EMERGING ADVANCES IN INTEGRATED TECHNOLOGY
e-ISSN: 2773-5540

Vol. 6 No. 1 (2025) 55-74
https://publisher.uthm.edu.my/ojs/index.php/emait

EmAIT

A Comprehensive Review of Network and Communication in IoT Systems

Shipun Anuar bin Hamzah[1], Mohd Salleh bin Md Roslan[1], Loh Yin Chyuan[1]*

[1] *Faculty of Electrical and Electronic Engineering,*
Universiti Tun Hussein Onn Malaysia, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: ge240065@student.uthm.edu.my

DOI: https://doi.org/10.30880/emait.2025.06.01.007

Article Info

Received: 9 May 2025
Accepted: 28 May 2025
Available online: 10 June 2025

Keywords

IoT network and communication, Wi-Fi, Bluetooth, 5G, LoRa

Abstract

The Internet of Things (IoT) has fundamentally changed the way we communicate by integrating devices equipped with sensors, software, and connectivity. This integration allows for efficient data exchange and automation, improving operational capabilities across various sectors. This paper provides a comprehensive review of IoT networks and communication technologies, categorizing them into short-range and wide-area communication. It examines key network technologies such as Wi-Fi, Bluetooth, cellular networks (4G/5G), and LoRa. Additionally, the study explores major IoT communication protocols including MQTT, CoAP, HTTP, and WebSocket, highlighting their roles in ensuring efficient and scalable data transmission. The paper also addresses critical challenges in IoT networks, such as energy efficiency, security vulnerabilities, interoperability issues, network congestion, and regulatory compliance. The findings emphasize the need for optimized network selection, secure communication protocols, and scalable architectures to support the expanding IoT ecosystem.

1. Introduction of IoT Network and Communication

The term Internet of Things, abbreviated as IoT, represents a groundbreaking transformation that involves the complex linking of an array of tangible objects, each integrated with high-tech sensors, innovative software, and a plethora of other modern technologies that together enable these items to accumulate, process, and transmit significant volumes of data smoothly over the vast expanse of the Internet. This intricate and interconnected network not only facilitates seamless communication among an array of devices but also significantly enhances automation capabilities and improves decision-making processes across a diverse range of applications, which extend from the innovative realms of smart homes to the complex systems utilized in various industrial settings. Specifically speaking, IoT can be defined as a significantly widespread network comprising numerous embedded systems, which communicate effectively using both wired and wireless means, thereby allowing for a seamless blend of the real and virtual environments [1].

The reliable connections that are part of the systems of the Internet of Things (IoT) are largely attained through the adoption of a variety of technologies, which embody an extensive assortment of practices and protocols, including, though not exclusively, Radio Frequency Identification (RFID), machine-to-machine (M2M) talk, and the establishment of wireless sensor networks (WSNs), each playing a significant role in supporting effective communication between devices.

The remarkable heterogeneity of devices found within an IoT network is, without a doubt, truly astonishing and noteworthy. These devices range widely from ubiquitous objects that we encounter daily, such as innovative smart lighting systems and advanced wearable technology, to highly complex and sophisticated industrial apparatuses designed for specific operational tasks. All these tools are fitted with top-notch sensors and innovative software that support the seamless accumulation, interpretation, and distribution of essential data. IoT technologies encompass an expansive and varied range of devices and systems, including those utilized explicitly in critical military operations and various environmental monitoring applications. Noteworthy initiatives like the Internet of Battlefield Things and the Ocean of Things stand out as exemplary collaborative efforts focused on advancing IoT technologies, enhancing surveillance capabilities, and improving ecological monitoring practices.

2. Type of IoT Network

IoT networks can be broadly classified based on their communication range capabilities: short-range communication and wide-area communication. Each category has distinct advantages and disadvantages, making them suitable for IoT applications.

2.1 Short Range Communications

Short-range communication networks are designed for IoT applications where devices are located near each other, typically within a few meters to a few hundred meters. These networks are ideal for environments such as smart homes, offices, and industrial settings where devices need to communicate over relatively short distances.

2.1.1 WiFi

The evolution of Wi-Fi technology has been remarkable since the introduction of the first standard, 802.11, in 1997, which offered a maximum speed of 2 Mbit/s. This was followed by the 802.11b version, which improved speeds to 11 Mbit/s, not 8 Mbit/s. Today, the latest standard, Wi-Fi 7 (802.11be), can achieve speeds of up to 46 Gbit/s under optimal conditions, marking a significant advancement in data transfer capabilities essential for modern digital communication technologies. Wi-Fi 7 expands channel bandwidth from 160 MHz to 320 MHz, enabling it to support high-demand applications such as 4K and 8K video streaming, data aggregation, and remote health monitoring [2].

The widespread availability of Wi-Fi networks in urban areas has facilitated the integration of various Internet of Things (IoT) technologies without the need for additional infrastructure investments, optimizing connectivity in smart environments. However, challenges arise when the number of simultaneous users exceeds the capacity of the 2.4 GHz and 5 GHz frequency bands, leading to increased interference and degraded data transfer speeds, which can impair application performance [3].

Both frequency bands typically have an indoor coverage limit of about 30 meters, which can be restrictive for IoT systems requiring broader coverage, such as in agriculture. The high costs of installing network cabling over large distances prompt many businesses to consider alternatives like private LTE networks.

Wi-Fi technology is crucial for smart home automation systems, seamlessly connecting devices like smart thermostats, lighting controls, and security cameras. This powerful connectivity empowers homeowners to effortlessly manage their environments remotely through smartphones or voice-activated assistants. Additionally, Wi-Fi drives smart city initiatives by providing essential public hotspots and optimizing traffic management and environmental monitoring via connected sensors.

2.1.2 Bluetooth

Bluetooth technology, originally conceived by Ericsson in 1989, has evolved into a widely adopted standard for short-range wireless communication, primarily operating in the 2.4 GHz frequency band [4]. This frequency range is shared with other technologies, including Wi-Fi and various household devices, which can lead to interference and performance degradation when multiple devices operate simultaneously [8]. Bluetooth was designed to replace traditional wired connections, such as RS-232, facilitating the wireless connection of devices like smartphones, headsets, and laptops.

The latest version of Bluetooth, specifically Bluetooth Low Energy (BLE), provides a distinct advantage over Wi-Fi for Internet of Things (IoT) applications due to its enhanced energy efficiency. This is particularly beneficial for IoT devices that require prolonged operation while minimizing the need for battery replacement, making it especially valuable for devices installed in remote or hard-to-reach locations.

In addition to energy efficiency, BLE supports various network topologies, including point-to-point and mesh networking, which further enhances its applicability in IoT environments. Mesh networking allows devices to communicate with one another directly, extending the range and reliability of the network without requiring a central hub. This functionality is especially advantageous in settings where conventional Wi-Fi networks face challenges from interference or limitations in range [9]. This feature can enhance connectivity and performance, ensuring reliable communication in diverse environments.

One notable limitation of Bluetooth technology is its restricted range. Typically, Bluetooth operates effectively within about 10 meters, which may be inadequate for applications that need wider coverage. This limitation is especially evident in indoor environments, where obstacles can further weaken the signal strength and reliability

[5]. For instance, Bluetooth Low Energy (BLE) often requires multiple nodes for adequate coverage in office environments, suggesting that multi-hop protocols may be needed to address range limitations.

The requirement for devices to operate in discoverable mode raises significant privacy concerns, as it heightens the risk of exposing these devices to unauthorized access. This scenario can lead to potential personal data breaches and security vulnerabilities, as malicious actors may exploit discoverable devices to establish unauthorized connections. Therefore, balancing the convenience of connectivity features and the implementation of robust security protocols to safeguard user privacy in a networked environment is essential. Additionally, enhancing user controls and promoting awareness regarding discoverability can substantially reduce these risks.

Bluetooth Low Energy (BLE), characterized by its minimal energy consumption, enables devices to function for prolonged durations on compact batteries, rendering it exceptionally suitable for home automation frameworks. For example, smart digital door locks can be operated through smartphones, thereby enhancing both security and convenience for homeowners. Additionally, temperature and humidity sensors that feature BLE technology can relay live data to optimize the management of indoor climate, thereby supporting enhanced energy efficiency.

2.2 Long Range Communications

Wide-area communication networks are specifically engineered for Internet of Things (IoT) applications that necessitate communication over extensive distances, frequently encompassing several kilometers. These networks are ideally suited for applications in smart agriculture, smart cities, and industrial IoT, where devices are distributed across vast regions.

2.2.1 Cellular (4G/5G)

Integrating advanced mobile technologies, particularly 4G and 5G, with the rapidly expanding Internet of Things (IoT) signifies a transformative shift in communication processes and operational dynamics among interconnected devices. The rollout of wireless networks is essential for providing diverse IoT functions that require extensive connectivity and reliable coverage across vast geographic areas.

The evolution of cellular technology from 2G to 5G has enabled IoT devices to meet communication requirements characterized by secure, high-speed data transmission and energy efficiency, which is particularly vital in industrial settings and remote locations where conventional connectivity may be lacking. The revolutionary 5G technology is poised to become the cornerstone of the burgeoning IoT applications ecosystem, promising significant enhancements in data transmission speed, capacity, and connectivity among devices [6]. The comprehensive rollout of 5G infrastructure facilitates the simultaneous connection of numerous devices, essential for accommodating the anticipated increase in IoT deployments.

The advancements in Cellular Internet of Things (IoT) technologies, particularly Narrowband IoT (NB-IoT) and Long-Term Evolution for Machines (LTE-M), are significantly transforming the connectivity landscape. These technologies, developed by the 3rd Generation Partnership Project (3GPP), are specifically designed to meet the intricate requirements of various IoT applications. They facilitate extensive IoT deployment scenarios by offering benefits such as reduced power consumption and enhanced coverage capabilities.

Despite these advantages, challenges remain, particularly concerning latency, which is critical for applications requiring rapid responses, such as self-driving vehicles and factory automation. Although 5G has made strides in reducing latency, certain applications may still experience unacceptable delays, necessitating further innovations. Additionally, the energy demands of IoT devices pose significant challenges, as continuous data transmission can strain battery life, requiring frequent recharging [7].

In agriculture, the benefits of 4G and 5G technologies are becoming increasingly apparent, particularly in precision farming and livestock monitoring. IoT devices equipped with advanced sensors can assess soil conditions, monitor crop health, and track livestock, enabling real-time data transmission that empowers farmers to make informed and confident decisions. The low latency and reliability of 5G technology further enhance these capabilities, resulting in more efficient resource allocation and improved productivity within agricultural practices.

2.2.2 LoRa

LoRa, which stands for Long Range, is a wireless communication technology designed specifically for long-distance transmission while ensuring low power consumption and accommodating low data rate applications. This technology has become a pivotal support for numerous Internet of Things (IoT) initiatives, enhancing the development and performance of the IoT framework. LoRa technology operates within the unlicensed Industrial, Scientific, and Medical (ISM) radio frequency bands, offering a cost-effective and scalable connectivity solution. This versatility allows for its application across a diverse array of use cases in various fields [10].

One of the most significant advantages of LoRa is its minimal energy expenditure, which is particularly beneficial for battery-operated IoT devices. This characteristic extends the operational lifespan of these devices and reduces the need for regular maintenance, especially in remote areas where access can be challenging. As a leading Low Power Wide Area Network (LPWAN) protocol, LoRa is engineered to support extensive deployment scenarios while providing reduced power consumption and impressive coverage.

However, LoRa does have constraints that can limit its utility in certain contexts. A primary limitation is its restricted data transmission rate, which is capped at approximately 50 kbps under optimal conditions, with actual rates varying based on the spreading factor used, typically ranging from 0.3 kbps to 5.4 kbps [11]. This limitation makes LoRa unsuitable for high-bandwidth applications, such as video streaming, which require higher data rates and lower latency. The throughput of LoRa networks is further constrained by factors such as the number of available demodulators for packet processing and the collision risks associated with the ALOHA protocol used in LoRaWAN [12].

The expansive range capabilities of LoRa technology offer comprehensive coverage across large agricultural landscapes, which is essential for effective management. For instance, soil moisture sensors can be strategically deployed throughout vast areas to provide real-time insights into soil conditions, enabling farmers to optimize their irrigation practices and conserve water resources. Furthermore, livestock tracking systems can harness LoRa technology to monitor both the health and location of animals across extensive pastures, thereby enhancing farm management and promoting animal welfare.

3. IoT Network and Communication

The Internet of Things (IoT) is defined by a multi-layered architecture that enables the seamless integration of devices, data processing, and user interaction. This architecture generally consists of several layers: The Perception Layer (which includes edge devices and sensors), the Network Layer (comprising gateways and connectivity), the Edge Computing Layer (for local processing), the Data Management Layer, and the Application Layer (which encompasses cloud services and user interfaces). Each layer enhances system performance, security, and data flow.

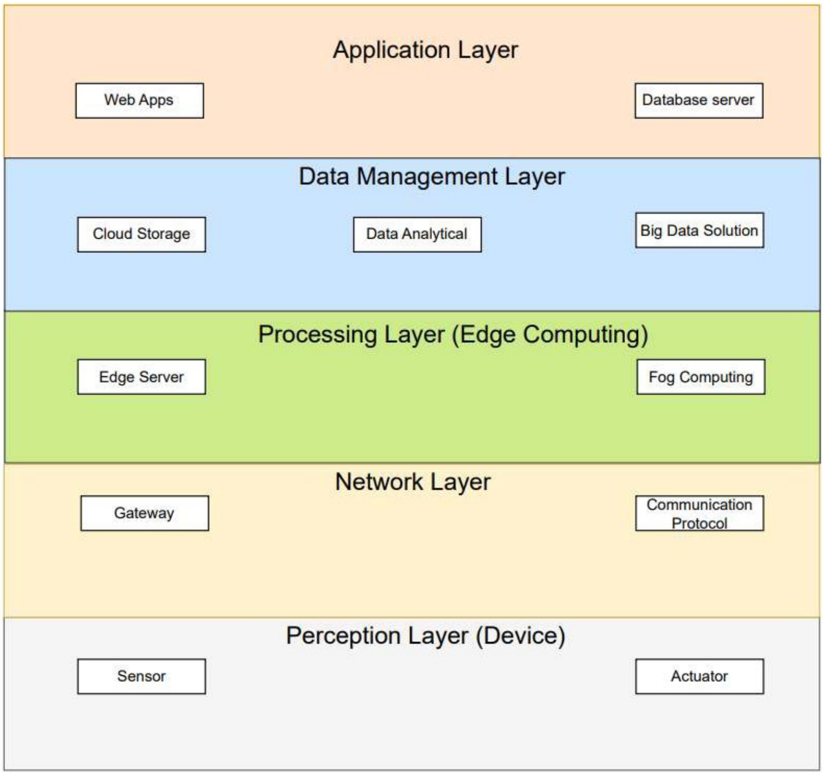

Fig. 1 *IoT network architecture*

The architecture of Internet of Things (IoT) networks is systematically designed to address the complexities inherent in the interconnection of diverse devices and systems. Each layer is meticulously crafted to fulfill specific functions, facilitating efficient communication and data processing while addressing pertinent security concerns. This layered approach enhances the overall robustness and reliability of IoT networks.

3.1 Perception Layer

The Perception Layer constitutes the foundational component of Internet of Things (IoT) architecture. It encompasses a range of sensors and devices that systematically collect environmental data, enabling the seamless acquisition of information crucial for informed decision-making and further processing within the IoT ecosystem. This layer includes instruments such as temperature and humidity sensors, cameras, and actuators, essential for monitoring and data collection. The primary function of this layer is to convert physical phenomena into electrical signals, enabling the digitization of analog data for processing and transmission over networks using protocols like MQTT, CoAP, or HTTP [13].

Edge devices, often situated within the Perception Layer, possess limited processing capabilities and are designed to perform preliminary data filtering and aggregation. This local processing allows for rapid responses to environmental changes, which is crucial for applications requiring immediate action. Moreover, local data handling reduces the volume of data transmitted to centralized servers, alleviating network congestion and minimizing operational costs associated with data management

Despite its importance, the Perception Layer faces challenges related to resource constraints, including limited computation, memory, and energy. Effective data management strategies, such as data compression and filtering, are necessary to enhance performance without compromising data integrity. For instance, pre-processing data from remote sensors before transmission can significantly improve system efficiency by reducing bandwidth usage and energy consumption.

3.2 Network Layer

The networking layer in Internet of Things (IoT) systems is fundamental for facilitating communication between edge devices and the upper application layers responsible for data processing and analysis. This layer utilizes dedicated gateways and diverse connectivity protocols to ensure seamless data transmission. Its role is vital in enhancing the overall performance and operational efficiency of IoT applications.

Gateways are essential in data transmission, facilitating the transfer of information from peripheral devices to cloud services or local storage. They carry out crucial functions such as data aggregation, packetization, and local filtering, all of which improve bandwidth efficiency and minimize latency. Research shows that cluster-based routing strategies can significantly reduce the total amount of data transmitted by eliminating redundant information prior to its arrival at the cloud, thereby enhancing system responsiveness. [14].

Protocol translation serves as a critical function of gateways, facilitating seamless interaction among devices that utilize varying communication standards, such as LoRa, Zigbee, and Ethernet. This interoperability is essential in heterogeneous environments where devices from different manufacturers must collaborate effectively. Additionally, the integration of data filtering and preprocessing functionalities within gateways enhances operational efficiency by minimizing the volume of data transmitted, conserving bandwidth, and alleviating the computational demands on cloud servers.

The scalability and data latency of IoT networks are significantly influenced by the architecture of the networking layer. Gateways facilitate scalability by aggregating data from multiple edge devices, allowing for the seamless integration of additional devices without overburdening the network infrastructure. Furthermore, the choice of communication protocols and effective data aggregation strategies directly impact latency and throughput, which are critical for applications requiring prompt data processing, such as autonomous transport systems [15}.

3.3 Edge Computing Layer

The Edge Computing Layer stands as a fundamental pillar of contemporary Internet of Things (IoT) architecture, empowering local data processing and analysis near the source. This layer consists of edge servers that utilize fog computing principles to enhance data processing capabilities, addressing the limitations of traditional cloud computing [16]. By processing data locally, edge servers reduce the need to transmit all raw data to centralized cloud facilities, resulting in improved response times and optimized bandwidth utilization.

Local data processing is a significant benefit of edge computing, as it enables data analytics to be conducted near the source of data generation. This strategy minimizes the dependence on continuous cloud communication, thereby conserving bandwidth and enhancing system performance, particularly in real-time applications such as intelligent manufacturing and healthcare monitoring. Furthermore, decentralizing data processing reduces the volume of data transmitted to the cloud, significantly mitigating transmission delays.

Another key advantage of edge computing is its ability to reduce latency. By processing data near its source, edge computing significantly minimizes the time required for data transmission to and from centralized servers. This reduction in latency is critical for time-sensitive applications, particularly in fields such as autonomous vehicles and industrial automation. Mobile edge computing (MEC) further enhances this capability by improving computational functions closer to users, thereby elevating service quality and reducing latency [17].

Moreover, edge computing enhances bandwidth efficiency by minimizing the volume of data that needs to be transmitted to the cloud. This reduction not only alleviates network congestion but also optimizes overall system performance. This optimization is vital in IoT ecosystems, where numerous devices generate substantial data outputs. The ability to process data locally enhances scalability and improves the overall efficiency of IoT systems, making edge computing an indispensable element of contemporary IoT frameworks.

3.4 Data Management Layer

The Data Management Layer constitutes a fundamental component of Internet of Things (IoT) architectures, tasked with the comprehensive management of substantial volumes of data generated by interconnected devices. Its effective operation is essential for ensuring data integrity, accessibility, and usability within IoT ecosystems. This layer encompasses essential components such as cloud storage systems, data analytics resources, application programming interfaces (APIs), and database frameworks, all of which enhance the performance and operational efficiency of IoT applications. APIs facilitate communication and data interchange, enabling developers to create applications that effectively utilize IoT-generated data. Database Management Systems (DBMS), including both SQL and NoSQL, provide the necessary flexibility to store structured and unstructured data, accommodating the diverse data types produced by IoT technologies [18].

Data aggregation and storage are fundamental functions within this layer, allowing for the integration of data from numerous IoT devices and edge processing nodes. This integration supports scalable and reliable long- term storage solutions, essential for applications requiring historical data analysis, such as environmental monitoring and industrial systems. The ability to analyze trends over time is vital for informed decision-making, underscoring the importance of this layer in IoT architecture.

The Data Management Layer is pivotal in influencing system performance, particularly through its contributions to scalability, optimization of data processing, and adherence to security and compliance standards. Implementing robust security protocols, such as encryption and identity management, is essential for safeguarding sensitive information and ensuring compliance with regulatory frameworks like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). As the proliferation of connected devices continues, maintaining secure access becomes increasingly complex. Consequently, establishing a comprehensive security architecture is critical for fostering trust among users and stakeholders, especially in high-stakes sectors such as healthcare and finance.

3.5 Application Layer

The Application Layer is a fundamental component of Internet of Things (IoT) systems, facilitating user interfaces and application services that enable end-users to effectively engage with and manage a variety of IoT devices. This layer encompasses user interfaces (UIs) and specialized application services tailored to specific use cases, ranging from smart home management to industrial monitoring and healthcare applications.

User Interfaces serve as the primary means for users to interact with IoT networks, available in various forms such as web platforms and mobile applications. These interfaces provide users with essential tools to monitor, control, and manage connected devices within their environments. Application Services, on the other hand, offer a suite of functionalities designed for diverse IoT ecosystems. For instance, smart home management systems allow users to control lighting and temperature, while industrial applications monitor equipment performance and environmental conditions.

A critical function of the Application Layer is the generation of real-time alerts, which enhances system responsiveness and reliability. By detecting specific thresholds or anomalies, the system can notify users of potential issues, such as security breaches or equipment malfunctions, enabling timely interventions. This capability is vital across various sectors, including healthcare and industrial monitoring, where prompt action can mitigate risks and enhance operational efficiency.

4. IoT Communication Protocol

Nowadays, there exist many communication protocols. Each communication protocol lacks key features or benefits that make it not suitable for certain IoT applications. The communication protocol's efficiency, reliability, and scalability are crucial in developing a tailored IoT solution. Efficiency in IoT applications typically refers to using energy, time, and bandwidth resources to optimize processes, reduce costs, and enhance performance among interconnected devices and systems. Scalability in IoT applications refers to a system's capacity to manage increasingly connected devices without significantly declining performance. A reliable IoT communication protocol design usually has a reliable device or sensor running without failure, stable network connectivity, and data collected and transmitted consistently and accurately.

4.1 MQTT (Message Queuing Telemetry Transport)

MQTT uses a TCP-based protocol and publish-subscribe (PubSub) architecture to transmit data. MQTT is an efficient communication protocol designed for seamless client data exchange, making it a perfect choice for IoT applications. It is a lightweight messaging protocol widely utilized in IoT applications due to its efficiency, reliability, and scalability.

In device-to-device communication (D2D), MQTT enables direct communication between devices through a central broker that manages message distribution. It ensures low latency and efficient data transfer. The protocol's lightweight design decreased bandwidth usage, making it suitable for resource-constrained environments like wireless sensor networks. Besides that, MQTT is capable of handling high message volumes. It also supports Quality of Service (QoS) levels and guarantees reliable message delivery, even under poor network conditions [19].

In device-to-cloud (D2C) communication, MQTT is a bridge that enables telemetry data transmission from IoT devices to cloud platforms. It uses a publish-subscribe model, allowing devices to send data to the central broker. After that, the broker forwards this information to the cloud for processing and analysis [20]. The three QoS levels ensure reliable message delivery, and the feature is crucial for maintaining data integrity during transmission to cloud platforms. The architecture streamlines the integration of diverse devices into the cloud and allows multiple devices to communicate within the cloud concurrently without declining the network performance. The lightweight design reduced latency. This advantage is essential for applications that solely rely on real-time data processing.

MQTT enables cloud applications to send commands or updates to devices in cloud-to-device (C2D) communication. This functionality is important for applications requiring remote control or IoT device configuration. The central broker ensures messages are sent to the correct devices based on their subscriptions. The protocol supports bi-directional communication, which enhances the interactivity of IoT systems and allows for dynamic adjustments based on real-time data [21].

MQTT messages are designed to be compact. The smallest message size is only two bytes. This characteristic leads to easy transmission over networks. The protocol also employs a binary format, which optimizes message size and minimizes bandwidth consumption during transmission. Consequently, MQTT is suitable for applications that require frequent fine-tuning in environments with limited network capacity.

MQTT allows users to adjust the reliability of message delivery to the recipients based on the QoS levels. Users can select between three QoS levels: 0, 1, and 2. QoS 0 offers no guarantee of reliable delivery, while QoS 2 ensures that a subscriber receives a message exactly once. MQTT can be advantageous when network stability is an issue. When a client is actively connected to a broker and has subscribed to a specific topic, the broker will retain any messages that the client has not yet received if the client goes offline. These messages will then be delivered to the subscriber upon their return online.

MQTT is highly scalable, and the protocol supports horizontal and vertical scalability approaches, enabling efficient communication and scaling. MQTT is also a many-to-many communication protocol for exchanging messages between multiple clients.

4.2 CoAP (Constrained Application Protocol)

CoAP uses a client-server (Request-Response) model that enables the client to request service from the server as needed, and the server responds to the client's request. It’s a web-based protocol that uses a User Datagram Protocol (UDP) to establish secure communications and enable data transmission between multiple points. Message dispatching happens on a unicasting basis, which is the one-to-one communication protocol that differs from MQTT. MQTT uses a central broker to handle message dispatching. CoAP is suitable for resource-constrained environments with low bandwidth, low availability, or low-energy devices. REST (Representational State Transfer) architecture views the various objects in the network as resources, each uniquely identified by a Uniform Resource Identifier (URI). Data is exchanged between resources through CoAP message packets. It utilizes a binary format, which is not similar with HTTP that employs a text-based format. The client initiates requests for resources, and the server responds accordingly. The client then acknowledges receipt of the server's response.

Key Features of CoAP

i. RESTful Design:
   - CoAP operates on REST architecture, which is similar to HTTP.
   - It uses methods like GET, POST, PUT, and DELETE to manage resources

ii. Compact and Binary:
   - Unlike HTTP, CoAP is not text-based. It uses a compact binary format, reducing overhead and making it ideal for constrained environments.

iii. Runs over UDP:
- CoAP operates over UDP, which is lightweight compared to TCP, although it sacrifices reliability for efficiency.
- Reliability is managed at the application layer by CoAP itself, with features like message acknowledgments and retransmissions.

Methods in CoAP

i. GET - The GET method retrieves resource information identified by the request URI. A 200 (OK) response indicates success for the GET method.

ii. POST - The POST method creates a new subordinate resource at the specified parent Uniform Resource Identifier (URI) on the server. The server returns a status code of 201 (Created) after successfully creating the resource. Conversely, if resource creation fails, the server responds with a 200 (OK) status code.

iii. DELETE - The delete method is designed to remove the resource identified by the specified URI. Upon successfully executing this operation, the method returns a 200 (OK) response code.

iv. PUT - The PUT method updates or creates a resource identified by the request URI, along with the body message provided in the request. If the resource already exists at the specified URI, the message body is interpreted as a modified version of that resource, resulting in a 200 (OK) response. Conversely, if a new resource is created at that URI, a 201 (Created) response is issued. In situations where the resource is neither created nor modified, an error response code will be returned.

In D2D communication, CoAP's lightweight characteristics are efficient for message exchange. The protocol supports unicast and multicast messaging. It allows multiple devices to communicate concurrently. This feature enhances resource utilization in constrained networks. The CoAP also enables a publish/subscribe model, allowing devices to subscribe to resource changes. This minimizes unnecessary polling and reduces network traffic. However, implementing these features can create significant state management challenges for resource-constrained devices, as servers must keep track of extensive state information for active subscriptions. [22].

In D2C scenarios, the CoAP linked constrained devices and cloud services, allowing smooth data transmission and remote monitoring. CoAP has a low overhead and efficient header structure of only 4 bytes. It is ideal for environments with limited bandwidth. Additionally, frameworks like Californium have been developed to manage many simultaneous CoAP connections. The integration of CoAP with cloud services allows for real-time data analytics and remote device control. It is crucial for applications such as smart health monitoring systems. However, the protocol relying on UDP can pose reliability challenges, especially in high-latency or poor networks, which makes it necessary to implement additional reliability mechanisms.

In C2D communication, CoAP supports asynchronous communication that allows the cloud to send updates to devices without constant polling. This feature is particularly advantageous when devices are intermittently connected or have limited processing power. Apart from that, Datagram Transport Layer Security (DTLS) is used to secure data integrity and confidentiality. It is important for data-sensitive applications such as healthcare. However, the challenge remains in managing the security overhead while maintaining communication efficiency, especially in large-scale deployments.

CoAP is designed to scale efficiently, effectively accommodating small, resource-constrained devices and more powerful servers. It is suitable for various IoT applications because it supports various device types and communication patterns. This characteristic allows seamless interaction among heterogeneous devices in IoT ecosystems. The protocol supports multicast communication, and its integration with cloud services like Californium simultaneously facilitates the management of thousands of devices.

4.3 HTTP/HTTPs

The HTTP (Hypertext Transfer Protocol) protocol is widely used due to its simplicity and flexibility. Besides that, it is a versatile choice because of its compatibility with IoT applications, capability to efficiently manage large volumes of data, and seamless integration with existing web technologies. HTTP architecture operates on a client-server model. The clients, such as web browsers, send requests to servers, which then provide the requested data in response. This mechanism enables the efficient exchange of data across the World Wide Web.

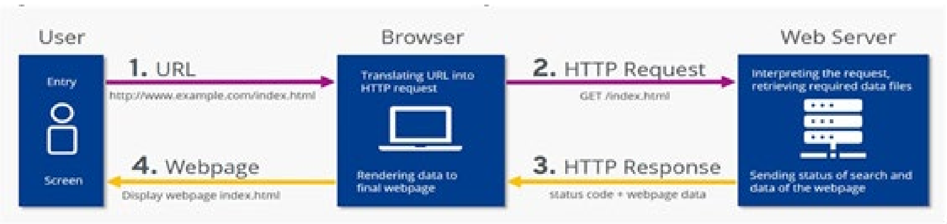
User
Browser
Web Server
Entry
Screen
1. URL
http://www.example.com/index.html
Translating URL into HTTP request
2. HTTP Request
GET /index.html
Interpreting the request, retrieving required data files
4. Webpage
Display webpage index.html
Rendering data to final webpage
3. HTTP Response
status code + webpage data
Sending status of search and data of the webpage

Fig. 2 *Client-server architecture in HTTP*

4.3.1 URL

Uniform Resource Locators (URLs) are uniquely identifying resources on the web. For example, the browser processes the URL http://www.iotgyaan.com/ in the subsequent request message.:

When this request message reaches the server, it can perform one of the actions below:

- The server processes the incoming request by mapping it to a corresponding file in its document directory. Subsequently, it returns the requested file to the client.
- The server analyzes the received request and maps it to a corresponding program stored within its system. Upon executing the program, the server subsequently returns the output generated by the program to the client.
- The request cannot be processed as the server returns an error message.
- Upon receiving the response message, the browser processes and interprets the content before displaying it in the browser window. The presentation of this content is dictated by the media type specified in the Content-Type response header.

Key features of HTTP for efficient device communication include:

i. HTTP is a standardized protocol with widespread adoption, facilitating seamless integration with existing web technologies. This ubiquity enhances its accessibility for a diverse range of IoT applications.

ii. The simplicity of HTTP facilitates its implementation and usage, providing significant advantages for developers and for devices with limited resources.

iii. HTTP demonstrates significant compatibility with established web technologies, facilitating seamless and efficient integration with web servers and services.

iv. HTTP exhibits versatility by supporting various data formats, including JSON and XML. This characteristic renders it particularly suitable for accommodating diverse requirements in IoT data exchange.

v. The built-in caching mechanism of HTTP offers significant advantages for IoT applications, as it enhances the efficiency of repeated requests for identical data.

Table 1 *Comparison between MQTT, CoAP and HTTP*

Protocol	Message Frequency	Message Size	Bits per Second	Effective Device
MQTT	Variable, Low	Small	Moderate to High	Efficient, Low Overhead
CoAP	Variable, Moderate	Small to Medium	Moderate to High	Efficient, Designed for IoT
HTTP	Variable, High	Medium to Large	High	Common, Higher Overhead

The above table demonstrates that each communication protocol possesses distinct strengths and weaknesses, such as message frequency and size. So, the selected protocol must align with the specific requirements of the IoT application, considering factors such as bandwidth, device limitations, and data exchange needs. In D2D communication, HTTP statelessness and simplicity enable straightforward interactions. However, these features can also lead to latency and overhead, especially during high-frequency data exchanges. Research indicates that optimizing HTTP communication can significantly reduce Round Trip Time (RTT) and overall latency, which are crucial for real-time applications. For instance, the shift from HTTP/1.1 to HTTP/2 has effectively addressed issues like head-of-line blocking and improving device data transfer efficiency [23].

For D2C communication, HTTP allows devices to transmit data to cloud services for processing and storage. The lightweight nature and the use of RESTful architecture facilitate scalable and efficient data transmission. It is important in applications like remote monitoring systems, where devices constantly send critical data to cloud platforms for analysis. HTTP in these scenarios supports scalability by allowing numerous devices to communicate simultaneously and enhances reliability through established protocols for error handling and data integrity.

In C2D communication, HTTP sends data and commands back to devices. This type of interaction is essential for applications that need real-time updates or control. This communication's effectiveness depends on the protocol's capability to manage multiple simultaneous connections and its support for persistent connections in HTTP/2. This feature streamlines the establishment of new connections and reduces the associated overhead. The introduction of HTTP/2 has significantly enhanced performance indicators like latency and throughput, which are important for modern IoT applications. Apart from that, the stateless nature of HTTP enables easy scaling, as new devices can be integrated into the network without requiring significant modifications to the existing infrastructure [24].

4.4 AMQP

The Advanced Message Queuing Protocol (AMQP) enables reliable and secure communication between distributed application components. It focuses on message-oriented middleware (MOM) implementations. AMQP is widely used in the financial services industry. In the industry, it serves as an open standard that promotes interoperability among various messaging systems. It effectively manages message routing by supporting both publish-subscribe and point-to-point communication models. The major advantage of AMQP is its ability to manage complex messaging needs, which include content-based routing and durable message exchanges. This advantage is vital for applications that prioritize the reliability and data integrity, especially in environments that experience high latency or poor network conditions. For instance, RabbitMQ, which utilizes the AMQP protocol, is well-regarded for its ability to ensure reliable message delivery and support asynchronous processing in distributed architectures. These features make AMQP suitable for data-intensive applications such as smart factories and autonomous systems. Even though AMQP has many advantages, it also presents certain challenges. AMQP has a higher overhead than the MQTT protocol. This drawback makes it unsuitable for use cases involving devices with limited processing capabilities. Besides, while AMQP shines in environments requiring reliable communication and comprehensive messaging features, its added complexity could discourage its adoption in more straightforward applications.

In D2D communication, AMQP allows asynchronous communication. This characteristic is particularly

beneficial in environments that require low latency, such as industrial automation. It also promotes decoupled communication that allows devices to operate independently and without the need for constant connectivity to a central server. This protocol ensures that messages are not lost, even during network disruptions. When multiple sensors or actuators must coordinate their actions based on shared data, these features help prevent data loss and ensure synchronized operations [25].

In D2C communication, AMQP manages to integrate a diverse range of IoT devices with cloud services. The structured message formats of AMQP enable smooth integration with cloud architecture. It also facilitates seamless data transfers from edge devices to cloud-based analytics services. This transmission efficiency is important for applications that require real-time analytics and decision-making capabilities, which are predictive maintenance in the industry. AMQP comes with security features, such as encryption and authentication, which can enhance the integrity of data exchanged between devices and cloud services. These mechanisms ensure that only authorized devices can access cloud resources and protect sensitive information [21].

AMQP allows the cloud services to control and transmit data to remote devices efficiently in C2D communication. This is important for delivering device updates, commands, or configuration changes. AMQP minimizes the risk of message overflow or loss through its queuing mechanisms. This capability ensures that critical updates are sent promptly without overloading the device’s processing capacity. Additionally, the built-in feedback mechanisms of AMQP enable devices to acknowledge the receipt of commands or data, thereby enhancing communication reliability.

Its ability to manage message queues and process large volumes of data results in high throughput and reduced latency are essential for optimal resource utilization in IoT systems. This relevance becomes even more important as IoT environments grow, requiring scalable communication protocols supporting a steadily increasing number of devices.

Features like message acknowledgments and persistent messaging ensure reliability in AMQP. It guarantees that messages are recorded and can be retried [21]. These features effectively mitigate the impact of temporary network failures so that it can ensure the continuous operation of critical applications. Its capability to create a durable queue allows the system to retain messages for future processing. This feature is particularly essential during maintenance windows or unexpected downtimes [25].

The architecture of AMQP supports the efficient scaling of IoT applications. It allows for the integration of additional devices without the need for significant modifications to the existing framework. This adaptability is essential in dynamic settings where the device landscape may change frequently due to rapid technological advancements or evolving market demands. Additionally, AMQP compatibility with other messaging standards enhances its scalability, facilitating the seamless integration of various IoT solutions as organizations refine and advance their IoT strategies.

4.5 Web Socket

WebSocket is a communication protocol that enables real-time, bidirectional interactions between clients and servers over the web. It operates on a request-response model that requires a new connection for each interaction. It maintains a persistent connection that allows for continuous data exchange. This is similar to keeping a phone call open, enabling the client and server to send messages instantly in either direction, rather than making repeated calls. This characteristic makes it valuable for IoT applications that require rapid and efficient communication. It also supports full-duplex communication. This feature allows data to be transmitted and received simultaneously. Consequently, it significantly reduces the overhead of establishing multiple connections, which is typical in standard HTTP interactions. Once the initial HTTP handshake has established a WebSocket connection, data can flow freely in both directions without further requests. This unique characteristic greatly enhances overall communication efficiency. This is especially important in contexts such as real-time monitoring and control of IoT devices, where prompt information delivery is essential.

WebSocket technology is advantageous for D2D communication because it allows devices to interact directly without a centralized server. By maintaining persistent open connections, devices can instantly exchange sensor data or control messages. For example, smart home devices can turn lights on/off or adjust thermostats in real-time based on user commands or sensor inputs and avoid delays commonly associated with traditional request-response methods.

In D2C communications, WebSocket enables IoT devices to send data continuously to cloud services. Devices can push updates in real-time and allow cloud services to analyze and respond to incoming data instantaneously by establishing a WebSocket connection.

The bi-directional nature of WebSocket is highly advantageous for C2D communication. Cloud servers can efficiently transmit commands to devices and facilitate features such as firmware updates or configuration changes. The real-time capabilities of WebSocket connections ensure that devices receive updates without significant delays, which is important for maintaining security and functionality across interconnected systems [26].

The connection management mechanisms of WebSocket can ensure the smooth re-establishment of connections if lost. This feature is essential for high-availability applications such as emergency response systems and critical monitoring setups. WebSocket allows devices and applications to maintain uninterrupted interactions, enhancing system reliability.

WebSocket can manage numerous simultaneous connections. It is crucial in the IoT landscape, where potentially thousands of devices may need to communicate with a server concurrently. Its capacity to support many concurrent connections without sacrificing performance makes WebSocket ideal for large-scale IoT implementations

5. Recent Issues in Network and Communication

5.1 Security Challenges: Vulnerabilities and Attacks on IoT Networks, including DDoS attacks and Data

The rapid growth of IoT applications introduced significant vulnerabilities and security challenges. It makes IoT networks become the prime targets for cyberattacks. Distributed Denial of Service (DDoS) attacks and data breaches are among the most critical threats. Both threats exploit the inherent weaknesses in IoT devices and their networks.

The main vulnerability in IoT networks is the user's weak or default password setting. It is common among many devices. Many IoT devices are shipped with factory-set passwords that users often forget to change. This problem makes these devices easily exploitable for attackers. The weak authentication mechanisms worsen the problem, resulting in unauthorized access to sensitive data and control of devices. User and device authentication mechanisms are crucial for securing IoT networks. This is because they help prevent unauthorized access and ensure that only legitimate devices can communicate. Combining multi-factor authentication (MFA) techniques with lightweight algorithms can enhance security without placing too much strain on resource-limited devices [27]. There is an approach that highlights the significance of combining biometrics with traditional authentication methods to bolster access security. Several research also suggested the utilization of blockchain technology to create a secure, decentralized framework for identity management and authentication. This decentralized structure enhances security against cyber threats, ensuring that data remains tamper-proof and is accessible only to authorized entities. Blockchain can also enable secure transactions between devices and supports the implementation of smart contracts. It automating processes when specific conditions are fulfilled. For example, stakeholders can verify transactions involving IoT devices to track goods in supply chain applications. This approach improves efficiency and strengthens the parties' trust [28]. Pseudonymous authentication combined with blockchain enables devices to communicate without revealing their identities and enhancing user privacy. This approach allows real-time transactions while ensuring high security and trust in the network.

Besides, the lack of encryption during data transmission makes IoT networks vulnerable to data interception and increasing the risk of data breaches that can severely impact user privacy and security. The architecture of IoT networks itself also contributes to their vulnerability. This is because many devices operate on outdated firmware. It may contain unpatched security flaws that attackers can exploit [29]. The heterogeneity of devices in IoT environments also complicates security management due to each device may have different security requirements and vulnerabilities. This diversity can lead to inconsistent security policies and practices and increase the risk of successful attacks. Apart from that, the lack of network segmentation enables attackers to move laterally within the network after compromising a single device in consequently it could potentially lead to the compromise of multiple systems. So, encryption is essential for protecting data transmitted between IoT devices and ensuring information confidentiality, integrity, and authenticity. Lightweight encryption algorithms are advantageous in IoT environments because of the limited resources typically found in these devices. Tiny Encryption Algorithm (TEA) is widely used due to its straightforward implementation and proven effectiveness in securing data during transmission [30]. To protect sensitive data from unauthorized access and tampering, secure communication is essential for various IoT applications, including smart home systems and industrial automation. Elliptic Curve Cryptography (ECC) has emerged as a popular asymmetric encryption method. ECC can offer strong security with smaller key sizes, making it ideal for resource-constrained IoT devices [31].

DDoS attacks pose a significant threat to IoT networks. Cybercriminals can exploit compromised IoT devices, commonly known as "botnets" to execute large-scale attacks. It targeted servers or networks with traffic and rendering them inoperable. The ability of attackers to easily find vulnerable devices through services like Shodan worsens the situation. It enables them to create a botnet using numerous insecure IoT devices rapidly. In addition to DDoS attacks, data breaches are a significant threat to IoT networks. The sensitive information collected and transmitted by IoT devices is an attractive target for cybercriminals. Once attackers gain access to an IoT device, they can harvest sensitive data and manipulate the device's functionality or even launch additional attacks on other connected systems. The implications of such breaches extend beyond individual users. This is because compromised IoT devices can be used to infiltrate larger networks and leading to widespread data exposure and security incidents [32]. There are various strategies that have been proposed to mitigate these vulnerabilities. Strong authentication mechanisms can significantly reduce the risk of unauthorized access. Secondly, regularly updating device firmware and thirdly, using robust data-transmission encryption protocols are essential to improving IoT security. Besides, network segmentation can help contain potential breaches and prevent attackers from moving freely across the network if one device is compromised. Moreover, the development of automated security assessment tools can aid in identifying vulnerabilities within IoT networks. These tools can analyze network traffic and device behavior to detect anomalies indicative of potential attacks. By employing machine learning and deep learning techniques, security systems can also adapt to evolving threats and improve their ability to predict and mitigate attacks.

5.2 Interoperability Issues: Difficulties in Integrating Diverse IoT Devices and Protocols

To integrate different IoT technologies, especially various application layer protocols, there exist many challenges in achieving seamless interoperability. For instance, integrating 6LoWPAN devices into legacy IPv4 networks highlights the difficulties caused by differing communication standards [33]. This challenge is made more difficult by the need for IoT systems to support multiple protocols and each with its specific requirements and capabilities. This problem directly leads to complexities in data exchange and device interaction. IoT networks' diverse nature requires multiple communication protocols. It can differ significantly in their transmission capabilities and operational ranges. This variety complicates devices' seamless integration and interaction, as different protocols may be incompatible. For example, integrating short-range protocols like Bluetooth with long-range protocols such as LoRaWAN demands careful consideration of the underlying network architecture to ensure effective communication. So, standardization efforts are essential for tackling interoperability challenges in IoT. Developing common communication protocols and interoperability standards is important to ensure seamless integration and data exchange among various IoT devices. Research has demonstrated that without such standardization, the potential of IoT applications is significantly limited. This is because many devices may face difficulties communicating effectively across different platforms and protocols. Additionally, integrating emerging technologies like blockchain into IoT systems adds further complexity since these technologies often require their own specific protocols and standards and further complicated the overall interoperability landscape. Besides that, the operational environment of IoT devices plays a crucial role in their integration. Devices deployed in outdoor or harsh conditions face numerous challenges, which are temperature fluctuations, humidity, and physical obstructions. All the challenges can adversely impact their performance. For example, devices that depend on wireless communication may experience poor signal quality in difficult environments, such as densely populated urban areas with numerous high-rise buildings [34]. Environmental factors can also significantly impact power consumption. This is because the devices must adjust to maintain functionality under varying conditions. This necessary adaptation may require more energy-intensive processing or increased communication attempts and intensifying power management challenges. Efficient integration must consider these environmental factors to ensure reliability and optimal performance across diverse environments. Interoperability issues within the IoT are complex and arise from the various devices and protocols currently used. To address these challenges, there must be a collaborative effort toward standardization and developing middleware solutions that enable communication across diverse networks. The continuous evolution of IoT technologies requires ongoing research and innovation to ensure that interoperability is achieved and unlock the full potential of IoT applications across various fields.

5.3 Network Congestion and Latency: The Impact of Increased Device Density on Communication Efficiency

The rapid expansion of IoT devices has introduced numerous challenges that affect scalability, bandwidth constraints, data volume management, traffic management, and spectrum utilization within IoT networks. Understanding these challenges is important for developing effective solutions and ensuring the sustainability of IoT ecosystems.

Scalability typically refers to the ability of the system to handle increasing workloads or increased connected devices without declining performance. With the number of connected devices projected to reach 75 billion by 2025, traditional centralized cloud architectures are proving increasingly inadequate for managing the resulting data traffic. Conventional network infrastructures also struggle to keep pace with such growth, which results in elevated latency and reduced throughput. The existing communication protocols may not be equipped to support the dynamic scaling required in IoT environments and limit the capacity of the network to expand and adapt as needed.

As the number of IoT devices continues to increase, the demand for available bandwidth has also significantly increased. Many IoT applications rely on uninterrupted connections and frequent data transmission. It places considerable pressure on existing bandwidth resources. This situation, called "spectrum crunch," arises when the number of devices competing for limited frequency bands escalates, leading to congestion and reduced network performance. Additionally, high-bandwidth applications, such as video monitoring, have worsened these constraints by consuming large amounts of available spectrum and leaving less bandwidth for devices that require lower data rates [35].

The limitations of traditional static spectrum allocation methods create significant challenges. Many wireless communication systems depend on predefined frequency bands. It may not be adequate to support the growing variety and number of connected IoT devices. Cognitive radio (CR) technology is a potential solution that enables devices to access and utilize the available spectrum more efficiently. By implementing spectrum sensing and opportunistic access protocols, CR-enabled IoT devices can detect unused frequency bands and dynamically reallocate resources based on real-time availability [36]. The complexity of these systems and the limited hardware of many IoT devices pose challenges for effective spectrum management.

High volumes of data are generated by IoT devices nowadays. This problem can overwhelm cloud storage systems and data processing resources and affect the responsiveness of the critical applications. Additionally, unnecessary or redundant data transmission can escalate operational costs and lead to resource inefficiencies. This underscores the need for intelligent data aggregation and compression techniques to optimize data flow within IoT networks.

Effective traffic management is important to prevent congestion and ensure seamless device communication. The complexity of traffic patterns resulting from the growth of connected devices can create bottlenecks within the network. The need for low-latency communication in applications such as autonomous vehicles and real-time monitoring systems further complicates this issue. Advanced traffic management strategies must be adopted to tackle these challenges. The strategies include dynamic load balancing and prioritization of critical applications to ensure that high-priority traffic is transmitted without delays. Besides that, transitioning to a more decentralized approach, such as fog computing, is essential to reduce high access latencies and network congestion. In the healthcare industry, the large data generated by IoT devices can cause significant network congestion, leading to increased latency. High round-trip times resulting from extensive data transmission and multiple hops between IoT devices and cloud servers can make healthcare data less effective for end-users [37]. Low-latency communication is vitally important in applications where timely data transmission can be lifesaving, underscoring the importance of optimizing network performance to handle the dense deployment of devices. Furthermore, integrating advanced technologies such as Multi-Access Edge Computing (MEC) and AI is being explored to improve communication efficiency in IoT networks. MEC enhances cloud capabilities at the network edge in order to enable real-time data processing and minimize latency. This is particularly relevant when IoT devices are energy-limited and require efficient resource management to maintain performance. Additionally, leveraging intelligent reflecting surfaces (IRS) in 6G networks is proposed to optimize energy-efficient communication further to tackle the challenges of high data traffic and the need for low-latency services. The challenges posed by increased device density are further complicated by the need for strong communication protocols that adjust to changing traffic conditions. Research shows that current protocols frequently have difficulty maintaining performance during high congestion, resulting in packet collisions and longer latency [38]. Therefore, developing adaptive transmission schemes and optimizing resource allocation are critical for sustaining communication efficiency in densely populated IoT environments.

5.4 Regulatory and Compliance Factors: How Evolving Regulations Affect IoT Network Design and Communication Practices

The changing regulatory landscape significantly impacts the design and communication practices of IoT networks. The urgency for strong regulatory frameworks is vitally important, as IoT technologies continue to grow. These frameworks ensure the security, privacy, and interoperability of various IoT devices and systems. Integrating regulatory compliance into IoT design requires a shift from traditional regulatory approaches to adaptive governance models that can effectively respond to the dynamic nature of technology and its associated risks. One of the main challenges in designing IoT networks is ensuring compliance with regulatory standards that differ across regions and sectors. The integration of hardware and software in IoT systems complicates the certification process because it necessitates adherence to various regulatory requirements regarding data protection, user privacy, and device interoperability. Establishing common security standards is also crucial for fostering trust and facilitating the widespread adoption of IoT technologies. Research indicates that standardization efforts can mitigate vulnerabilities and enhance the security of IoT ecosystems by defining protocols for secure communication, authentication, and data protection. Moreover, the right to data portability (RtDP) poses additional challenges in the IoT context. This is because the current IoT systems often lack the necessary infrastructure to support this right effectively. This limitation highlights the need for regulatory bodies to address the interoperability and data management issues inherent in IoT networks [39]. As IoT devices become increasingly interconnected, the potential for data breaches and privacy violations escalates. A stringent regulatory measure is necessary to safeguard user information and ensure compliance with data protection laws. The emergence of new technologies like 5G and edge computing makes IoT network design and regulatory compliance more complex. These technologies allow for the creation of more scalable and efficient IoT networks but also bring about new security challenges. To address these issues, comprehensive regulatory frameworks are necessary. Policymakers must balance the adoption of innovation and investment in IoT services with the need to protect societal interests. It requires a nuanced understanding of the relationship between technology, regulation, and public safety.

Legislation like the Personal Data Protection Act (PDPA) is important in guiding the development of systems. It is a guideline to ensure user privacy is a top priority in technological design. The principles of data minimization and purpose limitation, which are central to the PDPA, require IoT developers to collect only the data necessary for the intended function of the device. So, developers must carefully consider their design choices to prevent the unintentional collection of excessive data [40]. IoT devices should be designed to limit data collection to pre-defined functionalities and at the same time, to ensure compliance with legal frameworks and maintain user trust. Adhering to the PDPA requires robust security measures to protect personal data, which include data encryption, secure storage solutions, and access controls that enhance the integrity and confidentiality of data transmitted between devices. Developers must integrate privacy-by-design principles and emphasize incorporating privacy features throughout all phases of IoT network architecture. Even though it can increase complexity and development costs, it is essential. The PDPA mandates that individuals provide explicit consent before processing their personal data. Therefore, IoT networks must implement mechanisms that empower users to manage their consent effectively. This necessitates IoT devices to include built-in functionalities for users to approve or revoke consent for data collection at any time. These requirements can significantly influence the design of user interfaces and interaction models within the IoT ecosystem and highlight the need for user-friendly consent management solutions [41].

Under the PDPA, organizations must inform individuals about the purposes for which their data is collected. This requirement calls for IoT communication practices to include features that enhance transparency. For instance, devices should deliver clear notifications when data collection occurs and explain how that data will be utilized [42]. IoT systems typically involve multiple stakeholders, including application developers, service providers, and third-party vendors. Therefore, the PDPA strictly regulates the sharing of personal data with third parties. It necessitates organizations to create formal data-sharing agreements that clarify responsibilities related to privacy protection. Consequently, IoT communication protocols must incorporate provisions to safeguard information during sharing and establish accountability mechanisms throughout the data-sharing process.

Variations in data protection laws across different countries, such as the PDPA and GDPR, pose significant challenges for developers of IoT systems that are aimed at global markets. To ensure compliance with the most rigorous privacy standards, developers must create flexible IoT architectures that can adapt to various regulatory frameworks [40]. This may lead to considerable additional overhead throughout the development process. Many IoT devices, especially those used in industrial or remote environments, typically operate under stringent resource constraints, including limited processing power, memory, and battery life. Enforcing rigorous privacy measures can be resource-intensive and make it challenging to incorporate compliance features without undermining the functionalities of the device. Finding the right balance between privacy compliance, effective communication, and device performance continues to challenge IoT developers. The changing regulatory landscape substantially impacts IoT network design and communication practices. In summary, it is increasingly important to develop flexible governance models that can handle the complexities of IoT ecosystems. To support the sustainable development of IoT networks, it is also essential to ensure compliance with various regulatory requirements, promote interoperability through standardization, and address emerging security challenges.

6. Case Study Application: Smart Agriculture

Smart agriculture is a transformative approach for farming that integrates advanced technologies, which are the IoT, machine learning, and data analytics to improve productivity and sustainability. The development of smart agriculture frameworks relies on several key components, including sensing technologies, communication systems, and data analytic solutions. All these elements enable real-time monitoring and decision-making in agricultural practices. The main advantage of smart agriculture is its capacity to optimize resource management by precisely monitoring and controlling agricultural inputs. For example, IoT-based systems enable farmers to visualize sensor data, manage irrigation systems, and optimize water usage. These capabilities lead to improved crop yields and greater resource efficiency. Besides that, the integration of machine learning techniques further enhances these capabilities by enabling predictive analytics that can forecast crop performance based on environmental conditions and historical data [43].

However, challenges persist in their deployment. The first one is connectivity problems, especially in rural areas. This problem can limit the effectiveness of IoT applications and restrict access to real-time data and analytics by the farmers. Besides that, the power requirements, environmental robustness, and cost-effectiveness will also be considered. So, an effective, reliable, and scalable network and communication protocols must be tailored to suit the IoT design in smart agriculture.

The communication frameworks and networks used in smart agriculture are essential for efficient data transmission and real-time monitoring of agricultural practices. These frameworks utilize various wireless communication technologies, including 4G, 5G, LoRa, and Wi-Fi, to connect numerous sensors and devices deployed across agricultural fields. Each technology has its own unique advantages and challenges, so the choice of technology depends on specific agricultural needs and environmental conditions. Among these communication protocols, cellular technology is prioritized. The 4G and 5G technology is a transformative force in smart agriculture because of its high data transfer rates, low latency, and capacity to support a large number of connected devices per square kilometer. This capability is crucial for applications that require real-time data processing and immediate responses, such as automated irrigation systems and precision farming techniques [44]. The implementation of 5G technology in agriculture not only improves operational efficiency but also facilitates advanced applications such as autonomous vehicles and drones, which can gather and analyse data over large areas. The low-latency communication provided by 5G is particularly beneficial for applications that demand quick decision-making, such as pest control and crop monitoring.

If the 4G or 5G network is unavailable, an alternative option is necessary. LoRa technology is an important communication framework used in smart agriculture. This is because it is designed for long-range communication with low power consumption. LoRa is suitable for connecting sensors deployed over extensive agricultural areas, where traditional WiFi or cellular networks may be impractical due to their range limitations. This technology enables the deployment of numerous sensors to monitor soil moisture, temperature, and other environmental factors. These capabilities support precision agriculture practices that optimize resource use and enhance crop yields. LoRa technology is known for penetrating dense foliage and effectively functioning in rural areas, which is particularly valuable for smart farming initiatives. In addition, the Internet of Underground Things (IoUT) has emerged as an innovative approach to precision agriculture. This framework uses sensors and communication devices installed underground to monitor soil conditions in real time. The IoT allows for the seamless integration of underground data with surface-level agricultural practices. It provides comprehensive insights into soil health and moisture levels to the farmers. This integration is crucial for optimizing irrigation and fertilization practices and improving crop productivity and sustainability [45].

Integrating hybrid communication frameworks, particularly LoRa technology with cellular networks can offer a promising solution to address the connectivity challenges rural areas face. The regions for farming often struggle with connectivity issues due to geographical barriers, lower population density, and insufficient infrastructure investment. Traditional cellular networks typically require substantial investments to extend coverage to these areas, so, it is economically unviable for many service providers. As a result, numerous rural communities remain underserved and experience limited internet access that hinders the potential for IoT applications. Hybrid communication frameworks incorporating LoRa technology with cellular networks can help overcome these connectivity challenges. LoRaWAN is a low-power and long-range wireless protocol designed specifically for IoT. It allows devices to communicate over several kilometers while consuming minimal energy. LoRa can transmit data from remote sensors to cellular gateways when integrated with cellular networks. It significantly enhances coverage and connectivity options in rural areas. By implementing the long-range capabilities of LoRa, rural IoT applications can establish connections that would otherwise be inaccessible through cellular networks alone. LoRa operates effectively in remote areas and enables devices to relay data to nearby gateways. It bridges the connection to the cellular network. Deploying LoRa networks can be relatively cheap because fewer cellular base stations are needed to cover a broad area. This model allows smaller communities to implement IoT solutions without extensive infrastructure costs. IoT devices that utilize LoRa technology also consume significantly less power than their cellular counterparts. This advantage makes them suitable for applications in agriculture, where devices may rely on battery or solar power. Devices can monitor soil moisture, temperature, and nutrient levels across expansive agricultural lands. The data is collected through low-power sensors and transmitted using LoRa to a central gateway, and then the information is sent via a cellular network to the cloud server. This setup enables farmers to receive actionable insights in real-time and facilitates optimized irrigation and resource management. Smart irrigation systems can dynamically adjust water supply based on real-time soil moisture data. These solutions are effective in drought-prone areas. The value propositions are substantial water savings and improved crop yields, which are essential for sustainable agriculture [46]. Furthermore, technology like smart collars utilizing LoRa to track livestock location and health parameters in rural pastures. By gaining insight into animal behavior and location, farmers can make decisions based on the analyzed data from cloud computing. This data is also transmitted via cellular networks for continuous monitoring, supporting animal welfare and operational efficiency [47].

The integration of edge computing with communication frameworks enhances data processing speed, decreases central server load, and improves the efficiency of smart agriculture systems. Edge computing is transforming smart agriculture by enabling real-time data processing and decision-making directly at the source. This approach enhances efficiency, reduces latency, and optimizes resource management. As a decentralized computing model, edge computing supports various applications in smart farming, from precision agriculture to autonomous machinery. Data is being processed locally instead of relying on centralized cloud servers. When integrated with AI, edge computing significantly increases its potential to transform agriculture into a more data-driven and sustainable industry. It allows for immediate data analysis from IoT sensors and devices, facilitating real-time monitoring and decision-making in agricultural operations. It supports precision agriculture by enabling the analysis of on-field sensor data, which is essential for monitoring crop health and assessing soil conditions. Additionally, deploying AI algorithms on edge devices enhances decision-making capabilities directly in the field, allowing for improved disease detection and intelligent irrigation. Edge AI reduces reliance on cloud computing and indirectly enhances data privacy and security while addressing connectivity challenges in rural areas.

7. Conclusion

The evolving landscape of IoT systems requires tailored network and communication protocols to meet diverse operational needs. Every IoT application, from smart agriculture to industrial automation, requires a customized connectivity approach that take into account of power consumption, bandwidth, range, and latency. Wi-Fi and Bluetooth are ideal for short-range, high-bandwidth applications like smart homes. Meanwhile, 4G and 5G networks provide low latency and broad coverage, which is essential for real-time industrial and agricultural applications. LoRa technology is advantageous for large-scale deployments in rural areas with limited infrastructure. Communication protocols such as MQTT and CoAP emphasize the importance of lightweight, scalable solutions designed for resource-constrained devices to ensure efficiency and reliability. While AMQP provides a reliable framework for message queuing and communication across diverse technologies, especially in the finance services industry. The robust routing and support for advanced messaging patterns make it essential for large-scale, high-availability systems. WebSocket real-time capabilities enable dynamic interactions among interconnected devices and promote advanced or resource-efficient applications.

Implementation of encryption standards, authentication mechanisms, and blockchain technology are crucial to tackling the security challenges of IoT networks. The adoption of lightweight encryption algorithms can ensure secure data transmission. Multifactor authentication methods enhance the security of both users and devices. It reduces the risk of unauthorized access. While blockchain technology provides a strong framework for decentralized trust and efficient transactions among connected devices. All these security measures strengthen IoT ecosystems and pave the way for broader adoption and safer implementation of IoT applications across various sectors. Integrating diverse IoT devices and protocols presents multifaceted challenges. To overcome these difficulties arising from varying protocols, the environmental factors, power consumption constraints, and traffic management will be pivotal in developing cohesive and efficient IoT systems. Future research and innovation should focus on creating interoperable frameworks and adaptive technologies that acknowledge and respond to these challenges to ensure the sustainability and efficacy of IoT applications. Furthermore, integrating the PDPA into IoT network design and communication practices highlights the importance of privacy and data protection. By prioritizing privacy, it can enhance compliance with relevant regulations and foster user trust and long-term adoption of IoT technologies. The challenges posed by diverse regulatory landscapes and resource limitations necessitate ongoing dialogue among stakeholders to develop harmonized solutions that uphold user privacy rights and at the same time harnessing the full potential of IoT ecosystems.

Incorporating energy-efficient communication protocols and advanced security models can significantly enhance the performance and sustainability of IoT deployments. One of the protocols is the Energy-Efficient Datagram Transport Layer Security (eeDTLS). It reduces message headers and modifies the handshake process to minimize energy consumption during secure data transmissions. Another approach is the Lithe protocol that combines the benefits of the CoAP with the features of DTLS. This integration achieves secure data transmission and compress headers. These features allow IoT systems to operate efficiently by reducing the amount of data transmitted across networks. Consequently, this saves both power and bandwidth. The adoption of Narrowband IoT (NB-IoT) technology is also an effective approach. This is because it focuses on energy-efficient data routing and transmission. It ensures that IoT devices consume minimal power while maintaining reliable connectivity. Besides that, Energy-Efficient OpenHIP-Based Security (E-HIP) model represents an advanced security framework that prioritizes energy conservation and ensures robust security for IoT networks [48]. E-HIP can enhance overall security and keeps additional energy costs for IoT devices to a minimum. Furthermore, adopting a fuzzy logic approach to security can also improve decision-making processes within IoT networks and enable adaptive security measures that align with varying environmental and operational conditions. These systems can dynamically assess risks associated with data transmission and adjust security protocols as needed. Therefore, it can balance energy efficiency and security requirements [49]. Future research should continue to investigate these intersections and develop more sustainable and secure IoT ecosystems capable of supporting an expanding array of applications.

Integrating hybrid communication frameworks, such as LoRa technology with cellular networks, presents a promising solution for enhancing rural connectivity in IoT applications. These frameworks expand network coverage, reduce costs, and improve efficiency and sustainability in smart agriculture. The potential to transform rural communities through innovative connectivity solutions is significant because it provides a pathway to bridge existing gaps. The progression toward 6G networks also signifies a transformative shift. It can enhance connectivity, responsiveness, and functionality compared to hybrid systems that rely on 5G and LoRa communication protocols. This emerging trend focuses on higher data throughput and lower latency and emphasizes the integration of AI to support advanced applications across various sectors. 6G networks are expected to accommodate numerous IoT devices, estimated to be in the tens of billions. It will improve services and applications that current technologies cannot adequately support. Research suggests that 6G will utilize higher frequencies, such as terahertz (THz) bands, to facilitate ultra-reliable, low-latency communication systems. This improvement is crucial for applications requiring real-time data processing and rapid response times. It is expected to solve the limitations faced by existing hybrid 5G and LoRa frameworks. Moreover, the architectural advancements in 6G will incorporate a more robust and intelligent network design by utilizing AI algorithms to dynamically manage resources and optimize network conditions for enhanced efficiency and reliability. For example, drones with AI analytics can use 6G networks to transmit high-resolution images and data to farmers in real time. It enables immediate assessment and swift responses to pest infestations or diseases. The real-time data transfer capabilities in a 6G environment are greatly enhanced and make it difficult to replicate the same level of responsiveness with traditional hybrid 5G and LoRa connections, which may experience delays and bandwidth limitations. [50]. The 5G and LoRa communications hybrid model still faces challenges related to coverage limitations and data transmission rates. In contrast, 6G networks are designed to enhance reliability and scalability and address the throughput limitations that hinder large-scale IoT deployments. The combination of 6G technology and the analytical capability of AI offers a comprehensive solution to meet current and future IoT needs. Transitioning from hybrid 5G and LoRa communication frameworks to AI-powered 6G networks represents a significant advancement in tackling the challenges within the IoT landscape. IoT solutions can improve performance, responsiveness, and efficiency across various application domains by adopting this technology in the future. This convergence opens an exciting frontier for future research and innovation and paves the way for more intelligent, efficient, and sustainable smart systems.

Acknowledgement

We would like to thank the Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia for giving the opportunity to conduct this study.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Shipun Anuar Bin Hamzah, Loh Yin Chyuan;* ***data collection:*** *Shipun Anuar Bin Hamzah;* ***analysis and interpretation of results:*** *Shipun Anuar Bin Hamzah, Mohd Salleh bin Md Roslan;* ***draft manuscript preparation:*** *Shipun Anuar Bin Hamzah, Loh Yin Chyuan. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] Hussain, R., Hassan, S., & Hossain, E. (2020). Machine learning in iot security: current solutions and future challenges. Ieee Communications Surveys & Tutorials, 22(3), 1686-1721. https://doi.org/10.1109/comst.2020.2986444

[2] Jeknić, A. and Kočan, E. (2023). Development steps that brought to wi-fi 7. ETF Journal of Electrical Engineering, 29(1), 65-79. https://doi.org/10.59497/jee.v29i1.266

[3] Alawi, M., Sundararajan, E., Zin, A. M., Alsaqour, R., & Ismail, M. (2019). Opportunistic offloading scheme in heterogeneous vehicular network. International Journal of Innovative Technology and Exploring Engineering, 8(6S4), 1348-1351. https://doi.org/10.35940/ijitee.f1273.0486s419

[4] Nguyen, Tuan C. "Who Invented Bluetooth?". ThoughtCo. Archived from the original on 11 October 2019. Retrieved 11 October 2019.

[5] Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2018). Security threats in bluetooth technology. Computers &Amp; Security, 74, 308-322. https://doi.org/10.1016/j.cose.2017.03.008

[6] Jain, R. (2024). Impact of 5g wireless technologies on cloud computing and internet of things (iot). Advances in Robotic Technology, 2(1), 1-7. https://doi.org/10.23880/art-16000107

[7] Shang, X., Liu, A., Wang, Y., Xie, Q., & Wang, Y. (2018). Energy-efficient transmission based on direct links: toward secure cooperative internet of things. Wireless Communications and Mobile Computing, 2018(1). https://doi.org/10.1155/2018/5012096

[8] Centelles, R. P., Freitag, F., Meseguer, R., & Navarro, L. (2021). Beyond the star of stars: an introduction to multihop and mesh for lora and lorawan. IEEE Pervasive Computing, 20(2), 63-72. https://doi.org/10.1109/mprv.2021.3063443

[9] Wan, Q. and Liu, J. (2018). Smart-home architecture based on bluetooth mesh technology. IOP Conference Series: Materials Science and Engineering, 322, 072004. https://doi.org/10.1088/1757-899x/322/7/072004

[10] Saraereh, O. A., Alsaraira, A., Khan, I., & Uthansakul, P. (2020). Performance evaluation of uav-enabled lora networks for disaster management applications. Sensors, 20(8), 2396. https://doi.org/10.3390/s20082396

[11] Ibáñez, L. C., Mir, B., Vidal, R., & Gómez, C. (2017). Modeling the energy performance of lorawan. Sensors, 17(10), 2364. https://doi.org/10.3390/s17102364

[12] Lopes, I., Barbosa, R. S., Santos, D. D. d., Melo, J. M. M. d., Vellame, L. M., Oliveira, E. A. d., … & Schwiderke, S. K. (2024). Lora-based iot platform for remote soil parameter monitoring. Dyna, 91(231), 86-93. https://doi.org/10.15446/dyna.v91n231.111612

[13] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of things: a survey on the security of iot frameworks. Journal of Information Security and Applications, 38, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002

[14] Arachchige, K. G., Branch, P., & But, J. (2023). Evaluation of blockchain networks' scalability limitations in low- powered internet of things (iot) sensor networks. Future Internet, 15(9), 317. https://doi.org/10.3390/fi15090317

[15] Xiao, J., Chang, C., Wu, P., & Ma, Y. (2023). Attribute identification based iot fog data security control and forwarding. PeerJ Computer Science, 9, e1747. https://doi.org/10.7717/peerj-cs.1747

[16] Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: a survey. IEEE Internet of Things Journal, 5(1), 450-465. https://doi.org/10.1109/jiot.2017.2750180

[17] Hou, Y., Garg, S., Lin, H., Jayakody, D. N. K., Jin, R., & Hossain, M. S. (2020). A data security enhanced access control mechanism in mobile edge computing. IEEE Access, 8, 136119-136130. https://doi.org/10.1109/access.2020.3011477

[18] AlSuwaidan, L. (2020). The role of data management in the industrial internet of things. Concurrency and Computation: Practice and Experience, 33(23). https://doi.org/10.1002/cpe.6031

[19] Mishra et al. "Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements" Energies (2021) doi:10.3390/en14185817

[20] Shan "IoT Communication Based on MQTT and OneNET Cloud Platform in Big Data Environment" (2024)

[21] Khan et al. "A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT" Sensors (2021) doi:10.3390/s21217016

[22] Islam et al. "Transparent CoAP Services to IoT Endpoints through ICN Operator Networks" Sensors (2019) doi:10.3390/s19061339

[23] Darwish et al. "Impact of Implementing HTTP/2 in Web Services" (2016) doi: 10.5120/ijca2016911182

[24] Naik et al. "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP" (2017) doi: 10.1109/syseng.2017.8088251

[25] Ferlito, S., Ippolito, S., Santagata, C., Schiattarella, P., & Francia, G. D. (2024). A study on an iot-based scada system for photovoltaic utility plants. Electronics, 13(11), 2065. https://doi.org/10.3390/electronics13112065

[26] Banik, S., Cardenas, I. S., & Kim, J. (2019). Iot platforms for 5g network and practical considerations: a survey. https://doi.org/10.48550/arxiv.1907.03592

[27] Chiadighikaobi, I. R., Katuk, N., & Osman, B. (2022). Dmuas-iot: a decentralised multi-factor user authentication scheme for iot systems. International Journal of Computing, 424-434. https://doi.org/10.47839/ijc.21.4.2777

[28] Hasan, A. S. M. T., Sabah, S., Haque, R. U., Daria, A., Rasool, A., & Jiang, Q. (2022). Towards convergence of iot and blockchain for secure supply chain transaction. Symmetry, 14(1), 64. https://doi.org/10.3390/sym14010064

[29] Li, M., Yan, Y., & Zou, Y. (2023). Iot devices firmware security detection based on static analysis technology.. https://doi.org/10.1117/12.2679937

[30] Rajesh, S., Paul, V., Menon, V. G., & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded iot devices. Symmetry, 11(2), 293. https://doi.org/10.3390/sym11020293

[31] Agrawal, L. and Tiwari, N. (2020). Optimized ecdsa algorithm for secure and efficient use in iot network. International Journal of Recent Technology and Engineering (IJRTE), 8(5), 980-984. https://doi.org/10.35940/ijrte.e5767.018520

[32] Gu, D. (2023). Iot device identification based on network traffic.. https://doi.org/10.21203/rs.3.rs-3348638/v1

[33] Saavedra et al. "Leveraging IoT Harmonization: An Efficacious NB-IoT Relay for Integrating 6LoWPAN Devices into Legacy IPv4 Networks" (2024) doi: 10.3390/app14083411

[34] Aldossary, M. (2023). Multi-layer fog-cloud architecture for optimizing the placement of iot applications in smart cities. Computers, Materials &Amp; Continua, 75(1), 633-649. https://doi.org/10.32604/cmc.2023.035414

[35] Khalid, W. and Yu, H. (2019). Spatial–temporal sensing and utilization in full duplex spectrum-heterogeneous cognitive radio networks for the internet of things. Sensors, 19(6), 1441. https://doi.org/10.3390/s19061441

[36] Jaronde, P. (2024). Encapsulation of energy efficient, clustering algorithm and spectrum sensing for cognitive radio based internet of things networks. Journal of Electrical Systems, 20(5s), 2570-2578. https://doi.org/10.52783/jes.2696

[37] Shukla et al. "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment" (2019) doi: 10.1371/journal.pone.0224934

[38] Neelam et al. "Observation of Enhanced Network Performance in IoT Process Control and Data Sensing with RINA" (2021) doi: 10.24138/jcomss-2021-0027

[39] Turner et al. "The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment" (2021) doi: 10.2139/ssrn.3931040

[40] Sureani, N. B. N., Qurni, A. S. B. A., Azman, A. H. B., Othman, M. B., & Zahari, H. S. B. (2021). The adequacy of data protection laws in protecting personal data in malaysia. Malaysian Journal of Social Sciences and Humanities (MJSSH), 6(10), 488-495. https://doi.org/10.47405/mjssh.v6i10.1087

[41] Khatiwada, P., Yang, B., Lin, J., Mugurusi, G., & Underbekken, S. (2024). A reference design model to manage consent in data subjects-centered internet of things devices. IoT, 5(1), 100-122. https://doi.org/10.3390/iot5010006

[42] Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A., & Maynard, S. B. (2017). Towards responsive regulation of the internet of things: australian perspectives. Internet Policy Review, 6(1). https://doi.org/10.14763/2017.1.455

[43] Nagaraju et al. "IoT Implementation and Management for Smart Farming" (2019) doi: 10.35940/ijitee.j9545.0881019

[44] Liu et al. "Survey of Intelligent Agricultural IoT Based on 5G" (2023) doi: 10.3390/electronics12102336

[45] Vuran et al. "Internet of underground things: Sensing and communications on the field for precision agriculture" (2018) "doi: 10.1109/wf-iot.2018.8355096

[46] Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A survey on the role of iot in agriculture for the implementation of smartfarming.IEEE Access, 7, 156237-156271. https://doi.org/10.1109/access.2019.2949703

[47] Veloso, A. F. d. S., Silveira, J. D. F. d., Abreu, P. F. F., Silva, T. A. R. d., Neto, G. A. S., Rabêlo, R. A. L., … & Júnior, J. V. R. (2023). Multi-microgrid: advancing smart grids through hybrid iot architecture for efficient energy

management. Anais Estendidos Do XIII Simpósio Brasileiro De Engenharia De Sistemas Computacionais (SBESC Estendido 2023). https://doi.org/10.5753/sbesc_estendido.2023.235436

[48] Kaňuch, P. and Macko, D. (2019). E-hip: an energy-efficient openhip-based security in internet of things networks. Sensors, 19(22), 4921. https://doi.org/10.3390/s19224921

[49] Bhatia, V. K., Girdhar, A., & Khurmi, S. S. (2022). Gaussian functional shapes-based type-ii fuzzy membership- based cluster protocol for energy harvesting iot networks. International Journal of Communication Networks and Information Security (IJCNIS), 13(2). https://doi.org/10.17762/ijcnis.v13i2.4901

[50] Ansari, S., Ansari, A., & Nyamasvisva, T. E. (2024). 6g vision, iot technologies, challenges and emerging technology solutions—a survey. Journal of Independent Studies and Research Computing, 22(1). https://doi.org/10.31645/jisrc.24.22.1.5