Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Understanding IoT Working, Architecture and Protocols for Enhancing IoT Security: Strategies to Mitigate Cyber Threats

Ashwathi C[1,2*] and Jubilant J Kizhakkethottam[2,3†]

[1*]*Computer Science Department, Saintgits College of Engineering, Pathamuttom, Kottayam, 686532, Kerala, India.*
[2]*Computer Science Department, Saintgits College of Engineering, Pathamuttom, Kottayam, 686532, Kerala, India.*
**Corresponding author(s). E-mail(s): ashwathi.se2325@saintgits.org; Contributing authors: jubilant.j@saintgits.org;*
[†]*These authors contributed equally to this work.*

ARTICLE INFO

Received: 17 Nov 2024

Revised: 29 Dec 2024

Accepted: 12 Jan 2025

ABSTRACT

5G and 6G telecommunications development, big data, communication among machines (M2M), the global web, and the internet of things (IoT) are the key pillars of the next generation of technological platforms. The Internet of Things (IoT) is a revolutionary approach which is rapidly gaining traction both inter- nationally and domestically. It is smart, intelligent, autonomous, and portable. Numerous cutting-edge technologies are included into the Internet of Things, including blockchain, machine learning, and Artificial Intelligence (AI). This new trend is introducing various technologies, such as cloud computing, virtualization, cyber-physical systems, and the semantic web. This chapter provides a basic explanation of various IOT networks and the five layer architecture that IoT devices use to share information and function as smart, portable systems or applications. This research gathers up-to date information on all facets of the Internet of Things, such as standards, technology, risks, security, and remedies offered by IOT protocols. IoT protocols must address security breaches and security issues with data privacy, authentication, authorization, and trust management in a distributed, heterogeneous environment. We discussed the various attacks that might happen on the Internet of Things environment and the precautions that need to be taken in-depth.

Keywords: IoT security protocols, IoT security framework, IoT threats and attacks, Data privacy

1 INTRODUCTION

IoT continues to rank among the top three business IT priorities, per the most recent 148-page State of IoT – Spring 2024 report. Even though AI is now more important to businesses than IoT, the $236 billion IoT market is expected to benefit from the growing combination of AI and IoT rather than suffer competition. According to estimates, the annual financial impact of IoT is expected to reach $731 billion by 2030. The explosive growth of the Internet of Things (IoT) in the last few decades has fundamentally altered how we utilize various systems and gadgets that are a part of the infrastructure of information and communication technology (ICT), operate, and connect with one another. The Internet of Things is widely acknowledged to have started from wireless ad hoc networks, which allow direct connectivity between devices using wireless nodes.

IoT is having a big impact on a lot of application domains, including manufacturing, smart homes, energy, healthcare, transportation, and agriculture. The Internet of Things (IoT) includes sensors, software, and other technologies in daily appliances like fans, lights, refrigerators, heaters, and industrial machines as well as devices that can collect and share data. This connectivity enables automation, remote control, and real-time monitoring, which increases production and creates new opportunities in a variety of industries.

The key benefits of an IOT protocol that is standardized, and the accuracy and continuous monitoring are attributed to its standardized architecture. More access to our smart, IoT-connected devices is available to threats. Let's discuss about the threats and counter measures in later section. The main contributions of the paper are:

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- The history of the Internet of Things and the current security and privacy regulations are the two key lessons to be learned from this discussion.
- A thorough description of how the devices in the IoT ecosystem work.
- A thorough examination of the Internet of Things' architecture and various layers.
- A summary of current IoT security risks and countermeasures.

2 INTERNET OF THINGS [IOT]

In 1999, Kevin Ashton gave the first presentation on the idea of the Internet of Things (IoT). According to Ashton," The Internet of Things has the capacity to alter the world in the same way that the Internet did." Perhaps even more so. Later, in 2005, the International Telecommunication Union (ITU) made the Internet of Things fully official.

The term" Internet of Things" (IoT) describes a network of connected systems and devices that can communicate with one another over the internet. The Internet of Things (IoT) is the idea of interconnected devices that may exchange information, collect information from their surroundings, analyses it, and transmit the results to accomplish a certain objective.

IoT has made it possible to computerize numerous aspects of life today, including Smart Homes, which can be remotely monitored and controlled for multiple functions and equipment, including cooling and heating, lighting, and safety surveillance. Other facets of life for people have also been impacted, resulting in the creation of smart industries, smart farming, smart health care, and smart education systems, among others. The majority of IoT devices linked by wireless sensor networks (WSN), have minimal batteries, and minimal computational capability

3 APPLICATIONS OF IOT

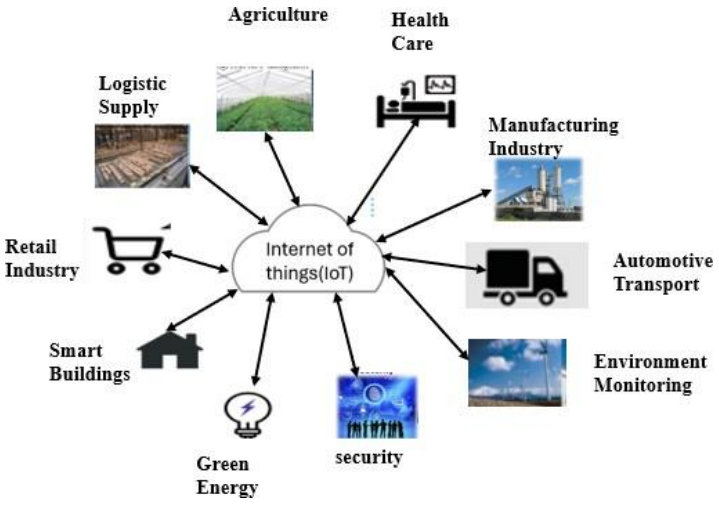

Fig. 1: Application Domains of IoT

IoT is anticipated to be used for a variety of purposes, including those described in above Figure 1, from household use to space applications.

1. Low power applications:

Smart homes, offices, cities, streetlights, metering, intelligent transportation systems (ITS), which include Vehicular communications (VANET, V2X), intelligent security systems, and disaster relief operations are examples of low power applications.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. **Sensor-based applications:**

Among machines (M2M) communication, smart transportation systems (ITS, autopilot, etc.), automated manufacturing (failure prediction, etc.), wearable device-based fitness tracking, statistical data analysis, weather surveillance, agriculture, and climatic disaster/status tracking (water height in a dam, etc.)

3. **Tactical applications**

Wireless robots, rocket travel, hazardous mines, drones (UAVs), and mission-critical Defense applications (such as military ad hoc communications and marine ship area ad hoc networks, among others).

4 WORKING OF IOT

The perception layer, network layer, middleware layer, application layer, and business layer are the five levels that make up Internet of Things architecture as shown in Figure 2. Every layer has its own functionality and protocols. In a later section, they are described. The fundamental components of an Internet of Things system are sensors, gateways, processors, and applications. To create a functional Internet of Things system, each of these nodes have unique qualities.

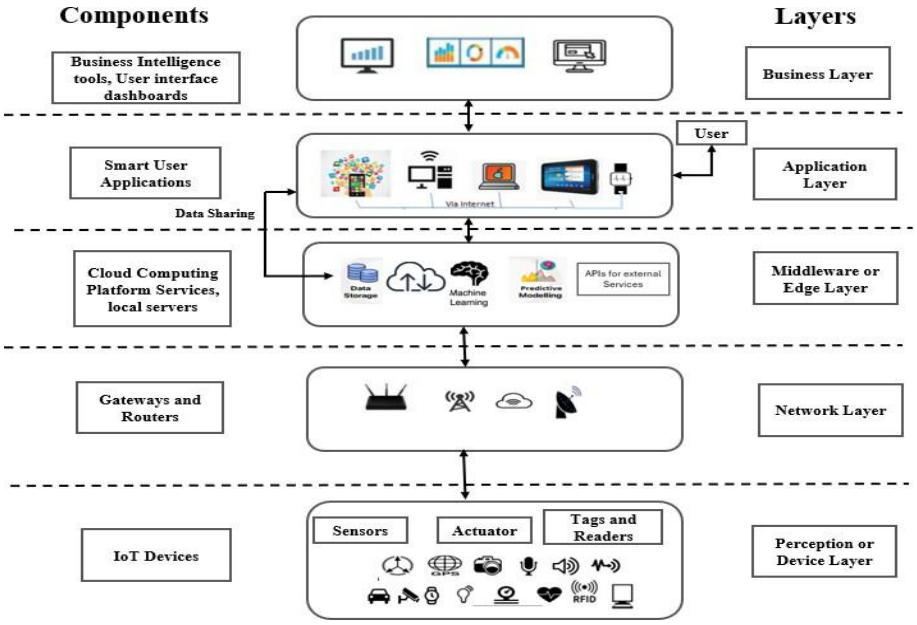

Fig. 2: Working of IoT Ecosystems

Sensor and actuator devices, whose primary goals are command actuation and sensor data gathering. Different types of sensors may be used to measure various parameters, such as pressure, humidity, and temperature. Every one of these gadgets collects data from its surroundings. The following step involves uploading this data to the server, either directly or through a gateway, as illustrated in Figure 2. Then, using the Network layer, which is defined by a variety of network technologies, the sensor data is sent to the Middleware layer.

Information processing takes place in the middleware layer, where received data can be stored and examined using cutting-edge data analytics techniques. To correctly modify a certain parameter, IoT devices may transmit instructions to actuators based on information obtained from servers in middleware. The primary goal is to use AI models to enable autonomous decision-making. These models will then transmit actuation commands back to the physical objects, directing them to take actions that will impact the physical environment's overall conditions.

The Application layer may use the gathered and analyzed data to control the system as a whole or to provide it to an end user. This layer was limited to smart cities, smart homes, and automobiles. The primary goals of the

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Application layer are handling data and service provision. Lastly, system administrators can strategically oversee and manage the IoT platform's overall functionality with the help of Business layer. The business layer functions as the hub for all IoT system operations, including services and applications. After receiving the data from the application layer, it creates graphs, flow charts, and business models in the business layer.

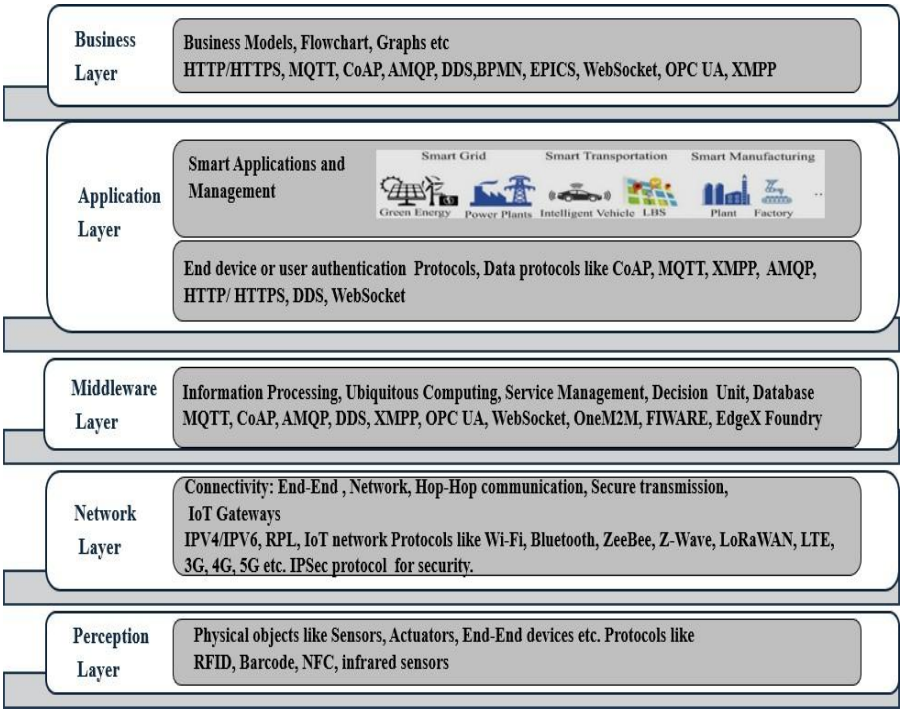

Fig. 3: IoT Architecture and Protocols

5 ARCHITECTURE OF IOT

The Internet of Things [IOT] architecture is a multilayered idea that includes protocols, standards, hardware, and software. The model that outlines how systems and devices interact with one another inside the IoT ecosystem is known as IoT architecture. It offers an organized method for joining, controlling, and gaining value from the enormous network of linked devices. The essential features of the Internet of Things architecture, such as its scalability, interoperability, real-time data processing, and capacity to leverage massive amounts of data for insightful analysis.

5.1 Different layers in IoT Architecture

IoT applications operate according to the methods used in their development, considering a variety of industry areas. The level of sophistication of various architectural layers varies according to the current industrial objective as shown Figure 2. A five- layer design is the most common and well-known format. According to the Internet of Things design, the data is dealt with, evaluated, and archived in five phases from sensor-connected devices via a network and the cloud.

1. **Perception Layer:** Device layer is another name for the perception layer. This layer facilitates gateway and device functionality. Device features include energy- saving sleep and wake cycles, as well as ad hoc networking between devices, direct and indirect connectivity with the communication network. Actuators and sensors are part of this layer. It oversees gathering environmental data and transforming it into signals that the Internet of Things system can use. Actuators, RFID tags, and sensors (temperature, humidity, motion, etc.) are some of the elements used in this layer.

2. **Network layer:** With the aid of Internet of Things network protocols, the network layer is primarily in charge of sending data to the following layer in the hierarchy. For data transmission, it makes use of both cable and wireless methods. Addition- ally, depending on the sensor devices, technologies including

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Bluetooth, Wi-Fi, 3G, 4G, and 5G as well as infrared and ZigBee can be employed. IoT data is dispersed and processed at the network's edge in this layer. Consequently, the middleware layer receives data from the device/sensor layer over this network layer.

3. **Middleware Layer:** This layer is often referred to as the processing layer or edge layer. Receiving data from the network layer and storing it in a database is the responsibility of this layer. Advanced data analytics can be used to analyze this received information. This layer processes data, does ubiquitous computation, and makes decisions automatically depending on the findings. Because IoT relates to cloud services, this layer is compatible with cloud infrastructures. As a result, this layer is primarily in charge of cloud computing processing and storage. Since these IoT devices are deployed to support various IoT services, the middleware layer is mostly employed for service administration.

4. **Application layer:** The application layer handles different applications like home automation, electronic health monitoring, etc. and is made up of the program's user interface. It puts into practice the Internet of Things' capacity to deliver enhanced smart services in response to user requests. This stage shows how industrial and Internet of Things technologies are combining to achieve intellectualization. This is the user-accessible front end of an Internet of Things application. This layer enables application administration based on the data handled by the middleware layer.

5. **Business layer:** To improve service quality, the business layer additionally assesses the outputs from each of the other four levels and analyses them with the anticipated output. Data received from the application layer is portrayed by the business layer, together with the business model. Additionally, it facilitates Big Data analysis-based decision-making processes. Furthermore, it is at this layer that the four below levels are managed and monitored.

6 TYPES OF IOT NETWORK

Four primary categories can be used to group IoT networks, protocols, cellular networks, and other networks. This classification aids in reducing the number of possibilities available for a given application.

1. **WLAN/WPAN networks**, like Wi-Fi and Bluetooth, have challenges with scaling and limited coverage, but they offer high speeds.

2. **Mesh protocols**, such as RFID, Z-Wave, and Zigbee, are made for distributed networks and have applications in the home automation, industrial, and asset tracking industries.

3. **LPWAN technologies**, such as Sigfox, LoRaWAN, and NB-IoT, are appropriate for low-power and remote applications.

4. Wide coverage and high bandwidth are provided by **Cellular Networks** such as LTE, 3G, 4G, and 5G; however, battery-powered IOT devices are unable to utilize these networks directly.

7 IOT PROTOCOLS

The selection of a protocol is influenced by various aspects, including machine-to- machine communication requirements, security, transmission area, consumption of energy, Packet size, and network bandwidth. Most procedures fall into one of three categories.

7.1 IoT Network Protocols

To facilitate smooth communication between medium- to high-power devices within the IoT ecosystem, IoT network protocols are essential.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Comparison of Network Types, Protocols, Ranges, and Data Rates

Network Type	Protocol	Range	Data Rates
WPAN	Bluetooth	1m–100m	125 Kbps–2 Mbps
WLAN	Wi-Fi	30m–100m	150–600 Mbps
Mesh	NFC	4 cm	100–424 Kbps
Mesh	Z-Wave	30m–100m	9.6 Kbps–100 Kbps
Mesh	Zigbee	10m–100m	20 Kbps–250 Kbps
LPWAN	LoRaWAN	Up to 15 Km	0.3 Kbps–50 Kbps
LPWAN	Sigfox	3Km–30 Km	100 bps–600 bps
LPWAN	NB-IOT	1Km–10 Km	Up to 250 Kbps (downlink), 125 Kbps (uplink)
Cellular	Cellular	5Km–30 Km	5 Mbps–100 Mbps (4G) 50 Mbps–3 Gbps (5G)

1. **Bluetooth**

This protocol is applicable to short-range (less than 100 m) applications and operates at the 2.4 GHz frequency. Bluetooth Low Energy (BLE) represents a further development in its evolution. BLE's low energy consumption means that batteries can now last for years at a time. For the transfer of little amounts of data from sensors or wearables, this kind can be helpful. Its high data rate, roughly 2 Mbps is evident. BLE is a strong contender for Internet of Things uses.

2. **Wireless Fidelity (Wi-Fi)**

Based on the IEEE 802.11 standard, Wi-Fi operates between 2.4 and 5 GHz in frequency. As previously indicated, the IEEE 802.11 standard is the basis for its use, mostly in homes and a variety of enterprises. It has speeds of hundreds of megabits/secs, which is suitable for file transfers but becomes excessively thirsty for power for many IoT applications. It is not commonly utilized in powered by batteries applications due to its primary downside, which is its excessive use of power.

3. **Radio Frequency Identification [RFID] Tags**

RFID tags and readers are the two components of an RFID system. To read the RFID tags, the reader sends radio signals that have been encoded. Because the RFID reader can read several tags at once, it is highly helpful for monitoring documents, tracking patients in medical circumstances, and retail logistics applications. It can even replace barcodes. The RFID tag implements the RFID system by responding to queries from the RFID reader with its identification and additional data based on the application.

4. **Near field communications (NFC)**

Communications in the Near Field (NFC): When two devices are within 1.5 inches (4 cm) of one another, NFC uses an active node, such as smartphone, to generate RFID to enable communication between them. NFC has a few centimeters of range and operates in the 13.56 MHz frequency spectrum. NFC makes it

possible for the other device to access online services via the link if one of these devices is online. The purpose of this kind of communication is to increase in-person interactions. Applications such as tap-to-pay maintain the vital function that this specialized protocol plays in day-to-day living.

5. ZIGBEE

ZigBee is a freely available protocol that combines cost, adaptability, and deploy-ability to make it easier for IoT devices to communicate with one another. Applications involving energy accumulating and sleeping end devices are a good fit for this technology. At 250 kbps, it can withstand up to 65,000 nodes. The purpose of the ZigBee RF4CE is to replace IR remotes seen on TVs and DVD players and do away with the requirement for a line of sight between the remote and the device.

6. Z-WAVE

Low-power RF communication technology serves as the foundation for this wire- less communication protocol. Additionally, it brought in the Smart-Start protocol, which allows security authorities to configure devices for the network before they are installed. It also brought in the Smart-Start protocol, which allows security authorities to configure devices to the network before they are installed. Z-wave: operating in ISM frequency bands at a rate of 30–100 Kbps, this technology is designed for home automation applications. Up to 232 devices can be allocated by it within the network.

7. SIGFOX

The low-cost M2M application areas that need wide-area coverage are the target market for Sigfox communication. ISM 868/902MHz bands are used by the proprietary LPWAN technology known as Sigfox. It uses a star network topology with DBPSK and GFSK modulation algorithms. Through AES-128, its security measures are customized. Very narrow frequency bands are used by Sigfox networks, and there is only one Sigfox network operator per nation. Sigfox devices are limited to sending and receiving incredibly tiny messages, which prevents them from being used for data-intensive tasks like firmware updates.

8. Long Range Wide Area Network (LoRaWAN)

Low-power, wide-area (LPWA) systems that run on battery Systems. An improvement on the LoRa protocol called LoRaWAN allows for direct communication over many kilometers at a distance. It usually uses star topologies, in which a collection of servers, gateways, and end nodes make up the components. With this, end-to- end encryption at the application level and network sessions between nodes and gateways are managed. The two primary benefits of low power wide area networks are multicasting and air registration/activation.

9. Narrowband IoT (NB-IoT)

The LTE FDD 180kHz frequency band is used by NB-IoT, which has three modes of operation: stand-alone, guard-band, and in-band. NB-IoT is part of the 4G LTE standard and is being integrated into 5G. It enables devices to use power-saving features, but its drawbacks include the lack of inefficient coverage and the need for multiple providers for global deployments due to the difficulty of roaming.

10. Cellular

Depending on the technology and brand choice, both low-power (like 2G) and high- data-rate (like LTE) applications can benefit from a cellular network. Additionally, there are variants of mobile communication like as NB-IoT and LTE-M that were developed to utilize less power or to offer greater data capacity, respectively. IoT devices can now be readily integrated into cellular networks. Although they need a lot more power, other technologies like 4G LTE and 5G can handle larger amounts of data, such digital video.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

11. IPSec (Internet Protocol Security)

Network links on the IP layer are secured using a method known as IPsec. It allows bilateral verification between entities in the network sharing information and uses keys to authorize data payloads. The data acquisition and processing latency will be too much for low-resource IoT gadgets to manage; IPsec is a viable solution for robust routers. An alternative in cellular technology is to outsource security to the wireless service provider, which establishes an IPsec link among the mobile network and Internet of Things apps.

7.2 IoT Application Protocols

1. MQTT (Message Queueing Telemetry Transport)

Applications and middleware can be connected to embedded devices and networks via MQTT. MQTT, which is based on the TCP protocol, works well with devices that have low bandwidth links, erratic availability of resources, or both. The three parts of MQTT are publisher, broker, and subscriber. When the publisher publishes some topics of interest, a broker will notify the registered subscriber. An interested device would register as a subscriber for specified topics. While the broker serves as the subscriber's information source, the publisher creates engaging content. For IOT and M2M communications, the MQTT protocol is perfect for sending messages. It can also be used to route small, inexpensive, low-power, and low-memory devices in networks with limited bandwidth and vulnerabilities.

2. AMQP (Advanced Message Queuing Protocol)

Message-oriented middleware (MOM) is used with the open-source AMQP protocol. Its goal is to facilitate communication across platforms, gadgets, and software from many providers; it wasn't developed especially for the Internet of Things. It has more forwarding options than only sending notifications to topics, in contrast to MQTT; however, this additional capability coupled with higher network latency and more complex app setup. AMQP uses a dependable transport protocol like TCP for message exchanges. Azure IoT supports AMQP as well for device connectivity.

3. CoAP (Constrained Application Protocol)

CoAP is intended for lossy, low-power networks, sometimes referred to as" con- strained" connections. CoAP and User Datagram Protocol (UDP) are frequently combined, which enhances its efficiency and appeals to IoT applications that prioritize battery saving. It is a specific web transfer protocol meant to be used with IoT networks with limited nodes. To provide secure communication, CoAP can be combined with Datagram Transport Layer Security (DTLS).

4. HTTP (Hypertext Transfer Protocol)

HTTP is the most widely used protocol for online browsing and data access via REST-APIs. The main advantage of utilizing HTTP for IoT is that developers who create web applications may use the identical technique—an HTTP POST request—to send data to a webserver. The use of connectionless request-respond communication in HTTP, which necessitates the inclusion of authentication information in every message and consumes data and energy, is one of its disadvantages.

5. WebSocket

WebSocket is a dual-direction communication protocol designed to enable web applications to send large volumes of information quickly. Each interaction after the initial one is made has a very small latency since a WebSocket establishes a connection between the end user and the web server. Because devices and servers may simultaneously send and gain data in actual time, this protocol is perfect for Inter- net of Things applications where minimal delay is essential, transmission happens often, and data consumption is not as important.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

6. XMPP (Extensive Messaging and Presence Protocol)

Extensible Markup Language (XML) is the foundation of the messaging system known as the Extensible Messaging and Presence system. Since instant messaging (IM) was the original purpose of XMPP, the cost associated with exchanging presence data and lack of device optimization for devices with limited memory can be explained. Nevertheless, XMPP defines a device's identity, makes it easier to communicate across platforms, and permits the defining of the message format, handling extremely well-structured data. This open-source technology is continually being improved with new IoT-related advancements and is very accessible.

7. Data Distribution Service (DDS)

DDS emphasizes communication that is data centric. It is very helpful for Complex IoT systems because it is made to provide scalable, real-time, and high-performance data transmission between remote systems. Data integrity, confidentiality, and access control are guaranteed by the integrated security elements in DDS. It facilitates the dynamic discovery of data providers and consumers, which makes system setup adaptable and flexible.

7.3 IoT Business Protocols

1. Open platform Communications Unified Architecture [OPC UA]

One of the most significant open-source, ubiquitous communication protocols for Industry 4.0 and the Internet IoT is OPC UA. The industrial M2M communication protocol covers it. Like MQTT, it is an independent of platforms protocol that enables request and answer messages to be sent between clients and servers to ease communication across different kinds of systems and devices. The purpose of it is to transfer data between the cloud and linked sensors. This extremely flexible protocol can also be used for non-industrial applications because it isn't restricted to any one operating system, computer language, or communication protocol.

2. Business Process Model and Notation [BPMN]

A graphical representation known as BPMN is used in business process models to express business processes, modelling, implementation, execution, monitoring, and analysis. The software design tool known as Unified Modelling Language is not the same as BPMN. The four BPMN components Swim-lanes, Artifacts (objects, group, annotation), Flow objects (events, activities, gateways), and Connecting objects (sequence flow, message flow, association).

3. Electronic Product Code Information Services [EPICS]

EPICS are significant, high-level business requirements or goals that direct the creation of features, goods, or services in the business layer of an organization. Usually found in an agile system, these epics aid in coordinating development efforts with corporate goals.

8 IOT SECURITY GOALS

1. Confidentiality

Maintaining safeguarding of private information by preventing unintentional dis- closure. To guarantee that only those with authorization and devices can access sensitive information, this includes controlling access measures, safe transmission protocols, and cryptography.

2. Integrity

Being assured all the data is true and hasn't been altered. Methods like digital certificates, checksums, and hashing aid in confirming that data doesn't change while it is transferred or saved.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

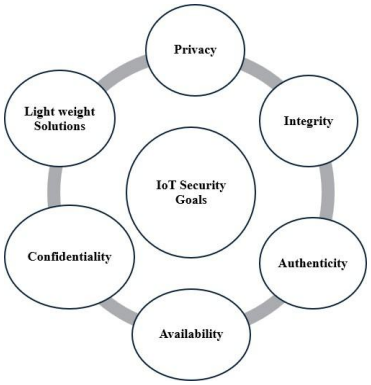

Fig. 4: IoT Security Goals

3. **Availability**

Providing guarantee that information and services are available when requested. To reduce interruptions this entails building systems that can withstand attacks (such as DDoS), adding redundancy, and maintaining backup procedures.

4. **Privacy**

Because connected IoT appliances gather so much confidential and intimate data, privacy is an important issue in IoT security. Evidently and succinctly define your privacy policies and explain the procedures for gathering, utilizing, and sharing data. Provide accountability systems, like periodic checks and evaluations of data handling procedures. A later section discusses privacy in IoT security.

5. **Authenticity**

Confirming the identity of users and devices within the Internet of Things network. Device certificates, secure key management, and robust authentication protocols are some of the techniques that can be used to accomplish this.

6. **Light weight Solution**

Lightweight solutions for IoT security are crucial, because several IoT devices are restricted in resources, processing, power, memory, and energy. The goal of lightweight IoT security solutions is to strike a compromise between resource efficiency and security. These techniques help IoT devices keep a strong security posture without using up too much of their scarce resources, which eventually promotes a safer IoT ecosystem.

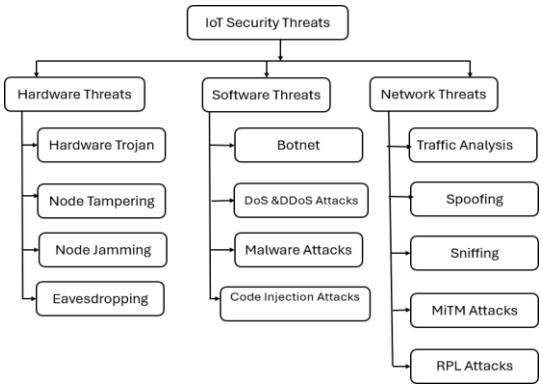

Fig. 5: IoT Security Threats

9 IOT SECURITY THREATS

Instead of focusing on a single PC, the majority of adversaries target IoT devices and infrastructure. The IoT

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

connects numerous appliances and devices, including some embedded ones. The following is a summary of the main reasons why IoT is a target:

- Each component of equipment and gadget in an Internet of things (IoT) needs to be always powered on, and it is simple for attackers to figure out which equipment is continuously in power mode.
- In an Internet of Things, gadgets and machinery are continually connected, and

an attacker can access all the connected devices from a single device.

- It is typically more difficult to protect against and handle attacks on an entire network of connected devices than it is on a single PC without the right security measures and understanding.
- Another reason why malware targets the IoT is weak passwords and improper

encryption mechanisms in connected devices.

- Compared to a single device, the IoT requires far less sophistication and is easier to use.
- Another reason why IoT is a malware target is when its equipment and gadgets

are exposed to the internet for twenty-four hours. The gadgets will accept the incoming traffic signals because of the limitless internet connection, making them susceptible to attacks.

As Shown in Figure 5 IoT security threats are categorized under Hardware threats, Software threats and Network threats. Let's us discuss in detail in this section.

9.1 Hardware Threats

Hardware risks in the context of the Internet of Things refer to flaws in the tangible parts of an IoT device that an intruder could exploit to steal data without permission, disrupt normal operations, or launch more complex assaults. In the following section, let's discuss some of the most significant hardware threats.

9.1.1 Hardware Trojans

A hardware Trojan in an Internet of Things device that describes malevolent alteration or incorporation of added components into hardware during the production process or at a later stage in the supply chain. These changes have the potential to adversely affect the safety and efficiency of the device by introducing vulnerabilities or giving attackers access through a backdoor.

1. **Functional Trojans:** These devices alter their intended functions to carry out destructive behaviors.
2. **Parametric Trojans:** Modify the parameters of the device, such as timing and power usage, to induce malfunctions or deteriorate performance.
3. **Side Channel Trojans:** These malicious software programs take advantage of unintentional data leaks from IoT devices by emitting side-channel emissions, such as irregularities in timing, electromagnetic radiation, or power usage. Differential fault evaluation, power tracking attack, electromagnetic analysis attack, and acoustic cryptography key extraction attack are methods used to carry outside channel attacks.

9.1.2 Tampering

Node tampering happens when an intruder modifies IC-related data after it has been applied. The majority of IoT devices will be installed in places without any security precautions to prevent intruders from physically gaining access to the device or from wirelessly modifying its firmware or software. The intruder can alter the behavior of an IC or device by adding malicious hardware or software.

9.1.3 Node Jamming

Jamming attacks include an adversary transmitting a high-range signal to disrupt transmission. A hacker

could potentially cause critical system crashes by using RF interference to impede IoT communication and interfere with device performance. Rogue nodes use sensor networks that broadcast jamming signals on frequencies that are identical to those of sensor nodes are known as jamming attacks. By producing noise in the IoT network, this jamming attack prevents sensor nodes from sending or receiving data, making services inaccessible.

9.1.4 Eavesdropping

Social engineering, which uses psychological tricks on people to trick them into breaking security rules, poses a danger to hardware security for the IoT. Data thefts and illegal access can result from the use of RF interference to collect and eavesdrop on wirelessly traffic between IoT devices.

9.2 Software Threats

These threats are frequently caused by inadequately managed or intended software on gadgets that are connected, which makes them a tempting target for intruders because of their frequently poor safety configurations. In the following section, let's discuss some of the most significant software threats.

9.2.1 Botnets

Botnets are internet-connected devices that have malicious software preinstalled on them. Cybercriminals find it easy to target IoT devices with limited resources since they lack robust security solutions. These devices could be transformed into fully controlled botnets by cybercriminals. Cybercriminals utilize botnets for Distributed Denial of Service (DDoS), spamming, phishing, and malware distribution. Botnet architecture might be a collaborative architecture, centralized architecture, or a hybrid of both designs.

9.2.2 DoS & DDoS Attacks

1. **A Denial-of-Service (DoS)** attacks seeks to prevent legitimate users from accessing an IoT device or service by flooding it with excessively large requests. This results in disturbances, which make the gadget or service sluggish or non-existent. An attacker might, for instance, send a deluge of requests to a smart thermostat, blocking people from changing the temperature in their homes.

2. **DDoS Assaults:** Like a DoS assault, but executed using a network of compromised devices, sometimes referred to as a botnet. Many IoT devices that have been compromised by weak security protocols may be included by these botnets. A DDoS attack might have a far bigger scope than a Dos attack.

9.2.3 Malware Attacks

Any software application that is meant to harm or crash a computer system or ecosystem is referred to as malware, or malicious software. Viruses, worms, Trojan horses, ransomware, adware, spyware, rootkits, keyloggers, wiper malware, mobile malware, etc. are a few examples of malware.

9.2.4 Code Injection Attacks

In terms of IoT security, a code injection attack is when malicious code is introduced into a system or application and then runs with the rights of the original program. The functioning and security of IoT devices might be seriously jeopardized by this kind of attack. SQL injection, command injection, Cross-Site Scripting (XSS) attacks, Buffer overflow attacks, and other attacks are examples of code injection attacks.

9.3 Network Threats

Essentially, any threat that leverages the often-inadequate security measures of IoT devices to get control to a network and its private information. Let's explore some of the biggest network threats in IoT in the section that follows.

9.3.1 Traffic Analysis

Traffic analysis is the process of looking at recorded network traffic to infer relevant information from

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

communication patterns. There are two kinds of attacks that analyses traffic: link-load analysis, which finds the traffic rate on an internet transmission connection, and flow-connectivity, which finds the rate of interconnectivity between a sender and a recipient.

1. **Foot-printing attacks:**

The initial stage of a cyberattack is called" Foot-printing," and it involves learning as much as possible about the target system to spot any possible flaws. Due to the frequently limited security mechanisms on many IoT devices, Foot-printing can be especially problematic in the context of IoT security.

2. **Network Scanning attacks:**

Network scanning attacks probe the network to find open ports, services that are available, and devices that are active. The attacks are especially troubling in the context of IoT security since there are more and more vulnerable devices that might be abused.

9.3.2 Spoofing

IoT security is threatened by spoofing, which is the act of pretending to be a user or a device to trick systems, obtain unauthorized access, or change data in network traffic. The procedure's main goals are to propagate malware, steal data, and get access to computers.

1. **Device spoofing:**

The most common spoofing attacks involve masquerading trusted IoT devices to provide deception, alter system operations, or obtain unauthorized access to a network.

2. **IP spoofing:**

To pose as reliable equipment and intercept, manipulate, or reroute messages, attackers change their IP addresses.

3. **MAC Spoofing:**

Attackers can obtain access to the network by modifying their MAC address, which allows them to get over safety protocols like MAC address filtering.

4. **GPS Spoofing:**

Attackers send out fake GPS signals, which leads to devices reporting erroneous locations in systems that rely on GPS data. Operations related to navigation, logistics, and other location-based services may be affected by this.

9.3.3 Sniffing

Sniffing attacks in IoT security entail recording and examining network communication to retrieve private data, such as data exchanged between IoT devices or between IoT devices and central servers. Cryptographic tools are used for evaluating the gathered data; if a device is not sufficiently protected, the attacker only needs to listen and read to steal vital information.

9.3.4 MiTM attacks

An attack known as a" Man in the Middle" occurs when an attacker acts as a channel or proxy between a sender and a recipient, entering the conversation between them. From this vantage point, the attacker can eavesdrop on and modify the messages being sent and received.

1. **Rogue Access Point Attacks:**

In this kind of assault, an unauthorized wireless access point known as a" rogue" is placed within the coverage area of an established wireless network, usually without the network administrator's knowledge or approval. The Rogue AP commonly uses the same SSID as the active network. Rogue AP launches a MiTM attack

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

because it has a stronger signal or because IoT devices are set up to automatically connect to a known SSID.

2. ARP Spoofing:

This technique links the hacked device's MAC address to the IP address of a different valid device in the network by sending spoof ARP (Address Resolution Protocol) signals. Attackers can now intercept, alter, or stop network communication as a result.

3. DNS spoofing:

Additionally, attackers have the ability spoof the DNS cache, which results in the redirection of real user traffic to bogus domains. For this to happen, attackers must take advantage of flaws in DNS servers or deceive users into downloading malware that modifies DNS settings.

9.3.5 RPL Attacks

Routing protocol for IoT ecosystems is called Protocol RPL. Due to several constraints such as computational power constraints, mobility issues, connection failures, and changes in network architecture, RPL protocol is vulnerable to network attacks. The following are a few typical RPL attack types:

1. Sybil Attacks:

The attacker takes the identities of multiple targets during a Sybil attack. This is one of the biggest obstacles when connecting with peer-to-peer networks. It may influence and fully control the network by creating multiple phony identities. IoT. Sybil attacks come in a variety of forms, including Denial-of-service, exhaustion of resources, fake identity, and bogus information attacks.

2. **Selection Forwarding:**

This is frequently accomplished by monitoring packets and selecting which ones to forward or delete, which may result in missing information or network problems in the routing path. This attack can enable DDoS.

3. Sinkhole Attack:

An intentional slowdown or shutdown of the entire network caused by an IoT sinkhole attack that sends erroneous routing information. Possible consequences include stifling user access to services, interfering with communication, and even initiating fresh threats on the network. Additionally, network data, such as IP addresses, packets of data, and login credentials might be stolen via a sinkhole attack. Blackhole and Grayhole attacks are the two most common types of sinkhole attacks.

a. **In a Blackhole Attack**, the attacker advertises that an unauthorized node has the quickest path to the destination node to draw in data packets. After attracting data packets, the rogue node drops them, essentially forming a" black hole" where data vanishes.

b. **A Grayhole Attack** occurs when an unauthorized node drops some packets to create a zone of obscurity while leaving other packets through. It is challenging to find.

4. Wormhole Attack:

This entails two or more coordinated attackers building a tunnel between them- selves to transmit communications, so deceiving the network into believing that the nodes are closer together than they are and possibly seriously disrupting it.

5. Reply Attack:

Replay attacks occur when an attacker intercepts data packets from an authorized device, saves them, and then pretends to be an authorized device to delay or retransmit the data later. Replay attacks of various kinds, such as session hijacking, encrypted data, and authentication replay attacks, can be used against IoT devices. An attacker can intercept an authentication request in an authentication replay attack, delay or repeat it, and use that information to obtain login to a system. An attacker can intercept a legitimate session and use it to get

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

around authentication and get access to the system known as session hijacking. An attacker can obtain sensitive information by eavesdropping and replaying encrypted data in an encrypted data replay attack.

6. Hello Flooding Attack:

Recently connected devices broadcast a hello message in the form of a broadcast packet. In this scenario, an attacker can pose as a neighboring device and use a potent antenna to broadcast many HELLO packets. The Hello Flood attack involves sending a significant volume of this message to the overflow network to hinder the exchange of other kinds of messages.

10 IoT Security Solution

IoT security structures, as shown in Figures 1 and 2, fall into five primary layers based on compute techniques and networking ecosystems. It is believed that the possibility of a security compromise is greatest at the cloud level and lowest at the device level. Figure 6 explains IoT Security solutions.

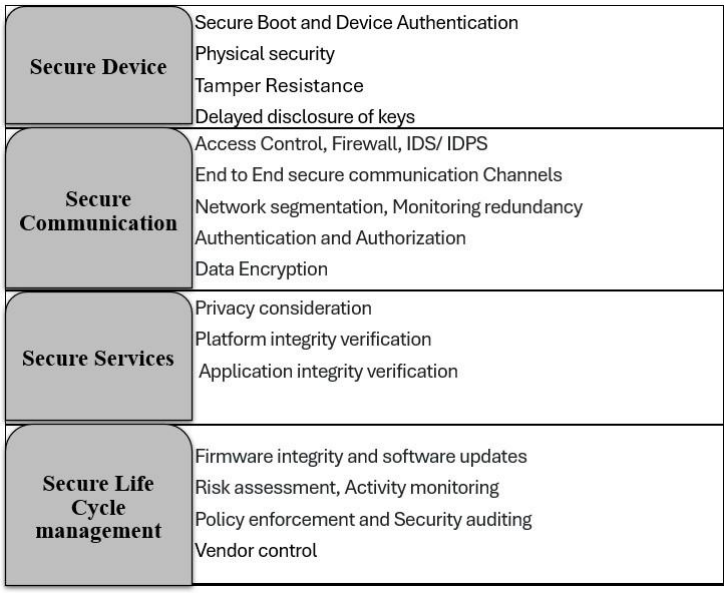

Fig. 6: IoT Security Solution

10.1 Secure Device

Hardware level includes aspects like secure booting, data when idle, chip protection, physical security, tampering proof, delayed key disclosure, and device identification authentication through edge processing, among others. Key ideas are discussed here as shown in Figure 6.

1. Secure Boot and Device Authentication

Validate the cryptographic signature to make sure that only legitimate firmware is loaded and implement a safe boot process. IoT device authentication that works requires a multi-layered strategy that combines safe key management, robust cryptographic techniques, and adherence to standards. You may greatly improve the security of your IoT infrastructure by taking care of these aspects.

2. Hardware Root of Trust (HRT)

To store cryptographic keys and carry out confidential tasks, use a Hardware Security Module (HSM) or Trusted Platform Module (TPM). This guarantees that crucial security operations are carried out in an environment that is impervious to tampering.

3. Physical Tamper Resistance

Use methods like enclosures, active tamper detection (sensors to detect tampering), tamper-evident seals

(which send alerts during tampering), and other ways to design hardware that is resistant to tampering.

4. **Delayed disclosure of keys**

When sensitive information, such as cryptographic keys, is only made public after a particular period or event, this is known as delayed disclosure of keys. There are several ways to implement delayed key disclosure, including Time-Locked Encryption, using escrow services (where the keys are held by trustworthy third parties and delivered only once certain requirements are completed), Blockchain-Based Time-locks, Time-Based One-Time Password (TOTP), etc.

5. **Side Channel Attack Protection**

Put defenses in place to fend against side-channel attacks. This entails utilizing hardware that reduces information loss, randomizing cryptographic procedures, and providing electromagnetic emission protection.

10.2 Secure Communication

Man-in-the-Middle attacks are particularly dangerous for networks that offer access across the OSI model's physical (Ethernet, Wi-Fi, etc.), network (Modbus, IPv6, etc.), and application (CoAP, MQTT, etc.) layers. To guarantee an adequately secure environment, this involves division of networks, approval, end-to-end encryption, firewalls, access control (ACL), intrusion detection systems (IDS), intrusion prevention systems (IPS) and tracking backup.

1. **End to End Secure Communication Channels**

Secure communication channels from end to end: Secure all communication connecting cloud services, gateways, and IoT devices by encrypting it with robust cryptographic protocols such as TLS, IPSec, or MQTT over SSL.

2. **Access Control**

Robust access control measures should be put in place to guarantee that only legitimate users and devices are able to communicate with the hardware. Using secure attributes to verify identification is one way to do this.

3. **Network Segmentation**

Network segmentation is the process of breaking up a larger network into smaller, more private subnets, each of which is allowed to have its own set of security rules and regulations. To prevent threats from spreading, segment IoT networks from other sections of the business's network. It makes it easier to detect anomalies, decreases attack surface area, etc. Physical Segmentation utilizing switches and routers, Logical Segmentation using VLANs, and Micro-Segmentation are a few of the segmentation techniques employed.

4. **Firewalls, IDS/IDPS**

Establish firewalls and intrusion detection/prevention systems (IDS/IPS) on your network to keep an eye out for unusual traffic patterns that could point to an attack and to take appropriate action.

5. **Authorization and Authorization**

Authentication mechanisms, in addition to encryption, guarantee that the data has not been tampered with during transit and that it was received from a reliable source. For this, digital signatures, certificates, and HMAC (Hash-based Message Authentication Code) are frequently utilized. The process of deciding and implementing what actions a specific user, device, or application is allowed to undertake inside an IoT ecosystem is known as authorization. so, defending the system against unapproved activities that can jeopardize security. Frequently utilized forms of authorization include Token- and OAuth-based authorization, Fine-grained authorization, multi-factor authorization, and role-based, attribute-based, policy-based, and so forth.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

6. **Data Encryption**

Data transmission within networks can be encrypted to keep it safe from interception and reading by unauthorized parties. TLS (Transport Layer Security) to utilized for securing web-based communication and DTLS (Datagram Transport Layer Security) utilized for securing datagram-based communication (UDP) are two popular encryption protocols, respectively. End-to-end encryption, or E2EE, makes sure that data is encrypted all the way from the source (an Internet of Things device) to the destination (a cloud server, for example), and that it is only decrypted at endpoints.

10.3 Secure Services

Software backend data is received, evaluated, and feasible conclusions are produced. Concerns at this stage include elements of data idle, platform/application integrity authentication, and unified threat control.

1. **Privacy Consideration**

Sensitive data is often collected by IoT devices. User privacy can be safeguarded by ensuring that data is collected and managed in compliance with confidentiality laws (such as the CCPA and GDPR) and by putting features like data anonymization into place.

2. **Platform Integrity**

The guarantee that the underlying hardware and software components of an Inter- net of Things device or system are safe, unaltered, and function as expected is known as platform integrity. Because penetrated platforms can result in illicit access, security breaches, and system failures, compromising platform integrity which is essential to ensuring the overall security of the IoT ecosystem.

3. **Application Integrity**

Application Integrity refers to safeguarding the reliability of the data that IoT devices process as well as the software programs that operate on them. Checksums, hashes, or digital signatures for verifying the authenticity of the data handled by the program; running applications in isolated settings (sandboxes) to restrict their access to the underlying infrastructure and other applications; and other factors are crucial to preserving application integrity in IoT security. The goal of maintaining application integrity is to secure IoT devices and guarantee that they operate as planned without being vulnerable to illegal changes or attacks.

9.4 Secure Life Cycle Management

Lifecycle management: Managing ongoing procedures to maintain adequate security in an updated manner. Thus, it is important to maintain risk identification, traffic evaluation, provider surveillance, consumer review, rules, accounting, upgrades patches, and safe decommissioning.

1. **Firmware Integrity and Updates**

To stop illicit code from executing on the device, make sure the firmware can be upgraded with properly signed, authenticated updates that are validated before installation. To stop the device from downgrading to a previous, vulnerable firmware version, implement rollback protection.

2. **Risk Assessment and Activity Monitoring**

To comprehend potential routes of attack and how they affect IoT services, regularly perform threat modelling. To lessen the possibility and impact of possible safety issues, continuously evaluate the threats to the IoT network and put the right mitigation strategies into place. Potential safety violations can be identified and mitigated by creating an incident response strategy and regularly keeping an eye out for unusual activity on IoT networks and devices.

3. **Policy Enforcement and Security Auditing**

Throughout the IoT architecture, implement and enforce security standards to make sure best practices and legal requirements are followed. To find and address vulnerabilities, do routine penetration tests and security

audits. Throughout the lifecycle of the IoT device, this should be a continuous activity.

4. **Vendor Control**

To guarantee the security, integrity, and dependability of IoT devices over the course of their operational lives, vendor control over the lifecycle management of the devices is essential. Monitoring the interaction with vendors is necessary to make sure that the hardware, software, hardware components, and updates they supply adhere to corporate regulations and security standards.

11 CONCLUSION

An organized framework for controlling the transfer of data and relations among devices and applications on the IoT network is provided by the layered architecture of the Internet of Things. For someone involved in organizing, establishing, or installing IoT solutions in this era, comprehending the architecture is essential. Understanding IoT architecture is crucial for developers, engineers, and business executives alike to make use of this game-changing technology. IoT could transform industries, increase productivity, and raise standards of living when the proper infrastructure is in effect. This study offers a thorough analysis of the security of IoT understanding, IoT-based intelligent conditions, related security issues, and safeguarding the IoT ecosystem against threats. This chapter have given an outline of how Internet of Things devices function, the architecture of the Internet, and the protocols used in its many tiers. The several types of IoT networks, including Wireless PAN, Wireless LAN, Mesh, Cellular, and others, as well as the protocols used in each, are also explained in this chapter. It investigated different approaches for enhancing IoT security. It covers protecting IoT devices, setting up secure communication, protecting application-layer services, and protecting lifecycle management. Wearable technology and the Internet of Things are revolutionizing people's daily lives and are having a significant worldwide influence. A" smart world" will emerge because of the ongoing development of IoT applications and technology, which will alter how people currently perceive the world.

Conflict of Interest

Assistance for this book chapter was provided by the R&D team of the Computer Science Department of Saintgits College of Engineering in Kottayam, Kerala, India. Their help and encouragement in making this paper a reality have been invaluable.

REFERENCES

[1] Raghavendra, M., Mishra, A.: Current research on internet of things (iot) security protocols: A survey. Computers Security **151** (2025) https://doi.org/10.1016/j. cose.2024.104310

[2] Laghari, A.A., Li, H., Khan, A.A., et al.: Internet of things (iot) applications security trends and challenges. Discover Internet of Things **4**(36) (2024) https: //doi.org/10.1007/s43926-024-00090-5

[3] Singh, S., Tiwari, V., Kirti, D., Vadi, V.: Protocols for the internet of things. IJARCCE **13**, 1062–1067 (2024)

[4] Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S.R., Rehman, A.U., Bharany, S.: Navigating iot security: Insights into architecture, key security features, attacks, current challenges and ai-driven solutions shaping the future of connectivity. Computers, Materials & Continua **81**(3) (2024)

[5] Dauda, A., Flauzac, O., Nolot, F.: A survey on iot application architectures. IJARCCE **24**(5320) (2024) https://doi.org/10.3390/s24165320

[6] Sun, P., Shen, S., Wan, Y., Wu, Z., Fang, Z., Gao, X.-Z.: A survey of iot privacy security: Architecture, technology, challenges, and trends. IEEE Internet of Things Journal **11**(21), 34567–34591 (2024) https://doi.org/10.1109/JIOT.2024. 3372518

[7] Adam, M., Hammoudeh, M., Alrawashdeh, R., Alsulaimy, B.: A survey on security, privacy, trust, and architectural challenges in iot systems. IEEE Access **12**, 57128–57149 (2024) https://doi.org/10.1109/ACCESS.2024.3382709

[8] Saleem, A., Shah, S., Iftikhar, H., Zywio-lek, J., Albalawi, O.: A comprehensive systematic survey of iot

protocols: Implications for data quality and performance. IEEE Access, 1–1 (2024) https://doi.org/10.1109/ACCESS.2024.3486927

[9] Shah, B., Junaid, M., Habib, M.: Enhancing iot protocol security through ai and ml: A comprehensive analysis. In: 2024 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–7 (2024). https://doi.org/10. 1109/ISNCC62547.2024.10758967

[10] Dahlmanns, M., Wehrle, K.: Protocol security in the industrial internet of things. In: NOMS 2024-2024 IEEE Network Operations and Management Symposium, pp. 1–4 (2024). https://doi.org/10.1109/NOMS59830.2024.10575096

[11] Wei, Z., Wei, Q., Geng, Y., Yang, Y.: A survey on iot security: Vulnerability detection and protection. In: Proceedings of the 2024 International Conference on Artificial Intelligence of Things and Computing, pp. 1–8 (2025). https://doi.org/10.1145/3708282.3708283

[12] Rakshe, A., Dongre, N.: Survey on security protocols for iot. In: 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), pp. 1–5 (2024). https://doi.org/10.1109/I2CT61223.2024.10544115

[13] Sasi, T., Lashkari, A.H., Lu, R.o.: A comprehensive survey on iot attacks: Taxonomy, detection mechanisms and challenges. Journal of Information and Intelligence **2**(6), 455–513 (2024) https://doi.org/10.1016/j.jiixd.2023.12.001

[14] Panwar, S.V., Boukabous, H.: A review on routing protocols in mobile iot networks based on sdn. In: 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1561–1566 (2024). https://doi.org/ 10.1109/ICAAIC60222.2024.10574975

[15] Tawffaq, M.R., Jasim, M.A., Mejbel, B.G., Issa, S.S., Alamro, L., Shulha, V., Aram, E.: Iot security in a connected world: Analyzing threats, vulnerabilities, and mitigation strategies. In: 2024 36th Conference of Open Innovations Asso- ciation (FRUCT), pp. 626–638 (2024). https://doi.org/10.23919/FRUCT64283.

[16] Ganda, V.D., Chhikara, R., Mehra, P.S., Chawla, D.: A systematic review on internet of things (iot) security: Applications, architecture, challenges and solutions. In: 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), pp. 1–8 (2024)

[17] Cambosuela, L., Kaur, M., Astya, R.: The vulnerabilities and risks of implementing internet of things (iot) in cyber security. In: 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1–5 (2024).

[18] Rana, P., Patil, B.: Cyber security threats in iot: A review. Journal of High Speed Networks 29(2), 105–120 (2023) https://doi.org/10.3233/JHS-222042

[19] Gerodimos, A., Maglaras, L., Ferrag, M.A., *et al.*: Iot: Communication protocols and security threats. Internet of Things and Cyber-Physical Systems **3**(2667- 3452), 1–13 (2023) https://doi.org/10.1016/j.iotcps.2022.12.003

[20] Prakash, R., Jyoti, N., Manjunatha, S.: A survey of security challenges, attacks in iot. E3S Web Conf **491** (2024) https://doi.org/10.1051/e3sconf/202449104018

[21] NAWAZ, S., SHAH, S.P.H., TASKEEN, et al.: Internet of things (iot) security and privacy. Journal of Tianjin University Science and Technology **56** (2023) https://doi.org/10.17605/OSF.IO/T8YCW

[22] AlSalem, T., Almaiah MA, L.A.: Cybersecurity risk analysis in the iot: A systematic review. Electronics **12**(18) (2023) https://doi.org/10.3390/ electronics12183958

[23] Aryavalli, S.N.G., Kumar, H.: Top 12 layer-wise security challenges and a secure architectural solution for internet of things. Computers and Electrical Engineering **105** (2023) https://doi.org/10.1016/j.compeleceng.2022.108487

[24] Akter, S., Khalil, K., Bayoumi, M.: A survey on hardware security: Current trends and challenges. IEEE Access **11**, 77543–77565 (2023) https://doi.org/10.1109/ ACCESS.2023.3288696

[25] Tariq, U., Ahmed, I., Bashir, A.K., Shaukat, K.: A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review.
Sensors **23** (2023) https://doi.org/10.3390/s23084117

[26] Chen, X., Yang, C., Nan, Y., Zheng, Z.: An empirical study of high-risk vulnerabilities in iot systems. IEEE Internet of Things Journal **12**(2), 1590–1601 (2025) https://doi.org/10.1109/JIOT.2024.3506976

[27] Pourrahmani, H., Yavarinasab, A., Monazzah, A.M.H., et al.: A review of the security vulnerabilities and countermeasures in the internet of things solutions: A bright future for the blockchain. Internet of Things **23**(100888) (2023) https:
//doi.org/10.1016/j.iot.2023.100888

[28] Iwuanyanwua, U., Oyewoleb, O.O., Fakeyedec, O.G.: Iot device security risks: A comprehensive overview and mitigation strategies. Journal of Technology Innovation **3**(1) (2023) https://doi.org/10.26480/jtin.01.2023.38.43

[29] Bilal, A., Shah, S.J., Khan, M.A., Khan, M., Bharmal, A.H., Mumtaz, T.: Security threats and research challenges of iot - a review. In: 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC), pp. 1–10 (2022). https://doi.org/10.1109/ICETECC56662.

[30] Choudhary, A.: Internet of things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discov Internet Things **4**(31) (2024) https://doi.org/10.1007/s43926-024-00084-3