TECHNISCHE UNIVERSITÄT
CHEMNITZ

A Survey of the Architecture, Enabling Technologies, and Applications of the Internet of Things

Seminar Report

Chair of Computer Engineering
Dept. of Computer Science

submitted by: Farjana Ahmed
Matrikel Nr.: 619518
submission date: 22.08.2021

Supervising tutor:
Prof.Dr. W. Hardt
René Schmidt

Abstract

The number of smart items is rapidly increasing. Tens of billions of objects will be deployed globally by 2025, gathering a vast amount of data. Traditional computer models collect data in the field and then send it to a central data center for analysis, but this is no longer a viable strategy. To turn massive amounts of collected data into useful information, new methodologies and technologies are necessary. In the IoT ecosystem, technology will also enable interconnection around things, although more study is needed in the development, convergence, and interoperability of the many IoT pieces. By examining application scenarios and practical experiments, this paper presents a picture of the essential technological components required to enable the interconnection of things in order to actualize IoT concepts and applications in the fields of agriculture, smart home security, and the automotive industry. Finally, some key areas for future IoT research are suggested and briefly explored.

Contents

List of Figures

List of Tables

List of Abbreviations

IoT Internet of Things

RFID Radio-frequency identification

UWB Ultra-Wideband

LPWA Low-Power Wide-Area

RF CMOS Radio Frequency Complementary Metal-Oxide Semiconductor

DTD Document Type Definitio

UDEF Universal Data Element Framework

DAM Darpa Agent Markup Lan-guage

RDF Resource Description Framework

OWL Open Web Language

FAO Food and Agriculture Organization

ICT Information and Communications Technology

GIS Geographic Information Systems

NB IoT NarrowBand-Internet of Things

LoRa Long Range

POC Proof of Concept

BoL Beginning of Life

MoL Middle of Life

EoL End of Life

VIN Vehicle Identification Number

ETC Electronic Toll Collection

1 Introduction

The goal of this article is to give the reader a thorough overview of the current state of the art in IoT, with a focus on what has been done in the areas of protocol, algorithm, and system design and development, as well as what future research and technology trends are in the works. This chapter also discusses precision agriculture, smart home security systems, and automobile recycling information management, examples of Internet of Things definitions that are reviewed and briefly discussed from diverse academic and industry perspectives.

1.1 Motivation

With the decline in sensor prices, the rise of remote storage services, and the rise of big data, a number of technologies have gained traction. The ease of access to these resources has also bolstered a trend that is becoming more prevalent in our lives: the Internet of Things (IoT). The word refers to the concept of device connectivity, as well as device-to-device and device-to-system communication.

This information sharing is made feasible by sensors and actuators built into these devices. In general, the internet of things aims to reduce the need for human intervention in a variety of areas while also making life easier for those who use it.

Many ordinary tasks can be automated using IoT by embedding computing devices in everyday objects, which can then be controlled digitally with the added benefit of remote infrastructure. Because most tasks will be automated, there will be less need for manual labor. Everyday devices generate a significant amount of data. This data may be collected effectively and used for Data Science problems to acquire insights and make educated decisions using an IoT architecture.

1.2 Internet of Things

In the field of wireless communications and networking, a novel paradigm known as the Internet of Things (IoT), which was first suggested by Kevin Ashton in 1998, has gotten a lot of interest in academia and industry during the last few years [17]. IoT would bring a new level to the world of information and communication by integrating short-range mobile transceivers into a wide range of extra gadgets and ordinary goods, enabling new types of communication between people and things, as well as between things themselves.

Without a doubt, the IoT vision's major strength is the significant impact it will have on various elements of everyday life and potential consumers' behavior. The most noticeable effects of the IoT will be visible in both the working and household spheres from the perspective of a private user. Assisted living, smart homes and offices, e-health, and enhanced learning are only a few examples of probable application scenarios where the new paradigm may play a key role in the near future [2]. Similarly, the most evident ramifications in sectors such as automation and industrial manufacturing, logistics, business process management, and intelligent transportation of people and goods will be equally noticeable from the perspective of business users.

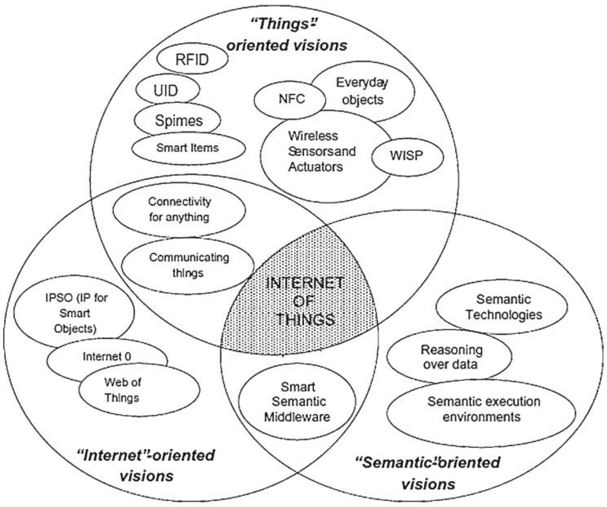
"Things"-
oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensorsand Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

Figure 1.1: Convergence of IoT isions [1].

1.3 Report Structure

The first chapter provides a quick overview of the Internet of Things. Chapter 2 delves into the fundamental properties, components, and architecture of the Internet of Things. Chapter 3 explains the technical background that is required in this field in order to successfully complete any application. Three Internet of Things-based application fields are studied and compared in Chapter 4.In Chapter 5, the paper discusses the problems and open questions of IoT, as well as some prospective research fields.

2 Architecture of the Internet of Things

2.1 The Basic Properties and Characteristics

We can see that IoT is the Internet extending and expanding into the physical world, and its linked qualities include focus, content, collection, computation, communications, and connectivity scenarios, based on the definition above. These traits demonstrate the seamless link that exists between people and objects, or between objects.Figure 2.1 depicts the link between qualities [4].

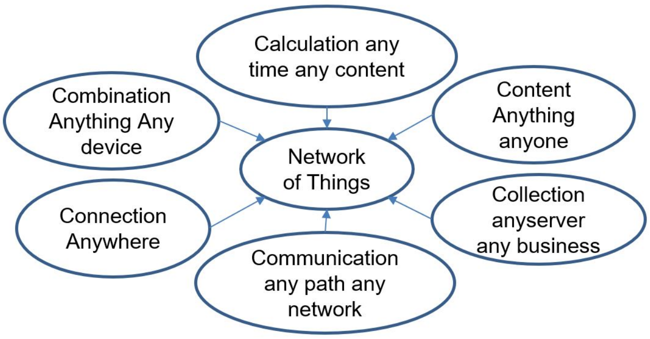
Calculation any time any content
Combination Anything Any device
Content Anything anyone
Network of Things
Connection Anywhere
Collection anyserver any business
Communication any path any network

Figure 2.1: The Basic Properties of IoT [4].

According to the features, consequences, and confinement relationship of the IoT component, it has five parts [4] such as (i) Basic Characteristics, (ii) Objects' General Characteristics, (iii) Social Characteristics, (iv) Autonomy Features, (v) Control and Self-Replication Features.

2.2 Hierarchy Architectures of Network of Things

The Internet of Things should be capable of networking billions or trillions of diverse things, therefore a flexible layered architecture is crucial. A reference model has yet to emerge from the ever-growing variety of potential designs [12].

The fundamental model, which consists of the Application, Network, and Perception Layers, is chosen from the pool of submitted models [10], [23], [21]. Other models that offer further abstraction to the IoT architecture have been presented in

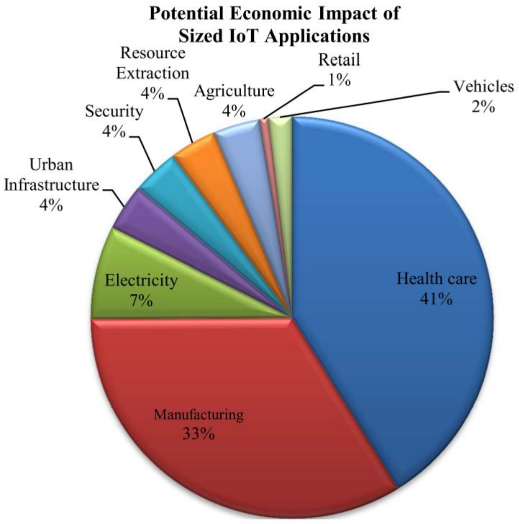

Figure 2.2: Projected market share of dominant IoT applications by 2025 [7]

recent literature [2], [10], [23],[21],[20], [3]. Figure 2.2 shows some popular architectures, including the 5-layer model (not to be confused with TCP/IP layers), which has been utilized in [10], [23], and [21]. Following that, we'll go over these five layers in more detail.

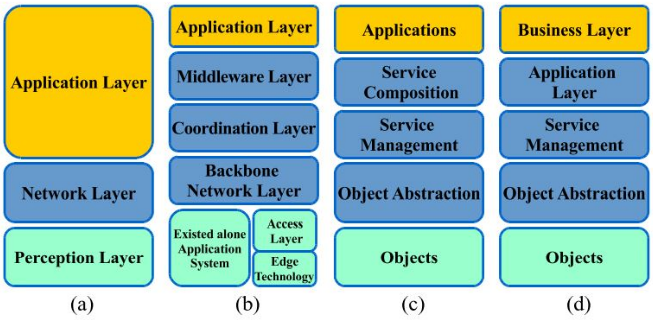

Figure 2.3: The IoT architecture. (a) Three-layer. (b) Middle-ware based. (c) SOA based. (d) Five-layer [7]

2.2.1 Object Layers

The physical sensors that gather and interpret data in the Internet of Things are represented by the first layer, the Objects (devices) or Perception layer. This layer contains sensors and actuators that may query position, temperature, weight, motion, vibration, acceleration, and humidity, among other things. This layer is where the IoT's large data is generated.

2.2.2 Object Abstraction Layer

Object Abstraction uses secure channels to transport data from the Objects layer to the Service Management layer. RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, and other technologies can all be used to convey data. This layer also handles other services such as cloud computing and data management activities [23].

2.2.3 Service Management Layer

Based on addresses and names, the Service Management or Middleware (pairing) layer matches a service with its requester. This layer allows IoT application programmers to operate with a variety of heterogeneous objects without regard for the hardware platform.

2.2.4 Application Layer

Customers request services, which are provided by the application layer. The application layer, for example, can supply temperature and air humidity metrics to a customer who requests them. This layer is critical for the Internet of Things because it can provide high-quality smart services to suit customers' needs.

2.2.5 Business Layer

The total IoT system operations and services are managed by the business (management) layer. This layer's tasks include creating a business model, graphs, flowcharts, and other visual representations of the data received from the Application layer. It is also responsible for the design, analysis, implementation, evaluation, monitoring, and development of IoT system components. The Business Layer enables decision-making processes based on Big Data analysis to be supported. This layer also handles the monitoring and management of the four layers beneath it. Furthermore, this layer compares each layer's output to the expected output in order to improve services and protect users' privacy [10], [21].

3 Technical Background

Understanding the interplay of different empowering technologies (such as data collecting and networking) might help to gain a better understanding of the IoT's true meaning and functionality. This section gives an overview of how these technologies are important in the IoT.

3.1 Key Technologies Involved in Internet of Things

3.1.1 Wireless Communication Technologies

Many wireless communication technologies have been proposed for a range of applications as information technology has progressed [11]. As shown in Fig. 3.1, these technologies are classified into three categories based on transmission distance: short-distance wireless communication technologies (distance less than 10 m), medium-distance wireless communication technologies (distance between 10 and 100 m), and long-distance wireless communication technologies (distance greater than 100 m). Radio-frequency identification (RFID), Bluetooth , ultra-wideband (UWB), and other short-range wireless communication technologies are examples. Two significant medium-distance wireless communication technologies are Wi-Fi and ZigBee. In addition to the well-known cellular networks (2G/3G/4G), LPWA is a new form of technology with a wide range of applications for long-range wireless communication technologies. Several LPWA technologies, including as LoRa, NB-IoT, and Sigfox, have arisen in recent years.

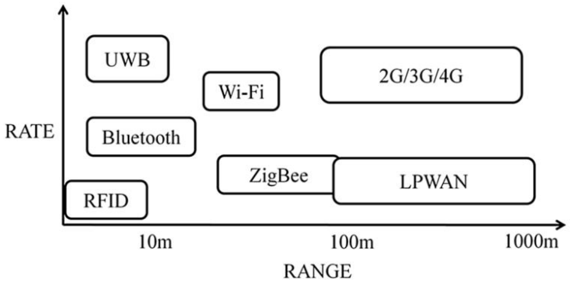

Figure 3.1: Wireless communication systems are compared in terms of range and rate [11].

Bluetooth, Wi-Fi, ZigBee, LoRa, and NB-IoT are among the most prevalent wireless communication technologies. Bluetooth is the most advanced technology available. The ZigBee technology is another viable option, with a communication range of 100 meters, a data rate of 250 kbps, and a transmission power consumption of 39.6 mw. If data rate isn't as crucial as long range and low battery consumption, the two types of LPWA technologies are the most appealing (LoRa and NB-IoT). They provide a communication range of more than 15 kilometers at an acceptable rate, with a transmission power consumption of around 100 mW.

3.1.2 Softwares and Algorithms

Contiki is one of the most promising micro operating systems for limited devices [8]. It has a full IP stack (IPv4 and IPv6), a local flash file system, and a huge development community as well as a comprehensive set of development tools. How to establish a common underlying software fabric for varied contexts and how to make a cohesive application out of a vast collection of diverse software modules is one of the challenges in developing IoT apps. Service-oriented computing is currently receiving a lot of attention as a way to construct distributed and federated applications that facilitate inter operable machine-to-machine and thing-to-thing interaction over a network.

3.1.3 Hardware

In terms of hardware, nano-electronics device research is focusing on shrinking, cheap cost, and greater functionality in the creation of wireless identifiable systems. Silicon IC technology will be used to create systems with more features and better nonvolatile memory for detecting and monitoring environmental parameters. More research is needed in several areas, including ultra-low power, low voltage, and low leakage designs in submicron RF CMOS technologies, high-efficiency DC-DC powermanagement solutions, ultra-low power, low voltage controllable nonvolatile memory, and the integration of RF MEMS and MEMS devices, to name a few. In the use of RFID tags, the following key patterns have been noted.

It has been discovered that ultra-low-cost tags with very minimal functionalities are being used. The value of information is found in the data management operations, which are concentrated on data servers controlled by service operators. There is also evidence of the use of low-cost tags with increased characteristics such as extra memory and sensing capabilities.

3.1.4 Technology for Data and Signal Processing

Many industries have established standardization groups to provide XML standards specific to their needs. These XML vocabularies are then made available to members of that industry vertical as a generalized document type definition (DTD) or XML schema. By providing globally unique cross-reference identifiers for data elements, initiatives such as the International Standard for Metadata Registries (ISO/IEC 11179) and its implementation, such as the Universal Data Element Framework

(UDEF) from OpenGroup, by providing globally unique cross-reference identities for semantically comparable data items, despite the fact that they may have distinct names in different XML markup standards.

Finally, W3C semantic web standards such as DAML (Darpa Agent Markup Language), RDF (Resource Description Framework), and OWL (Open Web Language) (Ontology Working Language) are useful for laying the semantic groundwork for dynamic situations involving the discovery of businesses and services.

3.1.5 Technologies for Discovery and Search Engine

IoT will necessitate the creation of lookup or referral services to connect things to information and services, as well as secure access to information and services that respects both individual privacy and company confidentiality. Requester and providers of information services might be matched based on trust relationships. As a smart thing travels through the real world, it will come across different environments, and both the smart thing and other agents monitoring it will need lookup techniques to figure out what capabilities are accessible in the local environment. Sensors and actuators, network connection interfaces, facilities for computation and processing of data into information, as well as facilities for onward transit, handling, physical processing, or notifying a human operator about problems, are examples of such capabilities.

3.1.6 Technologies for Security and privacy

Human privacy and business process confidentiality are two important challenges with the Internet of Things. The cloud of things is difficult to regulate due to its large size of deployment, mobility, and generally low complexity. A great range of standard encryption mechanisms are available for use in ensuring confidentiality. The key problem, though, is to make encryption methods faster and more energy efficient. Furthermore, if an encryption technique is to be used, an efficient key distribution scheme must be in place.

Key distribution for small-scale systems can take place in the factory or during deployment, but unique key distribution strategies for ad-hoc networks have only recently been presented. The situation is more bad when it comes to privacy; one of the reasons is that the general population is unaware of the issue [13]. Furthermore, privacy-preserving technology is still in its infancy: the systems that work are not designed for resource-constrained devices, and a holistic view of privacy (e.g., a vision of privacy throughout one's life) has yet to be developed.

4 Applications of Internet of Things

The IoT's capabilities enable the development of a wide range of applications, however just a few are already in use. Intelligent applications will be available in the future for smarter homes and workplaces, smarter transportation systems, smarter hospitals, smarter businesses, and smarter industries. Some of the most notable IoT example applications are briefly explored in the following subsections.

4.1 Wireless Communication Technologies on Internet of Things for Precision Agriculture

According to the UN's Food and Agriculture Organization (FAO), the world's population would reach 9.2 billion by 2050. It is a difficult undertaking to feed an ever-increasing population in these dire circumstances. Sensor technology, information and communications technology (ICT), information processing technology, geographic information systems (GIS), environmentally friendly farming through flexible fertilization technology, and information management are all integrated to ensure productivity even with a small workforce [15], [16], [6]. These technologies, as well as others, have recently played an essential role in stimulating innovation in the agriculture industry, giving rise to the notion of precision agriculture (PA) [6], [14]

4.1.1 Application Architecture for Precision Agriculture

The goal of IoT-based precision agriculture is to create a system that monitors crop fields and intellectualizes farmland management by using sensors (temperature, humidity, light, soil moisture, and so on). WSNs connect data collecting and processing across the whole system [16]. As shown in Fig. 4.1, the system architecture of IoT-based precise agriculture is made up of three parts: "things" (sensors/actuators or end-devices), local gateways (or base stations), and the network server (or cloud server). Typically, "Things" are used to collect and control feld data. "Things" are controlled and managed using data locally and/or connected to local gateways (or base stations) that give enhanced capability in IoT-based solutions. Gateways act as intermediaries between "things" and servers, providing the connectivity, interactivity, and security that they require. Data storage, management, analysis, and processing are all provided by the network server, as well as information assistance for intelligent decision-making. Three types of WSNs were used to evaluate the performance of the NB-IoT, LoRa, and ZigBee standards for monitoring farmlands.

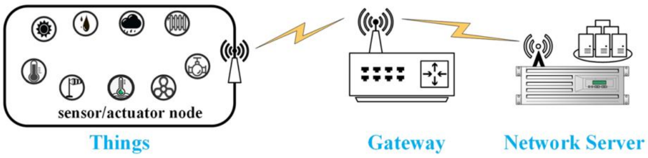

Figure 4.1: The system architecture of IoT-based precise agriculture [5].

Precision Agriculture with NB IoT-Based WSN

Figure 4.2 depicts an NB-IoT application framework for PA. NB-IoT terminals, transmission networks, and an application server are the three components of the framework. They are in charge of data gathering, data transfer, data analysis, and decision-making, among other things. The NB-IoT terminals are made up of various environmental sensors and NB-IoT modules that complete the function of field data gathering. Sensors are used to collect environmental data, which is then transmitted to NB-IoT modules through the RS485 bus; the data transmission network is made up of the NB-IoT network and the Internet network. Sensing data from NB-IoT terminals is sent to the Internet network via the NB-IoT network; the application server's responsibilities include receiving, preserving, and visualizing data, as well as making sensible decisions based on data analysis.

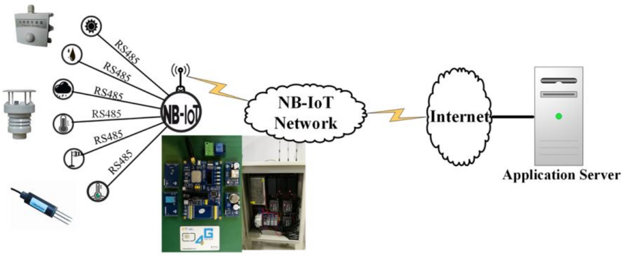

Figure 4.2: The application architecture of NB-IoT for precise agriculture [5].

Precision Agriculture with LoRa Based WSN

As demonstrated in Fig. 4.3, a LoRa-based WSN is shown. The star-topology network has three different sorts of components: end-devices, gateways, and network servers. Sensors/actuators, a LoRa transceiver, and a LoRa receiver make up the end-devices. Gateways send raw data frames from end-devices to the network server over a higher-throughput Ethernet backhaul interface. The network server is in charge of copying and decoding sensing packets supplied by end-devices, as well as creating decision-making packets to be sent back to them.

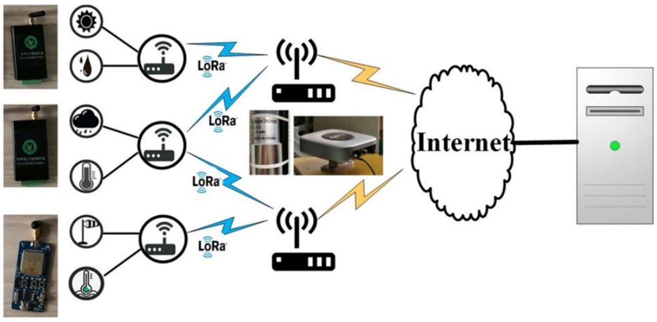

Figure 4.3: The application architecture of LoRa for precise agriculture [5].

Precision Agriculture with ZigBee Based WSN

The star, tree, and mesh topological structures exist in the ZigBee network. The tree topology, in comparison to the other two, offers the advantages of high connection and minimal routing overhead, making it better suited for agriculture periodic monitoring and other applications. The ZigBee-based tree networking topology shown in Fig. 4.4 is a highly reliable, energy-efficient, and low-cost solution that has been widely utilized in agriculture to monitor various environmental and soil data. There are three sorts of nodes that can be identified in this tree topology network: End-devices, routers, and coordinators are three types of end-devices.

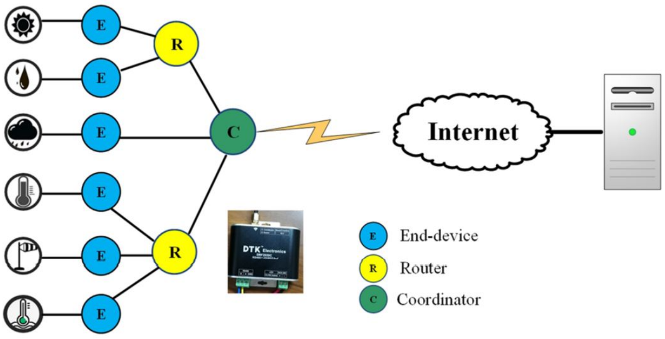

Figure 4.4: Precision Agriculture with ZigBee architecture [5].

4.1.2 Field Tests

All of the following tests were carried out on a nearly 12-square-meter field. The feld tests serve two purposes. The first is to assess the viability of the three application frameworks mentioned above, particularly the NB-IoT application architecture based on the latest LPAW technology. Second, three types of wireless communication technologies are evaluated in terms of power usage.

The Feasibility Tests

The viability of an NB-IoT-based application architecture is first explored, as shown in Fig. 4.2. The Quectel BC95-B5 NB-IoT module with the 850 MHz frequency band is the one that has been chosen. As a controller, the STM32 is used because of its low cost.

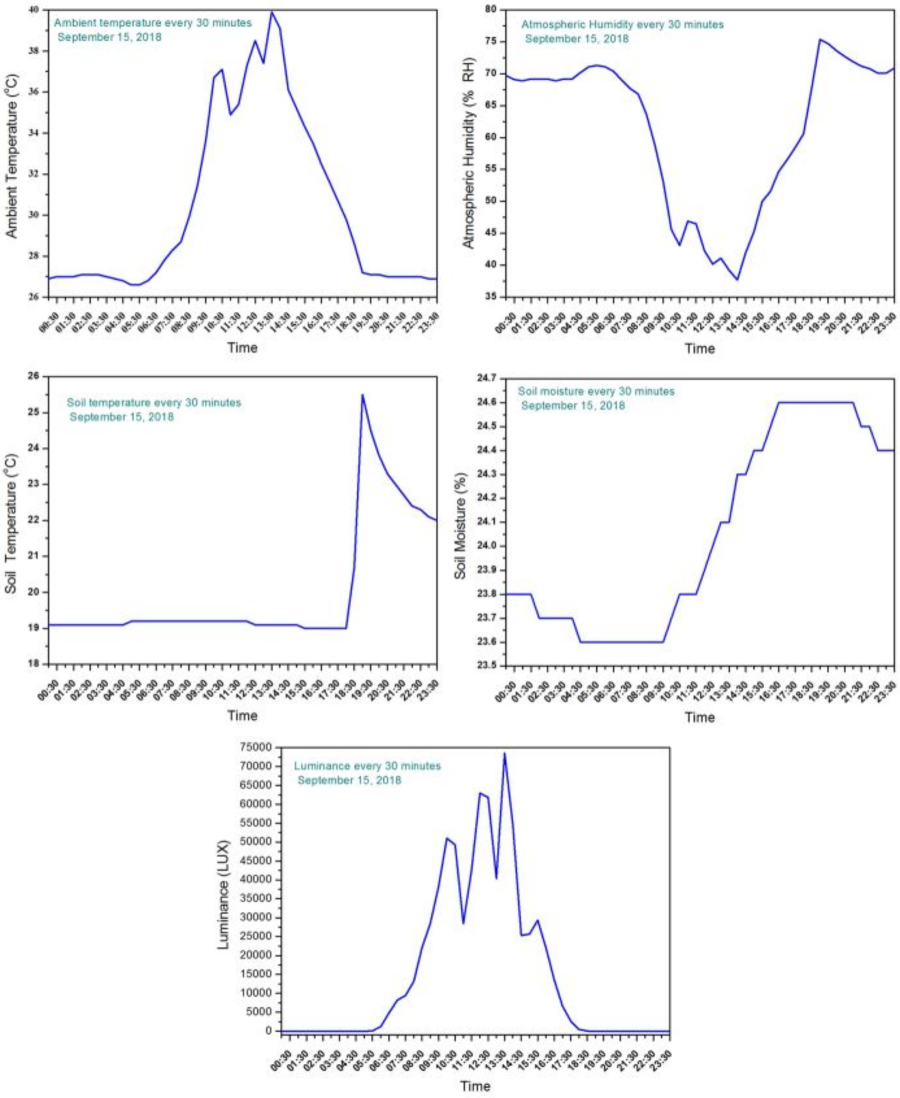

Figure 4.5: The daily testing curve obtained by NB-IoT based WSN [5].

Figure 4.5 depicts the results of 24 hours of feld testing. The WSNs depicted in Figs. 3, 4, and 5 are utilized to collect environmental and soil data in the following tests. The TI Company's CC2630 ZigBee modules are the ones we've chosen. The end-devices are a development board with Semtech SX1278.

Figure 4.6 depicts the testing topology. Longer communication lengths are given via route relay in ZigBee communication technology, as demonstrated in Fig. 4.6a.

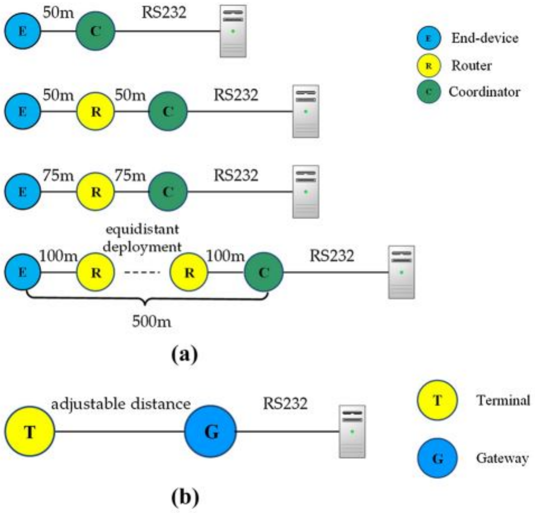

Figure 4.6: Topology for power consumption tests. a) Test for ZigBee communication technology. b) Test for LoRa and NB-IoT communication technologies [5].

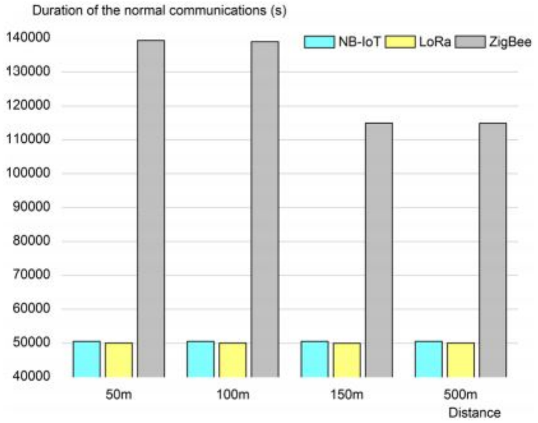

Figure 4.7: Comparison of normal communication time of three topological structures [5].

Communication distance is adjusted for NB-IoT and LoRa by adjusting the distance between the terminal and the gateway, as shown in Fig. 4.6b, with no relay required. The distance that can be adjusted is determined by the testing requirements when the testing distance is 50 m, 100 m, 150 m, and 500 m, respectively. Figure 4.7 depicts the length of regular communications for the three wireless communication methods.

4.2 Smart Home Security Analysis System Based on IoT

As the Internet of Things (IoT) has grown in popularity in recent years, more and more smart home devices have become available to make people's lives easier. The traffic collection module, traffic analysis module, system detection module, and warning notification module are the primary components. The traffic capture module records traffic that passes through the router and is used in the traffic analysis module that follows. The traffic analysis module will do a matching analysis on the collected traffic to identify whether it is malicious or unexpected traffic, and then clean and reissue the traffic. The system detection module detects "mining" malware, monitors the system's progress in real time, blocks any aberrant operations, and delivers warning alerts to users via the warning notification module.

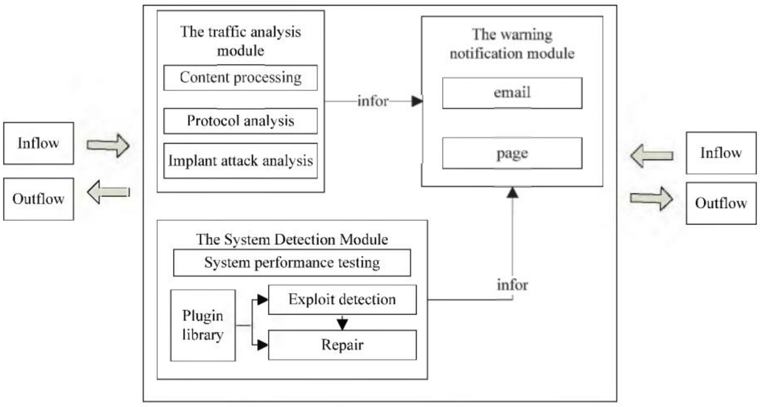

Figure 4.8: The process of smart home security analysis system [24].

4.2.1 Different Modules for Smart Home Security

The Traffic Capture Module

The data packets that need to be reviewed are collected by the traffic capture module and delivered to the traffic analysis module for further processing. To capture traffic, this module mostly employs the Netfilter framework. Five monitoring stations are set up by the Netfilter framework [22]. Developers can create their own callback functions (HOOK) to evaluate and process the traffic coming via each monitoring point. Figure 2 depicts the position of the monitoring points.

The network data packet passes through the PRE_ROUTING point after entering the IP layer to determine whether the destination address is local. If it is, it will be transmitted from the LOCA_IN point to the higher layer protocol stack; otherwise, it will flow out via POST_ROUTUNG after passing through the FORWARD point. The data packet sent by this machine flows out through POST_ROUTUNG after

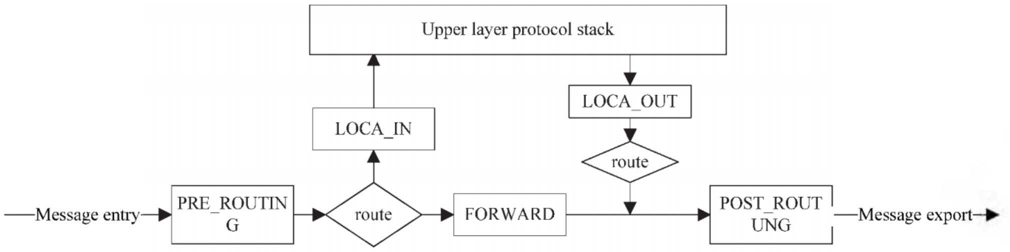

Figure 4.9: Netfilter monitoring points [24].

passing through the LOCA_OUT point. At the same time, after the Hook function has completed the data packet's verification, it might return various values in order to conduct various operations on the data packet. Table 4.1 displays the return value as well as the relevant operation.

Function Return Value	Operation
NF_DROP	Drop this packet
NF_ACCEPT	Keep this packet
NF_STOLEN	Ignore this packet
NF_QUEUE	Insert data packet into user space
NF_REPEAT	Call this callback function again

Table 4.1: Return Value of a Callback Function and Its Corresponding Operation [24].

The Traffic Analysis Module

This module examines the amount, content, and protocol kinds of traffic travelling through smart home devices and evaluates whether the data packet contains malicious content, aberrant protocols, or abnormal flow in the flow through it, as well as other factors. Following the acquisition of traffic, the traffic analysis module classifies and recognizes the protocol, address, major content, and other elements in the data packet for later detection and analysis.

The System Detection Module

The system detection module's main function is divided into two components. The detection of malicious files that are "mining" is the initial step. The main goal of "mining" harmful files is to gain profit by robbing the device's computer resources. The device's CPU is usually completely employed in order to optimize the benefits. The discovery of device vulnerabilities is the second part. This module contributes by keeping the POC plug-in library and the repair plug-in library up to date. For vulnerabilities that burst on the network, it is required to build POC scripts and repair scripts on a regular basis.

The Warning Notification Module

To enhance the success percentage of consumers receiving notifications, this module uses two notification techniques based on distinct security risk levels. The risk information is delivered to the owner's mailbox through email in the first approach, reminding the owner that a certain device poses a security risk and requesting that the owner conduct the necessary repairs. Page jump notification is the second technique. In an emergency, this strategy is employed. The user is led to the alert information page from any page he or she visits.

4.2.2 Evaluation

This paper installs the smart home security analysis system on an experimental router and connects smart home devices from various brands and models to the router in order to test the system's actual effect. To verify the system's impact on home network performance, the performance experiment picks common network operations of ordinary users.

Experimental Result

In the non-contact assault experiment, the open source botnet virus Mirai [18] was chosen to simulate the real scenario in order to approach the genuine usage scenario. Through scp, the "mining" malware script is tweaked and uploaded to the device. Table 4.2 displays the final experimental results.

Equipment	Protocol	Attack Method	Result
Smart Router(TP Link)	HTTP	Command Injection	Success
Smart Router(TP Link)	HTTP	Stack Overflow	Success
Smart Router(NETG EAR)	TCP	DDos Mirai	Success
Smart Router(NETG EAR)	HTTP	"Mining" Malware	Success

Table 4.2: Result of Non-Contact Attack Defense Result [24].

Four separate performance test items have been devised to cover the network operations of users who utilize the network on a daily basis. Table 4.3 displays the results.

- Using the ping command to test the network's response time.
- Downloading a certain file using the system ftp command and calculating the total duration and average download speed.
- Downloading files using the system wget command and calculating the total duration and average download speed.
- Using a browser to access commonly visited online pages and determining the average amount of time spent on each one.

Test Item	The system is turned on	The system is not turned on
pmg	22.951ms	24.287ms
ftp	3.32s(9.34MB/s)	3.91s(7.93MB/s)
wget	6.52s(10.41MB/s)	7.53s(9.02MB/s)
browser	10.91s	11.22s

Table 4.3: The Result of system Performance Test [24].

4.3 Automotive Industry based on Internet of Things

Automotive manufacturing ”IOT” is a critical intersection in the realm of two major rising industries: IOT and intelligent cars. It will also be a new trend. It brings together the most recent advances in the fields of supply chain management and information management, as well as RFID technology’s unique capacity to capture data in real time.

4.3.1 Automotive Recycle Data Management Application Framework

The applications of ”IOT” in automotive manufacturing can be summarized in terms of the car’s life cycle as follows: spare parts supply and vehicle manufacturing, warehousing and sales, use and service, community management, and scrap recycling process, and continue the summary in light of different processes. Figure 4.10 shows the ”IOT” service platform frame system, which includes an operation and maintenance center, as well as a data processing center [26].

Automotive Lifecycle Information System

There are three steps to the automobile supply chain. There are three stages: beginning of life (BOL), middle of life (MoL), and end of life (EoL). Each stage’s data should be able to communicate with one another. The data can be kept in a database on an information server, and authorized computers in the BoL, MoL, and EoL stages can access the database to retrieve the data. Figure 4.11 depicts the key internet of things in the automobile industry.

BoL Stage

Each material and component is incorporated into a single electrical code during the BoL stage. This code is the identity card for the component, and it contains information such as the Vehicle Identification Number (VIN), material information, date of manufacturing information, recyclability and recoverability information, and so on.

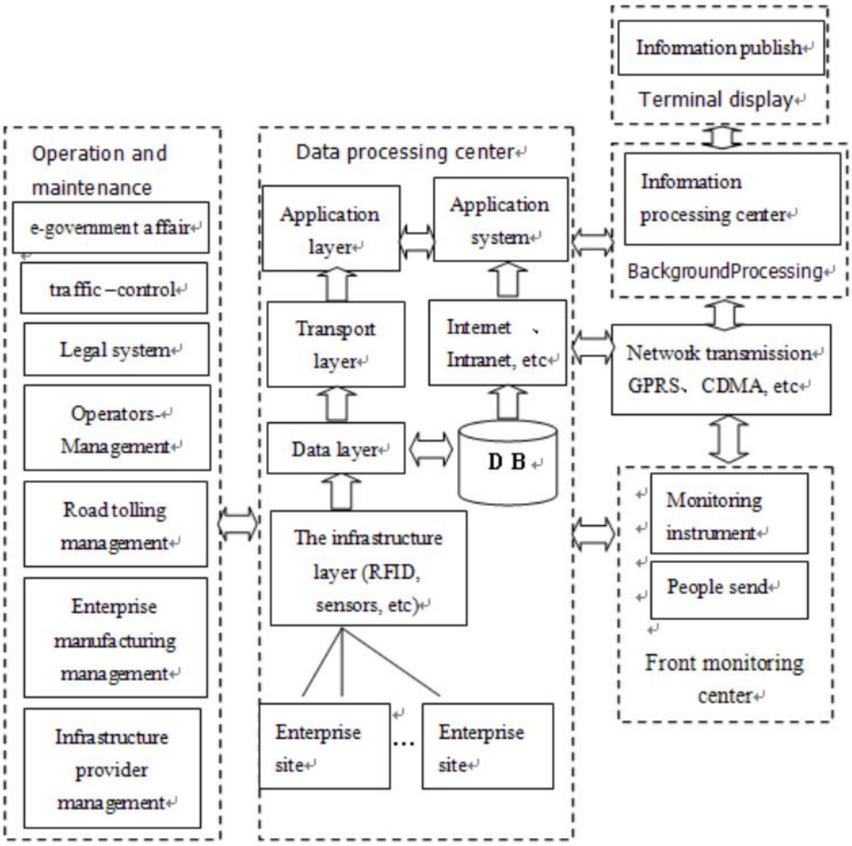

Figure 4.10: Service platform's framework system of automobile manufacture "IOT" [25].

MoL Stage

At the MoL stage, the car is in the hands of the consumer, and the only way to obtain vehicle usage information is to utilize an RFID reader/writer to interact with the labels in the automobile repair business. The information flow is depicted in Fig. 3 below. Furthermore, the Labels are programmed with the vehicles' VIN numbers, allowing us to implement an Electronic Toll Collection (ETC) system, intelligent parking management, vehicle scheduling management, and even vehicle location management, among other things.

EoL Stage

When a vehicle reaches the end of its life cycle, the dismantler can obtain vehicle information by reading the labels. The material information, dismantling information, and residual life information can then be obtained using decision support software. The company can then decide whether to reuse/remanufacture the components or dispose of them based on their remaining useful life. Recycling data can be provided back to manufacturers to help them improve product design, and customers can use

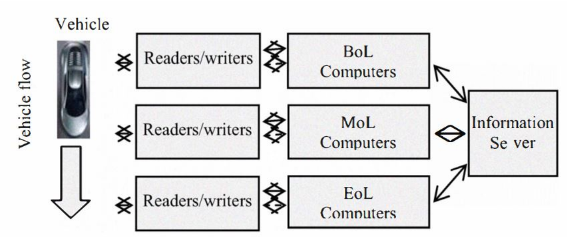

Figure 4.11: The automotive industry's main internet of things [25].

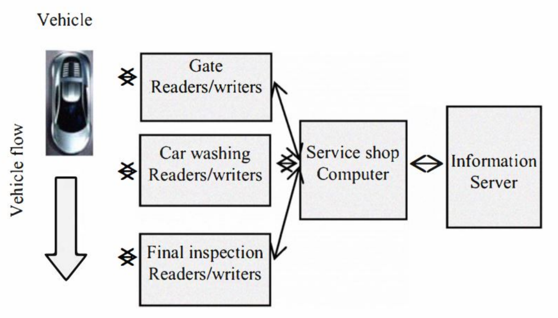

Figure 4.12: Infonnation flow in maintenance system [25].

the information server to find the parts they need. The information flow is depicted in Figure 4.12. Using a browser, accessing frequently frequented online pages and calculating the average time spent on each.

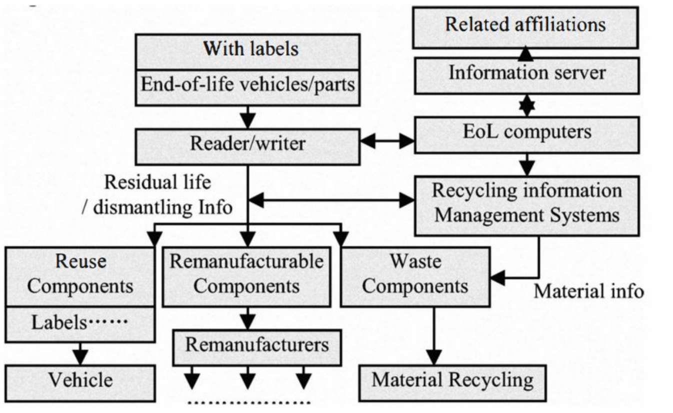

Figure 4.13: Infonnation flow at EoL stage [25].

5 Discussion

5.1 Challanges and Open Issues

There is a hidden chain of challenges behind every success story. The Internet of Things is the same way. It faces three key obstacles, according to Banafa A. et al. [19]:

- Technological difficulties
- Problems in the workplace
- societal issues

Different protocols and technologies are used to implement IoT components. As a result, many components have complicated designs and poor construction. Five parameters can be reflected in technological difficulties such as security, Connectivity, compatibility and longevity, standards, intelligent analysis and actions [19].

The main issue is a major source of inspiration for starting, investing in, and managing any venture; without a full proof plan of action for IoT, we will have another bubble; this model should meet all of the requirements for all types of e-commerce, including vertical markets, horizontal markets, and consumer markets.Regardless, this class is constantly subjected to administrative and legal scrutiny. The use of IoT technology can help to generate more revenue while also reducing the strain on existing communication infrastructure.

IoT data is highly sensitive information that, if released, might put the system's control in the hands of an attacker. As a result, we need powerful and dependable technology to secure how IoT data is handled. Business policies and processes, as well as government regulations and standards, provide social and legal hurdles to IOT use [9].

5.2 Future Research Areas

There are various areas where more study is needed in order to make the notion of IoT implementation reliable, robust, and efficient. The following are some of the areas that have been recognized.

More research is needed in the identification technology domain to develop new technologies that address global ID schemes, identity management, identity encoding/encryption, pseudonym, revocable anonymity, party authentication, repository management using identification, authentication, and addressing schemes. Some of the issues that need to be addressed in the domain of architecture design include: design of distributed open architecture with end-to-end characteristics, interoperability of heterogeneous systems, neutral access, clear layering, and resilience to physical network disruption, decentralized autonomic architectures based on node peering, and so on.

Design of energy efficient communication by multi frequency protocol, communication spectrum and frequency allocation, software defined radios to eliminate the need for hardware upgrades for new protocols, and design of high performance, scalable algorithms and protocols are all issues that need to be addressed in the communication protocol domain.

In the network technology domain, more study is needed on network on chip technology, which includes on-chip communication architectures for dynamic configurations, a dynamic routing system, and a configurable number of permissible virtual connections at each output. Furthermore, some of the key research issues are power-aware network design, which turns on and off links on demand in response to traffic bursts and dips, and scalable communication infrastructures design on chip, which dynamically support communication among circuit modules based on varying workloads and/or changing constraints.

6 Conclusion

Looking at today's cutting-edge technologies, we can see how the Internet of Things will be deployed on a global scale in the next years. We also get a sense of the key elements that need to be researched and developed further in order to make large-scale IoT deployment a reality. It has been recognized that major effort in the field of IoT governance is urgently required. Without a standardized approach, a plethora of designs, identification schemes, protocols, and frequencies is likely to occur in parallel, each tailored to a certain need. This will inevitably split the Internet of Things, hampereding its popularity and posing a significant barrier to its adoption. Interoperability is a must, and inter-tag communication is a must for widespread IoT adoption.

The technologies required to realize the omnipresent network society are predicted to mature in the next years. As RFID applications gain acceptance, a large number of things will be reachable and connected to IP-based networks, forming the first wave of the Internet of Things. In order to ensure seamless network access, there will be two big challenges: the first is the fact that several networks cohabit today, and the second is the sheer magnitude of the IoT. The existing IT sector has no expertise building a system that connects hundreds of millions of items to IP networks.

This article examined some of the most critical features of the Internet of Things, with an emphasis on what is being done and what concerns require more investigation. While current technology make the notion of IoT conceivable, there are numerous obstacles to overcome before IoT applications can be deployed on a broad scale in the real world. Addressing these issues will be a significant driving force for networking and communication research in both industrial and university laboratories in the coming years.

Bibliography

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials 17(4), 2347–2376 (2015)

[2] Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks 54(15), 2787–2805 (2010)

[3] Chaqfeh, M.A., Mohamed, N.: Challenges in middleware solutions for the internet of things. In: 2012 international conference on collaboration technologies and systems (CTS). pp. 21–26. IEEE (2012)

[4] Dobrilović, D., Čović, Z., Stojanov, Ž., Brtka, V.: Approach in teaching wireless sensor networks and iot enabling technologies in undergraduate university courses. In: Proceedings of the 2nd regional conference Mechatronics in Practice and Education, MechEdu. pp. 18–22 (2013)

[5] Feng, X., Yan, F., Liu, X.: Study of wireless communication technologies on internet of things for precision agriculture. Wireless Personal Communications 108(3), 1785–1802 (2019)

[6] Ferrández-Pastor, F.J., García-Chamizo, J.M., Nieto-Hidalgo, M., Mora-Martínez, J.: Precision agriculture design method using a distributed computing architecture on internet of things context. Sensors 18(6), 1731 (2018)

[7] Floyer, D.: Defining and sizing the industrial internet. Wikibon, Marlborough, MA, USA (2013)

[8] Govinda, K., Saravanaguru, R.: Review on iot technologies. International Journal of Applied Engineering Research 11(4), 2848–2853 (2016)

[9] Ji, Z., Anwen, Q.: The application of internet of things (iot) in emergency management system in china. In: 2010 IEEE International Conference on Technologies for Homeland Security (HST). pp. 139–142. IEEE (2010)

[10] Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 2012 10th international conference on frontiers of information technology. pp. 257–260. IEEE (2012)

[11] Khuwaja, A.A., Chen, Y., Zhao, N., Alouini, M.S., Dobbins, P.: A survey of channel modeling for uav communications. IEEE Communications Surveys & Tutorials 20(4), 2804–2821 (2018)

[12] Krčo, S., Pokrić, B., Carrez, F.: Designing iot architecture (s): A european perspective. In: 2014 IEEE world forum on internet of things (WF-IoT). pp. 79–84. IEEE (2014)

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

[14] Martínez, R., Pastor, J.Á., Álvarez, B., Iborra, A.: A testbed to evaluate the fiware-based iot platform in the domain of precision agriculture. Sensors 16(11), 1979 (2016)

[15] Navarro-Hellín, H., Martinez-del Rincon, J., Domingo-Miguel, R., Soto-Valles, F., Torres-Sánchez, R.: A decision support system for managing irrigation in agriculture. Computers and Electronics in Agriculture 124, 121–131 (2016)

[16] Ojha, T., Misra, S., Raghuwanshi, N.S.: Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. Computers and electronics in agriculture 118, 66–84 (2015)

[17] Santucci, G., et al.: From internet of data to internet of things. In: International conference on future trends of the internet. vol. 28, pp. 1–19 (2009)

[18] Shouran, Z., Ashari, A., Priyambodo, T.: Internet of things (iot) of smart home: privacy and security. International Journal of Computer Applications 182(39), 3–8 (2019)

[19] Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., et al.: Vision and challenges for realising the internet of things. Cluster of European research projects on the internet of things, European Commision 3(3), 34–36 (2010)

[20] Tan, L., Wang, N.: Future internet: The internet of things. In: 2010 3rd international conference on advanced computer theory and engineering (ICACTE). vol. 5, pp. V5–376. IEEE (2010)

[21] Wu, M., Lu, T.J., Ling, F.Y., Sun, J., Du, H.Y.: Research on the architecture of internet of things. In: 2010 3rd international conference on advanced computer theory and engineering (ICACTE). vol. 5, pp. V5–484. IEEE (2010)

[22] Yang, Y., Yonggang, W.: A software implementation for a hybrid firewall using linux netfilter. In: 2010 Second World Congress on Software Engineering. vol. 1, pp. 18–21. IEEE (2010)

[23] Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for iot. In: 2011 International Conference on Multimedia Technology. pp. 747–751. IEEE (2011)

[24] Yu, R., Zhang, X., Zhang, M.: Smart home security analysis system based on the internet of things. In: 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). pp. 596–599. IEEE (2021)

[25] Zhang, T., Wang, X., Chu, J., Liu, X., Cui, P.: Automotive recycling information management based on the internet of things and rfid technology. In: 2010 IEEE International Conference on Advanced Management Science (ICAMS 2010). vol. 2, pp. 620–622. IEEE (2010)

[26] Zhang, T., Wang, X., Liu, X., Chu, J., Cui, P.: Automotive green supply chain management based on the rfid technology. In: 2010 IEEE International Conference on Advanced Management Science (ICAMS 2010). vol. 2, pp. 617–619. IEEE (2010)