Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 215 (2022) 274–288

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Innovative Data Communication Technology and Application

Internet of Things: Protocols, Applications and Security Issues

Dr. Sarika Choudhary[a,*], Gaurav Meena[b,*]

[a]*Department of Computer Science & Engineering, PDM University, Haryana, India-124507*
[b]*Department of Computer Science, Central University of Rajasthan, Ajmer, Rajasthan, India- 305817*

Abstract

The Internet of Things is poised to become an important crossroads for several technologies. As a result, it will be possible to connect smart physical goods and enable smart decision-making across a wide range of applications. Various devices, including computers, actuators, and sensors, may link to one another and exchange data in a networked environment known as the Internet of Things (IoT). Smart refers to how humans communicate with technology, whereas ”smart objects” describes the machines themselves. As the market’s supply of gadgets grows, ensuring their safety becomes more critical than ever. The availability of cutting-edge methods and tools has been instrumental in the current surge of interest in IoT security studies. To guarantee success, these applications need the characteristics of the environment provided by the IoT framework. This essay dives deep into the IoT’s layered architecture, layer-by-layer protocols, cutting-edge use cases, and pervasive security concerns. In addition to analysing the current security structure, this paper provides a research taxonomy for IoT. Our study is more comprehensive than many that have come before it on the topic of the Internet of Things; we look at everything from sensors to real-world applications.

© 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 4th International Conference on Innovative Data Communication Technologies and Application

Keywords: Internet of Things (IoT); Smart Homes; Applications; Healthcare; Smart Agriculture; Smart Things; RPL; CoAP.

1. Introduction

The number of people using the Internet has increased at a rate that has never been seen before in recent years. It can be found practically everywhere on the earth and has had a profound impact on people’s lives across the board wherever it is found. Despite this, we now live in a society in which an extremely diverse array of electronic gadgets may be linked to the internet. We are now living in the era of the Internet of Things (IoT), which is distinguished by the connectedness of ”things” to the ”Internet.” This connectivity is a hallmark of the IoT. In the year 1999, it was Kevin Ashton who is credited with being the first person to use the word [4]. The traditional concept of the Internet of Things (IoT) has been defined in a number of different ways by several different publications. First, let’s take a look at a general definition. Objects are defined by Penã-Lòpez *et al.* [33] as having the networking and computational ca-

* Corresponding author: Dr. Sarika Choudhary, and Gaurav Meena
E-mail address: scpreety98@gmail.com, gaurav.meena@curaj.ac.in

1877-0509 © 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 4th International Conference on Innovative Data Communication Technologies and Application
10.1016/j.procs.2022.12.030

pabilities necessary to do the tasks that have been given to them. Because of this, the Internet of Things, often known as IoT, is a network that consists of every device in the physical world being linked to the internet. Figure 1 presents the global scenario for the Internet of Things. The future will bring an increase in complexity, which will need a high level of cognition to handle effectively.

Components such as actuators, sensors, transducers, transceivers, and central processing units are often found in Internet of Things devices. The Internet of Things (IoT) is an umbrella term for a collection of interoperable technologies. Actuators and sensors are the components of the Internet of Things system with the highest significance. They find applications in many situations that occur in the real world. The term ”sensor” refers to any device that is able to both receive and send signals. There are a variety of possible manifestations of the signal, including energy, light, motion, and others. Transducers are electronic devices that take one input energy and convert it to another form of output energy. Actuators are defined as devices that move objects by turning energy into motion, and there are a wide variety of different types of actuators.

As a consequence of this, an actuator may be thought of as a specific kind of transducer. These components are part of the physical layer. Once we have the data, we can go on to the different levels of processing and storage. The information is then sent to a server after that process is complete. However, due to the devices' limitations in energy, power, storage, and processing, things that are part of the Internet of Things have very little capacity for data storage. The most challenging part of the process is determining which device will be used for data collection, processing, handling, and transmission. The Internet of Things relies on using wireless connectivity among its many components. Wireless channels are notorious for their high distortion rates and lack dependability.

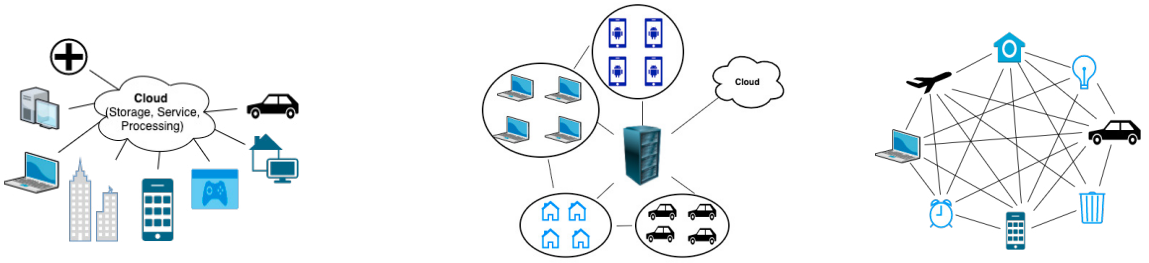

Fig. 1: Internet of Things architecture scenarios. (a) Past IoT Scenario (b) Present IoT Scenario (c) Future IoT Scenario

After the data has been processed, the appropriate action should be carried out according to the kind of application. The nature of the activities may vary; for instance, some apps link with one another rather than with people; this kind of interaction is referred to as M2M interaction, which stands for ”machine to machine.” There are several apps that are handled entirely by a human being. They can broadcast as well as receive messages, depending on the circumstances. IoT networks use a wide range of technologies, protocols, and standards to facilitate communication with many disparate types of devices. Figure 1 illustrates the basic architectures that make up the Internet of Things. At the moment, everything is linked to the cloud by means of a server. In the future, the devices are not directly linked to the Internet; nevertheless, they are connected to other Internet of Things devices. A new concept that is referred to as the social Internet of Things (IoT) develops [1] when electronic devices are linked to the Internet. The Internet of Things allows users of social networking sites to share their equipment online.

Concerns around users' personal information and their right to privacy have emerged in tandem with the expansion of the Internet of Things [12]. In the past, there have been a variety of security breaches that affected IoT app use. The cyberattack known as Mirai was the first to occur in 2016. It involved around three million devices connected to the Internet Flashpoint [16]. Mirai carried out an assault known as a distributed denial of service (DDoS). Two further botnet assaults that significantly affect Internet of Things devices have emerged in the wake of Mirai, Hajime, and Reaper [24].

This article provides a comprehensive review of IoT's framework, protocols, security issues, and proposed remedies (IoT). The remainder of the paper is structured as follows: In this Section 2, We present an overview of the basics of IoT design and protocol. Section 3 describes the development of IoT-based and real-world applications. In the Section 4, IoT security issues, of which there are many, are discussed at length. Possibilities for future study in the realm of

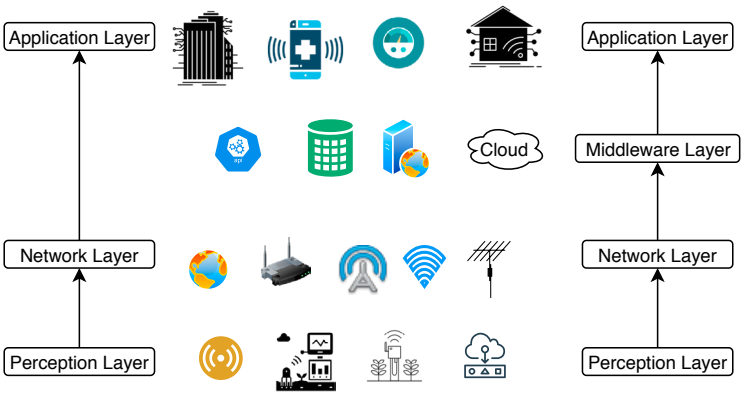

Fig. 2: IoT three-layer and four-layer architecture.

the Internet of Things (IoT) are broken down and addressed in Section 5, Section brings this collection of work to a satisfactory conclusion in this Section 6.

2. IoT Architecture and Protocols

Various researchers have proposed different IoT standard architectures. There isn't a standard universal architecture on which everyone agrees.

2.1. Three-layer and four-layer architecture

As illustrated in Figure 2, the most basic and widely accepted architecture is a three-layer architecture [36, 29]. It was first used when the research was only getting started. In recent studies, a new layer has been added [20].It is often referred to as architecture with four layers. The four levels are the perception layer, the network layer, the middleware layer, and the application layer.

2.1.1. Perception layer

The lowest layer is concerned with the actual physical Internet of Things devices, including sensors, actuators, and other components. Because it mainly interacts with sensors, some researchers also refer to it as a sensing layer [10]. Smoke detectors, temperature sensors, humidity sensors, light sensors, chemical and gas sensors, and other types of sensors can collect data specific to their respective types. The primary responsibility of this layer is to sense the surrounding environment to gather data about it. Eavesdropping, side-channel attacks, node capture attacks, bogus data injection attacks, and various other types of assaults are all possibilities. [26] The objective of these attacks is to cause the sensor to malfunction, increase the amount of power it consumes, and steal information in the process.

The physical IoT devices with sensors, actuators, and other components are dealt with in the lowest layer. Certain researchers also know it as a sensing layer because it mostly interacts with sensors [10]. Sensors such as smoke detectors, temperature sensors, humidity sensors, light sensors, chemical and gas sensors, and others collect data pertaining to their type. This layer's principal role is to collect data from the environment via sensing it. Side-channel attacks, node capture attacks, eavesdropping [26], fake data injection attacks, and other assaults are all possible. The purpose of these assaults is to leak information, increase power consumption, and cause the sensor to fail.

2.1.2. Network layer

The establishment of communications between Internet endpoints and servers falls within the purview of this second tier of the protocol stack. When information is delivered to it from the perception layer, it may perform an analysis on the data. Phishing, denial-of-service attacks, distributed denial-of-service attacks, routing attacks, access assaults, and other typical attacks may all succeed against this layer [10, 11, 9].

2.1.3. Middleware layer

You may think of this as the next layer in the network stack. The purpose of this layer is to facilitate communication between the network layer and the application layer. This is the ”processing layer,” another name for it. It’s helpful as both a storage facility for information and a computing environment. In addition, APIs are provided to accommodate all of the needs of the application layer. The middleware layer includes components such as brokers, data storage determination, queuing systems, and machine learning. While this layer is crucial to the development of a safe and reliable IoT application, it is also susceptible to a wide range of attacks. Once in place, the malicious middleware may exert control over the IoT infrastructure and issue harmful orders. SQL injection, signature attacks, man-in-the-middle attacks, and many more are only a few examples of the many different forms of assault. Database and cloud security have now reached the pinnacle of importance.

2.1.4. Application layer

You’ve reached the last stage of the process. With tailored applications, it’s easy for the user and meets their specific needs. A large number of IoT use cases, such as ”smart cities,” ”smart homes,” ”smart grids,” ”healthcare,” and many more, are defined at the application layer. The themes of data theft, privacy invasion, and security are discussed here. In these other systems, the application would sit on top of yet another business layer. This would function as a buffer between the software and the end user. The business layer manages the IoT architecture and is therefore accountable for things like user data security, financial management, and app management. The major goal of this layer is to foil any attempts at data theft.

2.2. Protocols

As shown in Figure 3, there are numerous protocols at each tier of the IoT system. Some protocols are similar to traditional IT systems, but others are unique to the IoT communication system. The protocols in question are IEEE 802.15.4, NFC, ZigBee, BLE, RPL, 6LoWPAN, and CoAP.

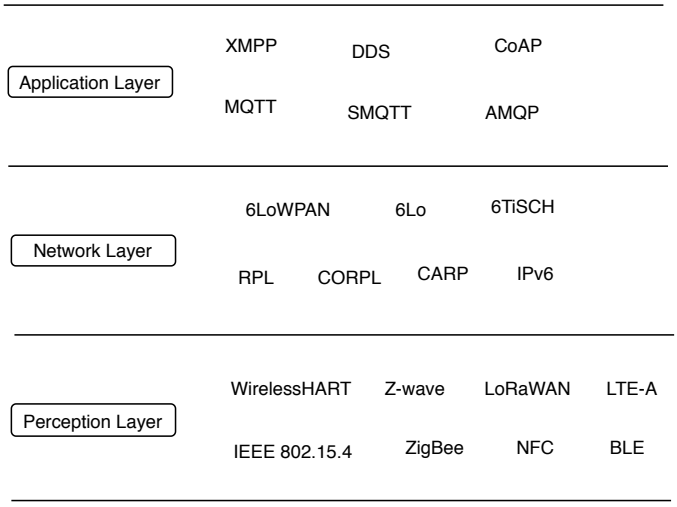

Fig. 3: IoT protocols at each layer.

2.2.1. IEEE 802.15.4

For the physical and link (MAC) levels of a typical IP stack and the perception layer of an IoT stack, the most popular standard used in Internet of Things architecture is IEEE 802.15.4. It enables communication over small distances while using little power and having a low overall cost. Because resource-constrained devices need minimal power, small frame sizes, and low bandwidth, it is best suited for using these devices. The coding method used in IEEE 802.15.4 has built-in redundancy, which improves the reliability of the connection, enables us to identify data loss, and permits the retransmission of packets that have been lost. Short 16-bit link addresses are also supported by

the protocol, which helps reduce the overall size of the header as well as the communication overheads and memory requirements [21].

2.2.2. NFC

Mobile devices can communicate a small distance of just a few millimeters using near-field communication (NFC), a kind of wireless communication with a minimal range. Simply coming together two devices outfitted with NFC and putting them into proximity allows for the instant transmission of any and all forms of data. RFID is the foundation for this technology. The data transmission between two NFC-enabled devices is accomplished by utilizing fluctuations in the magnetic field. High-frequency RFID and Near Field Communication use the 13.56 MHz frequency spectrum as their operating bandwidth. Active and passive are the two modes of operation that may be used. When operating in the active mode, both of the devices are responsible for the generation of magnetic fields; however, when operating in the passive mode, only one of the devices is responsible for the era of the area, and the other device relies on load modulation to transmit data [14]. To make the most efficient use of energy, battery-powered devices might benefit from using the passive mode. One advantage of the necessity of proximity between devices is that it is helpful for secure transactions such as payments. This is because the devices must be in close contact to one another. Note, last, that in contrast to RFID, NFC may be utilized for communication in both directions. Consequently, the vast majority of cellphones available on the market today support NFC.

2.2.3. ZigBee

PANs, which are ”personal area networks,” use it since it adheres to the communication protocol standard defined by IEEE 802.15.4 [5]. In the past, the low-power MAC and physical layers of the IEEE 802.15.4 standard have been dissected and investigated. Zigbee was developed by the Zigbee alliance, whose primary objective is to facilitate the production of communication solutions that are trustworthy, economical, and low in their overall energy consumption. Communication between Zigbee devices can only take place over a distance of a few metres at most (10–100 meters). Additionally, the Zigbee standard offers a set of requirements regarding the component elements and functionalities of the network and application layers. In contrast to Bluetooth Low Energy, this network layer provides support for the multihop routing protocol. In addition to a single Zigbee coordinator, a Zigbee network contains one of each of the following types of devices: a Fully Functional Device (abbreviated as FFD), a Reduced Functional Device (abbreviated as RFD), and a Fully Functional Device (RFD). It is possible for a node in the FFD to additionally perform the duties of a router. Zigbee may function in a star, tree, or mesh topology depending on the situation. The topology determines the implementation of the routing mechanism that should be used. Zigbee also has additional properties, like the ability to identify and maintain routes, support for nodes joining and exiting the network, short addresses that only need 16 bits, and multihop routing.

2.2.4. BLE

The Bluetooth Special Interest Group was the organisation that was in charge of the development of Bluetooth Low Energy, which is more generally known as ”Bluetooth Smart.” It requires a far lesser amount of energy to operate and has a much shorter range than other technologies, which are the alternatives. The protocol stack that BLE makes use of is analogous to the one that conventional Bluetooth technology makes use of. The controller and the host are the two parts that make up the whole thing. The implementation of both the physical layer and the link layer falls within the purview of the controller.

With conventional Bluetooth, the connection remains established even if no data is being sent or received. Furthermore, it allows for 79 data channels, each having a bandwidth of 1 MHz and a symbol rate of 1,000,000 Hz. However, Bluetooth Low Energy (BLE) only allows for 40 tracks, has a channel bandwidth of 2 MHz (twice that of standard Bluetooth), and a transmission throughput of 1 million symbols per second. Due to the tiny packet size and quick transmission time of BLE, the protocol may function with minimal duty cycle needs. Furthermore, the BLE protocol stack facilitates IP-based communication. When comparing BLE to Zigbee, its energy efficiency is around 2.5 times better.

2.2.5. Routing Protocol for Low power and Lossy Network (RPL)

The RPL protocol is a novel kind of routing technology developed specifically for IoT gadgets. This protocol is used in 6LoWPAN networks and has a small footprint. Using the nodes already present in the network and the Objective Function (OF) as a linking mechanism, RPL generates a Destination-Oriented Directed Acyclic Graph (DODAG). It makes use of an Internet Protocol version 6 address as its means of self-description. A further feature of this list is that each node remembers its neighbouring DODAG nodes. Nodes, excluding the root node, may have 0-1 or 2-4 parents. Starting with the root node and moving outwards to the child nodes, the network's topology is ranked from lowest to highest. RPL's ICMPv6 control messages are known by their acronyms: DODAG Information Object (DIO), DODAG Information Solicitation (DIS), and Destination Advertisement Object (DAO)/Destination Advertisement Object Acknowledgement (DAO-ACK). DIO messages are used to store and update information about routing paths. DAO messages, when read from the top down, publish the routing data sent between the child node and the sink node. Existing nodes provide DAO messages in the form of DIO messages to assist with the addition of a new node to the network. There is a special message type called DAO-ACK that may be used to confirm receipt of a DAO message.

2.2.6. CoAP

If you're looking for an alternative to HTTP, consider switching to CoAP. It's the standard for most Internet of Things applications [39]. It's not just another HTTP variant; it also has enhancements for limited application contexts [50]. The EXI (Efficient XML Interchanges) data format utilises binary, making it far more space-efficient than the HTML/XML standard that uses plain text. A few more capabilities include built-in header compression, resource discovery, auto-configuration, asynchronous message exchange, congestion control, and support for multicasting. All of these functions are standard. The four different types of messages that may be sent using CoAP are non confirmable messages, confirmable messages, reset (nack) messages, and acknowledgement messages. Confirmable messages guarantee that data delivered over UDP will reach its destination uncorrupted. You are welcome to put your response directly inside the acknowledgement that you sent. In addition, the Datagram Transport Layer Security protocol, often known as DTLS, is used for further protection.

3. IoT Applications

The Internet of Things encompasses various domains, and intelligent application developments have been in each of these domains. These applications are developed to make one's life simpler. Although preliminary study indicates that Internet of Things (IoT) devices improve people's quality of life, exercising care when using these technologies is important. The Internet of Things sees a daily rise in the number of applications. IoT applications have been implemented in many different industries, including home automation, smart cities, the healthcare sector, track fitness, environmental protection, the industrial sector, and smart metering. These are just some of the examples of what can be done with IoT. Before integrating smart technology into everyday life, there are important safety considerations to consider. This section will also discuss the security concerns associated with the Internet of Things applications.

4. Application Security Challenges and Possible Solutions for IoT

A wide variety of devices are linked together through an IoT. It makes everything accessible at any time and place, considerably streamlining daily living. As a consequence, everything is interrelated, which results in the formation of vulnerabilities. For the Internet of Things to become part of everyday life, students must major in security and privacy [18]. Consequently, it has to have an architecture that can manage security and other difficulties, such as illegal access, a flood of requests, and the loss of data. As was said before, many assaults are capable of taking place at any one moment inside the devices.

Unauthorized access is the most severe issue that Internet of Things devices must deal with. Because there are billions of Internet of Things devices already available, connecting them presents a substantial security risk and adds a layer of complexity. It is necessary to formalize many linked devices on a single platform. Authentication and identification of Internet of Things-based connected devices depending on the system architecture [9, 11, 13].. When a customer uses a product, the manufacturer is required to evaluate any potential safety risks. The vast majority of IoT devices do

not have their security updated. As time passes, the devices need to obtain updated versions of their security software. If it is not acquired, the devices are secure when purchased; nevertheless, as time passes, they become less safe and more susceptible to attacks. As a direct consequence, there must be continuous enhancements to security.
Another problem is the use of default passwords. When a customer purchases an Internet of Things device, the product can already have the login and password "admin" pre-set. Because they have weak credentials and login data, almost all IoT devices are susceptible to having their passwords hacked. Mirai was the first piece of malware to target Internet of Things devices; it emerged in late 2016 and infected over 600,000 devices across the world [3]. The success of the Mirai botnet may be attributed to the fact that it used attacks with default usernames and passwords. The WannaCry ransomware attack, which affected millions of devices in 2017, is a further illustration of an Internet of Things botnet [8, 31].

Table 1: Survey on Security mechanisms used for IoT applications.

Paper	Title	IoT application	Attack specific / Privacy preserving	Security mechanism used	Experimental / Simulation
[23]	SmartEdge: A framework that encrypts data from beginning to finish, designed specifically for use in edge-enabled smart city applications	Smart city	No attack identification, privacy preserving model	At the network edge and cloud data centres, they carried out the computationally demanding jobs. Additionally, a secure link was established between the smart core devices for multimedia streaming using a lightweight symmetric encryption approach.	Experimental
[6]	SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks	Smart city	Distributed Denial of Service (DDoS)	Estimated-weighted moving average (EWMA) filters have been developed using a modified version of the Secure and AgiLe model. Proactive, Active, and Passive filters have all been suggested and put into practise to calculate the dynamic threshold in real time for diverse purposes.	Mininet Emulator

Table 1 continued..

[40]	Blockchain and Fog Based Architecture for Internet of Everything in Smart Cities	Smart city	No attack identification, privacy preserving model	Authors proposed the Blockchain and Fog based security Architecture Network (BFAN) for sensitive data and used encryption, authentication. It is a two layer architecture i.e., fog node and Internet of Everything (IoE) layer.	iFogSim simulator
[28]	PrivySharing: A blockchain-based infrastructure enabling safe data exchange in smart cities while protecting privacy.	Smart city	No attack Identification, privacy preserving model	By segmenting the blockchain network into several channels, each of which is made up of a limited number of approved businesses, the data privacy is maintained. The REST API offers two layers of security in the form of an API Key and OAuth 2.0, allowing users to communicate with the blockchain network.	Simulation
[34]	Models of anomaly detection for use in intelligent home security systems	Smart home	DDoS attack detection	Hidden Markov Model (HMM) is used in smart homes to identify anomalies. A testbed with several sensors and devices is used to generate the network sensor data on which the HMM is trained.	Experiment

Table 1 continued..

[30]	IoT security and privacy using an effective Lightweight Integrated Blockchain (ELIB) paradigm	Smart home	No attack identification, privacy preserving model	The ELIB architecture creates a layer network that allows highly equipped resources to blend together to form a public blockchain that validates both privacy and security. A lightweight consensus algorithm, certificateless cryptography (CC), and a Distributed Throughput Management (DTM) scheme are the three optimizations that make up the set of three that are included with the ELIB model.	Network Simulator 3 (NS3)
[38]	Shsec: architecture for the internet of things that is built on a secure smart home network using SDN.	Smart home	DDoS attack detection	In order to develop and implement protection, including threat prevention, and to mitigate network security assaults, secure smart house (SHSec) architecture works as a controller with KNOT in smart homes.	Simulation
[2]	A Supervised Intrusion Detection System for Internet of Things Devices Installed in Smart Homes	Smart home	DoS/DDoS, Man-in-the-middle (MITM), Reconnaissance, Replay, Spoofing attack detection	They proposed a three layer supervised learning based intrusion detection system (IDS) to detect the cyber-attacks. Their model classify the normal behavior, identifies the malicious packets, and classify the type of attack happened.	Experiment

Table 1 continued..

[42]	SybilWatch: a novel approach to detect Sybil attack in IoT based smart health care	Smart Healthcare	Sybil attack detection	They proposed Enhanced Privacy-Aware Smart Health (E-PASH) which uses a lightweight encryption algorithm i.e., used to transfer health record from using prime order grouping in encrypted form. They also used Bluetits detection algorithm at detection phase to detect sybil attack by using node traceability.	NS3 simulator
[25]	IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application	Smart Healthcare	Man-in-the-middle (MITM) attack detection	Their approach consists energy-efficient clustering and cross layer attack detection and evaluation. They used probability computation for selecting cluster head (CH). Cross-layer trust evaluation approach used to evaluate nodes to detect the MIMA attack.	NS2 simulator
[17]	BSN-Care: A secure IoT-based modern healthcare system using body sensor network	Smart Healthcare	Replay and Forgery attack	They proposed secure BSN-care architecture to achieve the data security as well as network security. To achieve the security they proposed lightweight anonymous authentication protocol for network security and authenticated encryption scheme offset codebook (OCB) mode for data security.	Simulation

Table 1 continued..

[43]	Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud	Smart Healthcare	Eavesdropping, spoofing, and false data response	They combined IoT with edge cloud (IE) and named data networking (NDN) to achieve IE-based medical data retrieval and also secure the services with ciphertext and signature to enhance security. They reduced the data retrieval latency and cost.	Simulation
[27]	Blockchain and IoT based food traceability for smart agriculture	Smart agriculture	Security architecture	They proposed a model to make open, secure, trusted, decentralized and temper-proof system for LoRaWAN using blockchain technology. They integrated LoRaWAN IoT and blockchain technology.	theoretical approach
[19]	An Application to Smart Agriculture Based on an Energy-Efficient and Secure Internet of Things-Based Wireless Sensor Network Framework	Smart agriculture	Data privacy preservation	They used smart agriculture sensors to capture the relevant data and used multi-criteria decision function to form cluster heads (CH). Data transmission security is provided by using the recurrence of the linear congruential generator.	NS2 simulator

Table 1 continued..

[32]	A smart irrigation system that is both intelligent and safe, based on fuzzy logic and blockchain technology	Smart agriculture	Security architecture	They suggested a smart watering system, often known as a SWS, for use in intelligent agriculture. Sensors are used to gather data, and then the sensed data is processed on the server by SWS in order to provide a prediction of the watering schedule utilising blockchain technology and fuzzy logic. SWS is designed in Android for the purpose of intelligent consumption in gardens or fields of a small or medium size. Remotely monitoring and interacting with the programme is possible for many users and devices.	Experimental

A considerable danger of flooding the open cryptocurrency market is posed by the breach of blockchains, Internet of Things botnet miners, and manipulation of data integrity. Applications, frameworks, and platforms for the Internet of Things built on blockchain technology must be managed and monitored regularly. It is possible that in the future, it may need an upgrade to prevent new cryptocurrency abuses. IoT devices will become increasingly commonplace in our day-to-day lives, which means that organizations will have to deal with hundreds of thousands, if not millions, of IoT devices. The problems may be divided into two categories: preventing attacks on IoT devices and preventing theft of user data. Implementing robust legal and regulatory frameworks is one way these problems might be resolved [44]. The significance of authenticating information is not lost on any of us. Although symmetric-key cryptography's processing cost is higher, public-key cryptography is generally considered the more secure method. Consequently, the primary challenge faced by the Internet of Things (IoT) systems is reducing the computational resources required for public-key cryptography and other security protocols [47]. Table 1 presents the results of an investigation of the kinds of safety precautions used for different Internet of Things applications.

5. Research Opportunities

The first layer is the perception layer, which uses sensors to collect data. Sensors such as movement, camera, light, global positioning sensor (GPS) sensors, temperature sensors, and others are utilized in IoT devices. These sensors are used in IoT-based devices to detect motion, forecast the distance between nearby devices, detect smoke, and detect fire. Actuators are employed at this stratum as well. The actuator is a device that converts electrical energy into a different form of energy to change the environment. Speakers, motors, heating elements, and cooling components are examples of actuators. Actuators come in three different categories, depending on the operation: electrical, hydraulic, and pneumatic. A smart home system is the most excellent example of using sensors and actuators. Many sensors

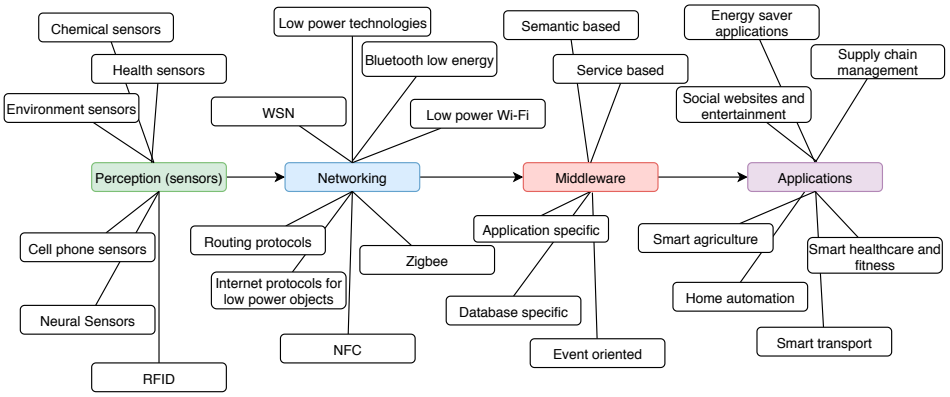

Fig. 4: Research taxonomy of Internet of Things technologies (layered wise).

and actuators are used in the home to lock and unlock doors, turn on and off lights, turn on and off other electrical appliances, and control the alert system, thermostat, and digital finger. Researchers can work in this approach to improve the accuracy of real-time data detection with sensors. Another consideration at this layer is the preservation of privacy. Figure 4 depicts the various research options available.

Next comes the networking layer, which facilitates communication and comprises various network infrastructure and protocols. Different networks use different protocols to make connections (see Figure 3 for more information) [45]. Common forms of low-power, short-range communication nowadays include Radio Frequency Identification (RFID) and Near Field Communication (NFC) (NFC). It supports Bluetooth, Zigbee, and Wireless Fidelity (Wi-Fi) for low to moderate speeds. Because of the distributed nature of IoT devices, your specialized protocols have been included in the architecture at all levels. It is possible to adapt protocols to the specific requirements of IoT gadgets. Attack detection and prevention fall within this layer's purview. Thus, it's crucial that any authentication system used there be both lightweight and efficient to accommodate the restricted resources of IoT devices. To achieve this goal, researchers need establish an essential means of communication among themselves.

The middleware and application layers are combined into a single layer in the IoT architecture with three levels. An abstraction is made available to the programmer via the middleware layer. By supplying various services, this layer also helps promote the interoperability of smart devices. Just a few examples of open source and commercial middleware services are OpenIoT [41], FiWare [46], Hydra [15]. Applications that use the Internet of Things have been put to use in several different contexts [35].. Automation of the home, tracking of fitness and health, monitoring of either, intelligent transportation systems, protection of the environment, intelligent cities, social life and entertainment, and industrial settings are only some of the applications of the internet of things. Constrained Application Protocol (CoAP) [7], Message Queuing Telemetry Transport (MQTT) [22], and Extensible Messaging and Presence Protocol (XMPP) [37] are some of the alternative protocols that may be used for the Internet of Things applications on the application layer. Each protocol has to be expanded in order to maintain its level of security. As a consequence, researchers could think of working in this manner.

6. Conclusion

The IoT, or Internet of Things, is a widely deployed network that connects everyday objects and services. There is a trade-off between the convenience and security that intelligent Internet of Things devices provide: increased vulnerability to attackers. The absence of standards in the Internet of Things allows any device to be connected to it. As a result, it's open to attack. In this study, we introduced the protocols and layered architecture of the IoT and provided an overview of their utilisation (IoT). Each IoT application's security flaws were detailed. We have also shown the IoT architecture that is becoming the norm and analysed the security issues at each level (i.e., perception layer, network layer, and application layer). The number of devices connected to the Internet (IoT) continues to grow. Wise yet vulnerable, IoT gadgets make people's lives easier while also posing risks to their privacy and security. Due

to the lack of standards, the IoT is susceptible to attack since any device may join. This talk provided an introduction to the protocols and layered architecture of the IoT. Every IoT application we looked at had serious security flaws, and we pointed them out. Furthermore, we have investigated the vulnerabilities in the IoT's architecture at every level.

References

[1] Afzal, B., Umair, M., Shah, G.A., Ahmed, E., 2019. Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges. Future Generation Computer Systems 92, 718–731.

[2] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., Burnap, P., 2019. A supervised intrusion detection system for smart home iot devices. IEEE Internet of Things Journal 6, 9042–9053. doi:10.1109/JIOT.2019.2926365.

[3] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al., 2017. Understanding the mirai botnet, in: 26th {USENIX} security symposium ({USENIX} Security 17), pp. 1093–1110.

[4] Ashton, K., et al., 2009. That 'internet of things' thing. RFID journal 22, 97–114.

[5] Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A., Hu, Y.F., 2007. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards. Computer communications 30, 1655–1695.

[6] Bawany, N.Z., Shamsi, J.A., 2019. Seal: Sdn based secure and agile framework for protecting smart city applications from ddos attacks. Journal of Network and Computer Applications 145, 102381.

[7] Bormann, C., Castellani, A.P., Shelby, Z., 2012. Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Computing 16, 62–67.

[8] Brewer, R., 2016. Ransomware attacks: detection, prevention and cure. Network Security 2016, 5–9.

[9] Choudhary, S., Kesswani, N., 2018. Detection and prevention of routing attacks in internet of things, in: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 1537–1540.

[10] Choudhary, S., Kesswani, N., 2019. A Survey: Intrusion Detection Techniques for Internet of Things. International Journal of Information Security and Privacy (IJISP) 13, 86–105.

[11] Choudhary, S., Kesswani, N., 2019. Cluster-based intrusion detection method for internet of things, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1–8.

[12] Choudhary, S., Kesswani, N., Majhi, S., 2021a. An ensemble intrusion detection model for internet of things network .

[13] Choudhary, S., Kesswani, N., et al., 2021b. A hybrid classification approach for intrusion detection in iot network. Journal of Scientific and Industrial Research (JSIR) 80, 809–816.

[14] Coskun, V., Ozdenizci, B., Ok, K., 2013. A survey on near field communication (nfc) technology. Wireless personal communications 71, 2259–2294.

[15] Eisenhauer, M., Rosengren, P., Antolin, P., 2009. A development platform for integrating wireless devices and sensors into ambient intelligence systems, in: 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, IEEE. pp. 1–3.

[16] Flashpoint, . Mirao Botnet Linked to Dyn DNS DDoS Attacks. Accessed: April 21, 2020. URL: https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/.

[17] Gope, P., Hwang, T., 2015. Bsn-care: A secure iot-based modern healthcare system using body sensor network. IEEE sensors journal 16, 1368–1376.

[18] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems 29, 1645–1660.

[19] Haseeb, K., Ud Din, I., Almogren, A., Islam, N., 2020. An energy efficient and secure iot-based wsn framework: An application to smart agriculture. Sensors 20, 2081.

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

[21] Hui, J.W., Culler, D.E., 2008. Extending ip to low-power, wireless personal area networks. IEEE Internet Computing 12, 37–45.

[22] Hunkeler, U., Truong, H.L., Stanford-Clark, A., 2008. Mqtt-s—a publish/subscribe protocol for wireless sensor networks, in: 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), IEEE. pp. 791–798.

[23] Jan, M.A., Zhang, W., Usman, M., Tan, Z., Khan, F., Luo, E., 2019. Smartedge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications 137, 1–10.

[24] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. Computer 50, 80–84.

[25] Kore, A., Patil, S., 2020. Ic-mads: Iot enabled cross layer man-in-middle attack detection system for smart healthcare application. Wireless Personal Communications , 1–20.

[26] Liao, C.H., Shuai, H.H., Wang, L.C., 2018. Eavesdropping prevention for heterogeneous Internet of Things systems, in: 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE. pp. 1–2.

[27] Lin, J., Shen, Z., Zhang, A., Chai, Y., 2018. Blockchain and iot based food traceability for smart agriculture, in: Proceedings of the 3rd International Conference on Crowd Science and Engineering, pp. 1–6.

[28] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W., 2020. Privysharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security 88, 101653.

[29] Mashal, I., Alsaryrah, O., Chung, T.Y., Yang, C.Z., Kuo, W.H., Agrawal, D.P., 2015. Choices for interaction with things on Internet and underlying issues. Ad Hoc Networks 28, 68–90.
[30] Mohanty, S.N., Ramya, K., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S., Khanna, A., 2020. An efficient lightweight integrated blockchain (elib) model for iot security and privacy. Future Generation Computer Systems 102, 1027–1037.
[31] Mohurle, S., Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science 8.
[32] Munir, M.S., Bajwa, I.S., Cheema, S.M., 2019. An intelligent and secure smart watering system using fuzzy logic and blockchain. Computers & Electrical Engineering 77, 109–119.
[33] Peña-López, I., et al., 2005. ITU Internet report 2005: the internet of things .
[34] Ramapatruni, S., Narayanan, S.N., Mittal, S., Joshi, A., Joshi, K., 2019. Anomaly detection models for smart home security, in: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), IEEE. pp. 19–24.
[35] Ranganathan, A., Al-Muhtadi, J., Chetan, S., Campbell, R., Mickunas, M.D., 2004. Middlewhere: a middleware for location awareness in ubiquitous computing applications, in: ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing, Springer. pp. 397–416.
[36] Said, O., Masud, M., 2013. Towards internet of things: Survey and future vision. International Journal of Computer Networks 5, 1–17.
[37] Saint-Andre, P., et al., 2004. Extensible messaging and presence protocol (xmpp): Core .
[38] Sharma, P.K., Park, J.H., Jeong, Y.S., Park, J.H., 2019. Shsec: sdn based secure smart home network architecture for internet of things. Mobile Networks and Applications 24, 913–924.
[39] Shelby, Z., Hartke, K., Bormann, C., 2014. The constrained application protocol (coap) .
[40] Singh, P., Nayyar, A., Kaur, A., Ghosh, U., 2020. Blockchain and fog based architecture for internet of everything in smart cities. Future Internet 12, 61.
[41] Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J.P., Riahi, M., Aberer, K., Jayaraman, P.P., Zaslavsky, A., Žarko, I.P., et al., 2015. Openiot: Open source internet-of-things in the cloud, in: Interoperability and open-source solutions for the internet of things. Springer, pp. 13–25.
[42] Vaishnavi, S., Sethukarasi, T., 2020. Sybilwatch: a novel approach to detect sybil attack in iot based smart health care. Journal of Ambient Intelligence and Humanized Computing , 1–15.
[43] Wang, X., Cai, S., 2020. Secure healthcare monitoring framework integrating ndn-based iot with edge cloud. Future Generation Computer Systems .
[44] Weber, R.H., Studer, E., 2016. Cybersecurity in the internet of things: Legal aspects. Computer Law & Security Review 32, 715–728.
[45] Whitmore, A., Agarwal, A., Da Xu, L., 2015. The internet of things—a survey of topics and trends. Information systems frontiers 17, 261–274.
[46] Zahariadis, T., Papadakis, A., Alvarez, F., Gonzalez, J., Lopez, F., Facca, F., Al-Hazmi, Y., 2014. Fiware lab: managing resources and services in a cloud federation supporting future internet applications, in: 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, IEEE. pp. 792–799.
[47] Zhang, Z., Cho, M.C.Y., Wang, C., Hsu, C., Chen, C., Shieh, S., 2014. Iot security: Ongoing challenges and research opportunities, in: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234.