.
- iot:Actuator: A subclass of iot:IoTDevice that represents actuators.
- iot:Gateway: A subclass of iot:IoTDevice that represents gateways for IoT network communications.

Protocol classes:

- iot:Protocol: Generic class for all protocol types.
- iot:CommunicationProtocol: A subclass of iot:Protocol that represents communication protocols.
- iot:NetworkingProtocol: A subclass of iot:Protocol that represents networking protocols.

Data format classes:

- iot:DataFormat: Generic class for all types of data formats.
- iot:DataSchema: A subclass of iot:DataFormat that represents data schemas.
- iot:DataModel: A subclass of iot:DataFormat that represents data models.

Service classes:

- iot:Service: Generic class for all service types.
- iot:WebOfThings: A subclass of iot:Service that represents services based on the Web of Things concept.
- iot:IoTApplication: A subclass of iot:Service that represents IoT applications.

IoT platform class:

- iot:IoTPlatform: Describes a class for IoT platforms.

In the context of the Internet of Things (IoT), the generated generic ontology is a formal model that explains the key ideas and connections. It acts as a framework for knowledge representation and semantic analysis of information pertaining to IoT platforms, devices, protocols, data formats, and services (see Figure 5.1).

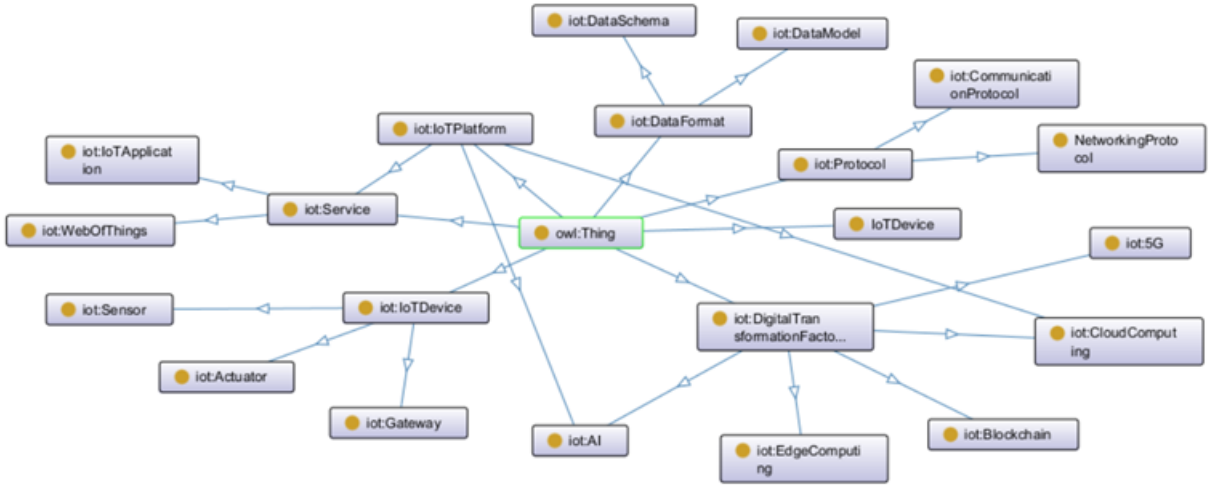

Figure 5.1: Ontology for the Internet of Things

The ontology contains classes and subclasses that define various IoT device kinds. For instance, the iot:Gateway class represents IoT network communication gateways, the iot:Actuator class represents actuators, and the iot:Sensor class represents sensor devices. This enables the functional classification and organization of devices. The ontology also specifies protocol classes that explain the many kinds of network protocols and communication protocols used in the Internet of Things. For instance, the iot:NetworkingProtocol class relates to network protocols like TCP/IP, whereas the iot:CommunicationProtocol class represents communication protocols like Wi-Fi, Bluetooth Low Energy (BLE), and Zigbee.

Classifying data formats is a crucial component of ontology. The iot:DataSchema class refers to data schemas that specify the format and categories of data that IoT devices gather and communicate. The data models that provide the semantics and connections between various data kinds are represented by the iot:DataModel class. The ontology also specifies service classes that describe various IoT services, such as iot:WebOfThings and iot:IoTApplication. For instance, the term "iot:WebOfThings" refers to online of Things-based services that enable device interaction and control via online interfaces. IoT platforms fall under the umbrella of the iot:IoTPlatform class. Platforms that offer the necessary tools and infrastructure for creating, deploying, and maintaining IoT applications fall under this category.

Ontology is built on the fundamental ideas of semantic modeling, which enable knowledge organization and the creation of connections between concepts. It may be used to design IoT applications, build semantic data models, and assist the integration of different IoT systems and gadgets. The implementation of such a common ontology in the IoT environment can streamline the creation and administration of intricate systems, make data sharing easier, and standardize language. The IoT's elements and interactions may be described and understood using a formal and organized method provided by ontology, which improves the effectiveness and interoperability of systems in this field.

Chapter 6

Conclusions and future work

6.1 Discussion

A formal model that unifies ideas and connections found in Internet of Things (IoT) systems was created as a result of the study's work. This has numerous substantial practical ramifications and contributes significantly to the growth of the IoT industry.

Initial guidelines and standards for the consistent display of information within the IoT are established by the created generic ontology of the IoT. This enhances the interoperability and interoperability of various IoT systems since they may communicate using a common language and conceptual framework. This is particularly crucial in the context of the growth of sizable IoT ecosystems, where a variety of platforms and devices must collaborate.

6.2 Conclusions

We created a generic ontology for the Internet of Things (IoT) as part of the project, which is a formal model that organizes ideas and connections in IoT systems. The study's findings led to the following conclusions:

- The dissertation's hypothesis, which suggested the potential for developing a common ontology of IoT, is verified. An organized and consistent repre-

sentation of concepts and connections in the IoT sphere is provided by the created ontology.

- Utilizing the created universal ontology for the Internet of Things is very significant and useful. It encourages consistent idea representation and data management, makes application development and data administration easier, and fosters knowledge transfer and interoperability across various IoT systems.
- The findings are broadly applicable to many fields where IoT technology are employed. The invention of IoT standards and protocols, the integration of multiple IoT platforms and devices, and the design and development of IoT systems may all make use of the ontology.

As a result, the created generic ontology of IoT is a crucial tool for standardizing and presenting concepts in the Internet of Things domain consistently.

6.3 Future work

Several characteristics of the established IoT overall ontology should be taken into consideration in future study.

First, by including new classes, subclasses, and connections, the ontology may be improved and expanded upon. IoT is a broad field with numerous devices, protocols, and services, and by considering the various situations of their use, the ontology's utility and applicability may be greatly increased.

The produced ontology has to be tested in practice and evaluated using actual IoT projects, which is the second step. Its efficacy, usefulness, and potential for improvement will be determined by this. It is possible to get useful outcomes and suggestions by incorporating ontology into certain IoT systems and assessing how it affects development, data management, and interaction.

The third area of future development is the incorporation of the created universal ontology of IoT with other techniques and methodologies, such data analysis and machine learning. This will make it possible to use more complicated algo-

rithms for knowledge extraction and prediction and make deeper use of the data collected from IoT devices.

Bibliography

[1] G. Pradyumna, B. Omkar, and B. Sagar. Introduction to iot. International Advanced Research Journal in Science, Engineering and Technology, 5(1): 1–3, 2018.

[2] Injong Lee and Kyungho Lee. The internet of things (iot): Applications, investments, and challenges for enterprises. Business Horizons, 58(4):431–440, 2015.

[3] Eleonora Borgia. The internet of things vision: Key features, applications and open issues. Computer Communications, 54:1–31, 2014.

[4] Brian Russell, Drew Van Duren, and John Sammons. Practical Internet of Things Security. Syngress, 2018.

[5] Maciej Kranz. Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry. Wiley, 2016.

[6] Inseok Janggwan, Kim Seonghoon, and Kim Daeyoung. Iot mashup as a service: cloud-based mashup service for the internet of things. In Proceedings of IEEE International Conference on Services Computing (SCC), pages 462–469, 2013.

[7] Isabelle Ganche, Zhe Ji, and Máirtín O'Droma. A generic iot architecture for smart cities. In Proceedings of 25th IET Irish Signals & Systems Conference, pages 196–199, 2013.

[8] Yan Zhang, Yan Shen, Hua Wang, Jun Yong, and Xiaohong Jiang. On secure wireless communications for iot under eavesdropper collusion. IEEE Internet of Things Journal, 13(3):1281–1293, 2016.

[9] H.Z. Yuchen Yang, Longfei Wu, Guisheng Yin, and Lijie Li. A survey on security and privacy issues in internet-of-things. In 2015 10th International Conference on Internet Technology and Secured Transactions, volume 4, pages 202–207, 2015.

[10] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5):1125–1142, 2017.

[11] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally. Internet of things (iot): Research. IEEE Internet of Things Journal, 5(3):1637–1647, 2018.

[12] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.R. Choo. A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet of Things Journal, 5(3):1606–1615, 2018.

[13] T.M. Fernández-Caramés and P. Fraga-Lamas. A review on the use of blockchain for the internet of things. IEEE Access, 6:32979–33001, 2018.

[14] Ahmad Gharaibeh, Mohammad A. Salahuddin, Saeed J. Hussini, Abdallah Khreishah, Ibrahim Khalil, Mohsen Guizani, and Ala Al-Fuqaha. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials, 19(4):2456–2501, 4th Quart. 2017.

[15] Ramesh K. Barik, Hemant Dubey, and Kunal Mankodiya. Soa-fog: Secure service-oriented edge computing architecture for smart health big data analytics. In Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP), pages 477–481, Nov. 2017.

[16] Hemant Dubey, Anand Monteiro, Nirvana Constant, Mehran Abtahi, Deepak Borthakur, Lukas Mahler, Yijun Sun, Qing Yang, Usman Akbar, and Kunal Mankodiya. Fog computing in medical Internet-of-Things: Architecture, implementation, and applications, pages 281–321. Springer, 2017.

[17] Dauren Rakhmetolla and Gulfarida Tulemissova. Conceptual approach to the formation of the digital twin of the destination earth (first glance). In 2023

17th International Conference on Electronics Computer and Computation (ICECCO), pages 1–6. IEEE, 2023.

[18] Debiao He, Sammy Chan, and Mohsen Guizani. Security in the internet of things supported by mobile edge computing. IEEE Commun. Mag., 56(8): 56–61, Aug. 2018.

[19] Muhammad Naveed Aman, Kee Chaing Chua, and Biplab Sikdar. Mutual authentication in iot systems using physical unclonable functions. IEEE Internet Things J., 4(5):1327–1340, Oct. 2017.

[20] Meshal Alrowaily and Zhi Lu. Secure edge computing in iot systems: Review and case studies. In Proc. IEEE/ACM Symp. Edge Comput. (SEC), pages 440–444, Oct. 2018.

[21] Jie Zhou, Zhenfu Cao, Xiaodong Dong, and Xiaolin Lin. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. IEEE Wireless Commun., 22(2):136–144, Apr. 2015.

[22] Dave Raggett. The web of things: Challenges and opportunities. Computer, 48(5):26–32, 2015.

[23] Yong Shi, Guanyu Li, Xiaofang Zhou, and Xiaoyu Zhang. Sensor ontology building in semantic sensor web. In Internet of Things, pages 277–284. Springer, 2012.

[24] Dominique Guinard, Vlad Trifa, Stamatis Karnouskos, Patrik Spiess, and Davide Savio. Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services. IEEE Transactions on Services Computing, 3(3):223–235, 2010.

[25] Yiran Li and Roy T. Fielding. Iot-lite: A lightweight semantic model for the internet of things. IEEE Internet of Things Journal, 4(6):1836–1847, 2017.

[26] Holger Neuhaus and Michael Compton. The semantic sensor network ontology. In AGILE Workshop on Challenges in Geospatial Data Harmonisation, pages 1–33, 2009.

[27] Tiago Teixeira, Salima Hachem, Valérie Issarny, and Nikolaos Georgantas.

Service oriented middleware for the internet of things: A perspective. In Servicewave, October 2011. To appear.

[28] Dominique D. Guinard and Vlad Trifa. Towards the web of things: Web mashups for embedded devices. In Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences), Madrid, Spain, April 2009.

[29] Shahid Ehsan and Bechir Hamdaoui. A survey on energy-efficient routing techniques with qos assurances for wireless multimedia sensor networks. IEEE Communications Surveys & Tutorials, 14(2):265–278, 2012.

[30] Fan Wang and Jing Liu. Networked wireless sensor data collection: issues, challenges, and approaches. IEEE Communications Surveys & Tutorials, 13 (4):673–687, 2011.

[31] Flavia Delicato, Felipe Protti, Luci Pirmez, and Jose de Rezende. An efficient heuristic for selecting active nodes in wireless sensor networks. Computer Networks, 50(18):3701–3720, 2006.

[32] Abdulrahman E Al-Fagih, Fadi M Al-Turjman, Waleed M Alsalih, and Hossam S Hassanein. A priced public sensing framework for heterogeneous iot architectures. IEEE Transactions on Emerging Topics in Computing, 1(1): 133–147, 2013.

Appendix A

Appendix A

A.1 Comparison tables

IoT Platforms	Advantages	Disadvantages	RTOS Cloud	Protocols	Application Area	Using Frequency	Pricing
AWS IoT	Highly scalable, wide range of services	Steep learning curve, complex pricing model	FreeRTOS,	MQTT, HTTP, WebSocket, LoRaWAN, Sigfox	Industrial automation, smart homes, healthcare, etc.	High	Pay-as-you-go
Microsoft Azure IoT	Integrates well with other Microsoft services	Limited support for nonMicrosoft platforms	Azure RTOS, ThreadX,	MQTT, AMQP, HTTP, WebSocket, OPC UA	Predictive maintenance, remote monitoring, etc.	High	Pay-as-you-go
Google Cloud IoT	Large ecosystem of tools and services	Limited device management capabilities	Zephyr, FreeRTOS	MQTT, HTTP, WebSocket, CoAP	Asset tracking, smart cities, etc.	High	Pay-as-you-go
IBM Watson IoT	AI and analytics capabilities	Limited support for smaller businesses	FreeRTOS, mbed OS	MQTT, HTTP, CoAP, AMQP, WebSocket	Predictive maintenance, quality control, etc.	Medium	Pay-as-you-go
Siemens MindSphere	Open and modular architecture	Limited support for nonSiemens hardware	FreeRTOS, Yocto	MQTT, HTTP, OPC UA	Predictive maintenance, quality control, etc.	Low	Subscription-based

Figure A.1: IoT platforms comparison table 1

PTC ThingWorx	Large developer community, customizable	Expensive	FreeRTOS, VxWorks	MQTT, HTTP, CoAP, WebSocket	Remote monitoring, predictive maintenance, etc.	Medium	Subscription-based
Bosch IoT Suite	Secure, scalable, and flexible	Limited support for nonBosch hardware	FreeRTOS, VxWorks	MQTT, HTTP, AMQP, CoAP, DDS, OPC UA	Industrial automation, smart homes, etc.	Medium	Pay-as-you-go
Oracle IoT	Integrated with other Oracle services	Limited support for nonOracle platforms	FreeRTOS, Zephyr	MQTT, HTTP, CoAP, WebSocket,	Smart homes, transportation, etc.	Low	Pay-as-you-go

Figure A.2: IoT platforms comparison table 2

IoT Platforms	Advantages	Disadvantages	RTOS Cloud	Protocols	Application Area	Using Frequency	Pricing
				REST, OPC UA			
Cisco IoT Cloud Connect	Robust security features, integrates with other Cisco products	Limited device management capabilities	FreeRTOS, VxWorks	MQTT, CoAP, AMQP, HTTP, WebSocket	Industrial automation, healthcare, etc.	Low	Pay-as-you-go
SAP Leonardo IoT	Integrated with other SAP services	Limited support for nonSAP platforms	FreeRTOS, mbed OS	MQTT, HTTP, CoAP, AMQP, WebSocket	Predictive maintenance, asset tracking, etc.	Medium	Pay-as-you-go
GE Predix	Large ecosystem of tools and services	Limited support for nonGE hardware	FreeRTOS, VxWorks	MQTT, HTTP, WebSocket, DDS, OPC UA, CoAP	Asset monitoring, predictive maintenance, etc.	Low	Pay-as-you-go
Altair SmartWorks	Customizable and easytouse	Limited support for nonAltair hardware	FreeRTOS, VxWorks	MQTT, HTTP, WebSocket, OPC UA, REST	Predictive maintenance, industrial automation, etc.	Low	Subscription-based

Figure A.3: IoT platforms comparison table 3

GE Predix	Large ecosystem of tools and services	Limited support for nonGE hardware	FreeRTOS, VxWorks	MQTT, HTTP, WebSocket, DDS, OPC UA, CoAP	Asset monitoring, predictive maintenance, etc.	Low	Pay-as-you-go
Altair SmartWorks	Customizable and easytouse	Limited support for nonAltair hardware	FreeRTOS, VxWorks	MQTT, HTTP, WebSocket, OPC UA, REST	Predictive maintenance, industrial automation, etc.	Low	Subscription-based
Particle IoT	Simple and easytouse, supports multiple platforms	Limited scalability	FreeRTOS, Particle OS	MQTT, HTTP, WebSocket, CoAP, Particle Protocol	Industrial automation, smart homes, etc.	High	Pay-as-you-go
Ubidots IoT Application Enablement Platform	Easytouse draganddrop interface, supports multiple platforms	Limited data analytics capabilities	FreeRTOS	MQTT, HTTP, TCP, UDP, CoAP	Remote monitoring, asset tracking, etc.	Medium	Subscription-based
Zebra Savanna	Robust data analytics capabilities, integrated	Limited support for nonZebra hardware	FreeRTOS	MQTT, HTTP, WebSocket, Zebra	Asset tracking, supply chain	Low	Pay-as-you-go

Figure A.4: IoT platforms comparison table 4

Kaa IoT Platform	Opensource, customizable, and scalable	Limited support for nonKaa hardware	FreeRTOS, Zephyr	MQTT, HTTP, WebSocket, CoAP, DDS, MQTTSN	Industrial automation, smart homes, etc.	Low	Subscription-based
Afero IoT Platform	Secure and scalable, supports multiple platforms	Limited support for nonAfero hardware	FreeRTOS	MQTT, HTTP, WebSocket, BLE, WiFi	Smart homes, healthcare, etc.	Low	Subscription-based
Axonize IoT Platform	Customizable and flexible, integrates with other Axonize products	Limited support for nonAxonize hardware	FreeRTOS	MQTT, HTTP, WebSocket, CoAP, Modbus TCP	Predictive maintenance, industrial automation, etc.	Low	Pay-as-you-go
Hologram IoT Platform	Easytouse and affordable	Limited data analytics capabilities	FreeRTOS	MQTT, HTTP, CoAP, UDP, TCP, Hologram Protocol	Industrial automation, smart homes, etc.	High	Subscription-based

Figure A.5: IoT platforms comparison table 5

IoT Platform	Features of Architecture	Types of Devices Used	Used Software	Area of Use
AWS IoT	Device management, data collection and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	AWS IoT Core	Industrial Automation, Healthcare, Smart Home
Microsoft Azure IoT	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Azure IoT Hub	Smart Cities, Agriculture, Transportation
Google Cloud IoT	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Google Cloud IoT Core	Energy Management, Building Automation, Retail
IBM Watson IoT	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	IBM Watson IoT Platform	Predictive Maintenance, Asset Tracking, Security
Siemens MindSphere	Industrial IoT platform, machine learning, analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	MindSphere	Industrial IoT, Manufacturing, Energy
PTC ThingWorx	IoT application enablement, device connectivity	FPGA, Arduino, Raspberry Pi	ThingWorx	Smart Manufacturing, Service Management, Retail

Figure A.6: IoT platforms architecture table 1

Bosch IoT Suite	Device management, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Bosch IoT Suite	Mobility, Industrial Automation, Smart City
Oracle IoT	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Oracle IoT	Supply Chain Management, Smart Grid, Fleet
Cisco IoT Cloud Connect	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Cisco IoT Cloud Connect	Connected Vehicles, Smart Grid, Oil and Gas
SAP Leonardo IoT	Data integration, machine learning, analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	SAP Leonardo IoT	Smart Logistics, Smart Cities, Asset Management
GE Predix	Device management, data processing and analytics	FPGA, Raspberry Pi, Zigbee	Predix	Aviation, Healthcare, Oil and Gas
Altair SmartWorks	IoT application enablement, data analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Altair SmartWorks	Predictive Maintenance, Quality Management, IoT
Particle IoT	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Particle Cloud	Agriculture, Healthcare, Smart Home

Figure A.7: IoT platforms architecture table 2

Ubidots IoT Application Enablement Platform	IoT application enablement, data visualization	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Ubidots IoT Application Enablement Platform	Agriculture, Smart Cities, Retail
Zebra Savanna	Device connectivity, data processing and analytics	LoRaWAN, Zigbee	Zebra Savanna	Industrial IoT, Healthcare, Retail
Kaa IoT Platform	Device connectivity, data processing and analytics	Raspberry Pi, LoRaWAN, Zigbee	Kaa IoT Platform	Industrial Automation, Smart Home, Energy

Figure A.8: IoT platforms architecture table 3

IoT Platform	Features of Architecture	Types of Devices Used	Used Software	Area of Use
Afero IoT Platform	Device connectivity, data processing and analytics	Bluetooth, WiFi	Afero IoT Platform	Smart Home, Healthcare, Automotive
Axonize IoT Platform	IoT application enablement, data analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Axonize IoT Platform	Smart Building, Energy Management, Agriculture
Hologram IoT Platform	Device connectivity, data processing and analytics	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Hologram IoT Platform	Fleet Management, Smart Agriculture, Healthcare
Losant IoT Platform	IoT application enablement, device connectivity	Arduino, Raspberry Pi, LoRaWAN, Zigbee	Losant IoT Platform	Industrial Automation, Smart Home, Logistics

Figure A.9: IoT platforms architecture table 4

IoT Platforms	Device Control Layer	Integration	Scalability	Data Analytics	Profitability	Flexibility	Security
AWS IoT	Yes	Yes	High	Yes	Profitable	High	High
Microsoft Azure IoT	Yes	Yes	High	Yes	Profitable	High	High
Google Cloud IoT	Yes	Yes	High	Yes	Profitable	High	High
IBM Watson IoT	Yes	Yes	High	Yes	Profitable	High	High
Siemens MindSphere	Yes	Yes	High	Yes	Profitable	High	High
PTC ThingWorx	Yes	Yes	High	Yes	Profitable	High	High
Bosch IoT Suite	Yes	Yes	High	Yes	Profitable	High	High
Oracle IoT	Yes	Yes	High	Yes	Profitable	High	High

Figure A.10: IoT platforms advantages table 1

IoT Platforms	Device Control Layer	Integration	Scalability	Data Analytics	Profitability	Flexibility	Security
AWS IoT	Yes	Yes	High	Yes	Profitable	High	High
Microsoft Azure IoT	Yes	Yes	High	Yes	Profitable	High	High
Google Cloud IoT	Yes	Yes	High	Yes	Profitable	High	High
IBM Watson IoT	Yes	Yes	High	Yes	Profitable	High	High
Siemens MindSphere	Yes	Yes	High	Yes	Profitable	High	High
PTC ThingWorx	Yes	Yes	High	Yes	Profitable	High	High
Bosch IoT Suite	Yes	Yes	High	Yes	Profitable	High	High
Oracle IoT	Yes	Yes	High	Yes	Profitable	High	High

Figure A.11: IoT platforms advantages table 2

IoT Platforms	Device Control Layer	Integration	Scalability	Data Analytics	Profitability	Flexibility	Security
Afero IoT Platform	Yes	Yes	High	Yes	Profitable	High	High
Axonize IoT Platform	Yes	Yes	High	Yes	Profitable	High	High
Hologram IoT Platform	Yes	Yes	Low	Yes	Profitable	Low	High
Losant IoT Platform	Yes	Yes	High	Yes	Profitable	High	High

Figure A.12: IoT platforms advantages table 3

IoT Platforms	Complexity	Dependence	Individual Settings	Price	Binding to a Supplier
AWS IoT	High	High	Difficult	High	Yes
Microsoft Azure IoT	High	High	Difficult	High	Yes
Google Cloud IoT	High	High	Difficult	High	Yes
IBM Watson IoT	High	High	Difficult	High	Yes
Siemens MindSphere	High	High	Difficult	High	Yes
PTC ThingWorx	High	High	Difficult	High	Yes
Bosch IoT Suite	High	High	Difficult	High	Yes
Oracle IoT	High	High	Difficult	High	Yes

Figure A.13: IoT platforms disadvantages table 1

IoT Platforms	Complexity	Dependence	Individual Settings	Price	Binding to a Supplier
Cisco IoT Cloud Connect	High	High	Difficult	High	Yes
SAP Leonardo IoT	High	High	Difficult	High	Yes
GE Predix	High	High	Difficult	High	Yes
Altair SmartWorks	High	High	Difficult	High	Yes
Particle IoT	Medium	High	Difficult	High	Yes
Ubidots IoT Application Platform	Low	High	Easy	Medium	Yes
Zebra Savanna	High	High	Difficult	High	Yes

Figure A.14: IoT platforms disadvantages table 2

Kaa IoT Platform	High	High	Difficult	High	Yes
Afero IoT Platform	High	High	Difficult	High	Yes

Figure A.15: IoT platforms disadvantages table 3

IoT Platforms	Complexity	Dependence	Individual Settings	Price	Binding to a Supplier
Axonize IoT Platform	High	High	Difficult	High	Yes
Hologram IoT Platform	Medium	Low	Easy	Medium	No
Losant IoT Platform	Medium	Low	Easy	High	No

Figure A.16: IoT platforms disadvantages table 4

Aspect	Cloud-based IoT Platforms	Non-Cloud IoT Platforms
Scalability	Highly scalable, can handle large amounts of data	Limited scalability
Flexibility	More flexible, can be customized to meet specific needs	Less flexible
Cost(deploying)	Generally more expensive due to subscription model	Generally cheaper
Maintenance	Maintenance and updates are handled by the provider	Maintenance and updates are handled by the user
Data Security	Data security is generally reliable and up-to-date	Security may be less reliable

Figure A.17: Cloud and non-cloud platforms comparison

Aspect	Cloud-based IoT Platforms	Non-Cloud IoT Platforms
Scalability	Highly scalable, can handle large amounts of data	Limited scalability
Flexibility	More flexible, can be customized to meet specific needs	Less flexible
Cost(deploying)	Generally more expensive due to subscription model	Generally cheaper
Maintenance	Maintenance and updates are handled by the provider	Maintenance and updates are handled by the user
Data Security	Data security is generally reliable and up-to-date	Security may be less reliable

Figure A.18: Cloud and non-cloud platforms comparison 1

Connectivity	Can easily connect to other cloud-based services	Limited connectivity to other services or platforms
Data Analytics	Advanced analytics tools and algorithms available	Limited analytics capabilities

Figure A.19: Cloud and non-cloud platforms comparison 2

Aspect	Cloud-based IoT Platforms	Non-Cloud IoT Platforms
Device Management	Centralized device management and monitoring	Decentralized management and monitoring
Integration with Third-Party Services	Easy integration with third-party services and APIs	Limited integration capabilities

Figure A.20: Cloud and non-cloud platforms comparison 3