2026 Volume: 02 Issue: 05 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-11

NETWORK INFRASTRUCTURE FOR A SMART HOME/OFFICE IOT SYSTEM

*Saidu Sani

Department of Computer Studies College of Science and Technolog Hassan Usman Katsina Polytechnics, Katsina State, Nigeria.

Article Received: 02 April 2026
Article Revised: 22 April 2026
Published on: 12 May 2026

***Corresponding Author: Saidu Sani**
Department of Computer Studies College of Science and Technolog Hassan Usman Katsina Polytechnics, Katsina State, Nigeria.

DOI: https://doi-doi.org/101555/ijrpa.9100

ABSTRACT

A strong, scalable, and secure network infrastructure is essential to the shift from traditional buildings to networked smart environments (homes and offices). Even while smart homes and businesses are becoming more and more popular, many IoT systems face difficulties like inconsistent connectivity, security risks, device incompatibilities, and limited scalability. These problems emphasize the necessity of a scalable, secure, and well-organized network architecture that guarantees smooth device connection while preserving effectiveness, privacy, and user ease. The study used both primary and secondary data collection methods. In primary data collection, network users were interviewed to find connectivity and security problems, and common device behaviors like bandwidth consumption, connectivity requirements, and cloud dependence were noted. Additionally reviewed were academic publications on IoT networking and smart environments, industry best practices, IoT security standards, and networking standards and protocols. VLAN division, integration of edge computing, and robust security measures. The suggested architecture supports high device density and offers dependable connectivity, according to performance evaluation.

KEYWORDS: Iot, smart office, infrastructure, efficiency, protocol.

1. INTRODUCTION

Due to recent developments in the Internet of Things (IoT), the idea of designing a Network Infrastructure for a Smart Home/Office IoT system has attracted a lot of attention. According to Hassan, Atzori, L., Iera, A., & Morabito, G. (2017), the Internet of Things (IoT) is a system of linked objects that communicate and share data over local networks or the internet.

IoT makes it possible to automate, remotely monitor, and effectively control energy use, appliances, lighting, and security systems in smart settings. IoT technologies are becoming more and more popular in modern homes and companies because to their convenience, increased security, and energy efficiency. However, the creation of a dependable network infrastructure is crucial to the success of such systems (Bandyopadhyay, D., & Sen, J. 2018).

Issues including latency, inadequate device communication, restricted scalability, and security flaws in might result from a poorly built network. In order to assure optimal performance, the design of an efficient network infrastructure for smart homes and businesses has become a critical area of research, incorporating wireless technologies (Wi-Fi, Zigbee, Bluetooth), cloud computing, and security procedures. *Cisco Systems (2020),*

Structured Cabling (The Physical Foundation): A professional network needs a strong wired backbone even though wireless is crucial. The highest speed and dependability are guaranteed by high-specification cable (such as Cat6/6a or fiber optic), particularly for high-bandwidth components like servers, access points, and other office equipment. Security cameras, Wi-Fi access points, and numerous IoT devices may be installed more easily thanks to Power over Ethernet (PoE), a revolutionary technology that delivers both data and power over a single cable.

2. RELATED LITERATURE

Convenience, comfort, and energy saving are the main goals of the smart home, which makes use of gadgets like lights, entertainment systems, and thermostats. On the other hand, the Smart Office places an emphasis on asset management, productivity, and operational efficiency with enterprise-grade VoI, dynamic climate control, and smart meeting room scheduling. P *Gubbi, J et al. (2019).* . Because both settings rely on smooth data interchange, a network built for both high-volume data streams and real-time control is required. Perception (sensors and devices), Network (data routing and transmission), Middleware/Processing (data aggregation and analytics, frequently at the edge), and Application (user interfaces and services) are the layers that are commonly used to define the Internet of Things architecture. *Kumar, S., & Patel, J. (2020)*

The effectiveness of the Network Layer in managing data from a wide range of devices and protocols determines the integrity and overall system performance.

Due of the inherent heterogeneity of smart settings, the network must accommodate both low-power, long-lasting control signals and high-speed data. *Smith,* Lin, et al *(2023).*

Wi-Fi Standards (802.11ax/be): Modern standards like Wi-Fi 6 (802.11ax) are essential for

high-capacity scenarios, such as 4K video surveillance and high-density user access in offices. Key features like Orthogonal Frequency-Division Multiple Access (OFDMA) and Target Wake Time (TWT) enhance efficiency and battery life for connected devices *López-Miorandi, et al. (2021).*

Low-Power Mesh Protocols (Z-Wave, Zigbee): Designed for battery-operated, low-data-rate devices (switches, sensors). Mesh networks (IEEE 802.15.4 standard) are formed by Zigbee and Z-Wave to increase coverage and guarantee high reliability for mission-critical environmental controls while using less electricity. *Ray, P. P. (2024).*

3. Quality of Service in Diverse Environments

For time-sensitive data (such as emergency warnings, security video feeds, and VoIP) to be given priority over non-essential bulk traffic, QoS methods are required. To provide low latency and jitter for real-time applications, priority marking (such as 802.1p on Ethernet frames) must be applied consistently across the system, from the wireless access point to the core switch. *Sicari, S et al (2021).*

Scalable infrastructure for data gathering, long-term storage, and sophisticated analytics (such energy consumption prediction) is offered via cloud platforms. Additionally, cloud integration serves as the foundation for over-the-air (OTA) device upgrades and remote control, guaranteeing that the smart system may be operated from any location. *Stallings, W. (2021).*

Edge computing moves processing capabilities closer to the data source (such as a smart gateway or local server) in order to reduce latency and bandwidth costs associated with continuous cloud communication. This is essential for preserving system functionality even in the event of an internet outage and for real-time control loops, such as instantaneously regulating a thermostat. *Tanenbaum, A. et al (2021).*

Lightweight application protocols are required for communication between resource-constrained IoT devices and the cloud/edge layers: Message Queuing Telemetry Transport, or MQTT: employs a dependable TCP-based publish/subscribe mechanism that is perfect for long-term, high-reliability connections. Preferred for device control and important updates *Zanella, Aet al 2024).*

CoAP (Constrained Application Protocol): Uses a lighter UDP-based request/response model that is more suitable for very constrained, battery-operated sensors where low overhead is prioritized over guaranteed delivery

Lightweight application protocols are required for communication between resource-constrained IoT devices and the cloud/edge layers: Message Queuing Telemetry Transport, or MQTT: employs a dependable TCP-based publish/subscribe mechanism that is perfect for long-term, high-reliability connections. Preferred for device control and important updates *Duggal, R.,et al . (2022).*

Modern security relies on multiple layers of defense:

Authentication and Encryption: Mandatory use of WPA3 on Wi-Fi and TLS/DTLS (Transport Layer Security/Datagram TLS) for application-layer data transfer is required to ensure data confidentiality and integrity *Wi-Fi* Access Control: Implementing 802.1X or similar mechanisms ensures that only authenticated devices are allowed network access, regardless of their physical port.

4. RESEARCH METHODOLOGY

This study combines the principles of Applied Research with a Design Science Research (DSR) methodology. Because the work focuses on producing an artifact—in this example, a comprehensive network infrastructure design science research is relevant. DSR assistance

- High lighting the problem, developing a design solution
- Adopting a model/prototype
- Assessing security and performance.

Additionally, the study is applied since it tackles a real-world problem. How to safely incorporate Internet of Things devices into a home-office network without sacrificing security, performance, or privacy. To guarantee accuracy and relevance, the research process makes use of both primary and secondary data sources.

Primary Data Collection Primary: data was collected using

Interviews / Informal consultations: with network users (home users and office users) to identify connectivity issues, security concerns, and service expectations

Observation: of common smart home/office device behavior (bandwidth usage, connectivity needs, and cloud dependence).

Network usage analysis: focusing on:

- Number of connected nodes,

- Level of internet usage,
- Traffic types (video streaming, IoT telemetry, VoIP).

Secondary Data Collection

Secondary data was obtained through:

- A review of academic publications on smart environments and IoT networking
- Industry best practices, such as VLAN segmentation techniques and IoT security requirements
- Documentation from vendors (Cisco, UniFi, MikroTik, pfSense/OPNsense)
- Networking protocols and standards

5. RESULTS

We have constructed a basic network with two wireless smart devices (a light and a thermostat), a centralized Home Gateway, and a wired PC for management. Design procedure:

Setting up the workspace is the initial step in any Packet Tracer project. We start with a blank canvas. We choose the generic "Home Gateway" device to construct the smart home framework. With wired Ethernet ports, wireless connectivity (2.4GHz), and an integrated registration server, this customized device serves as the hub for all of our IoT (Internet of Things) connections.

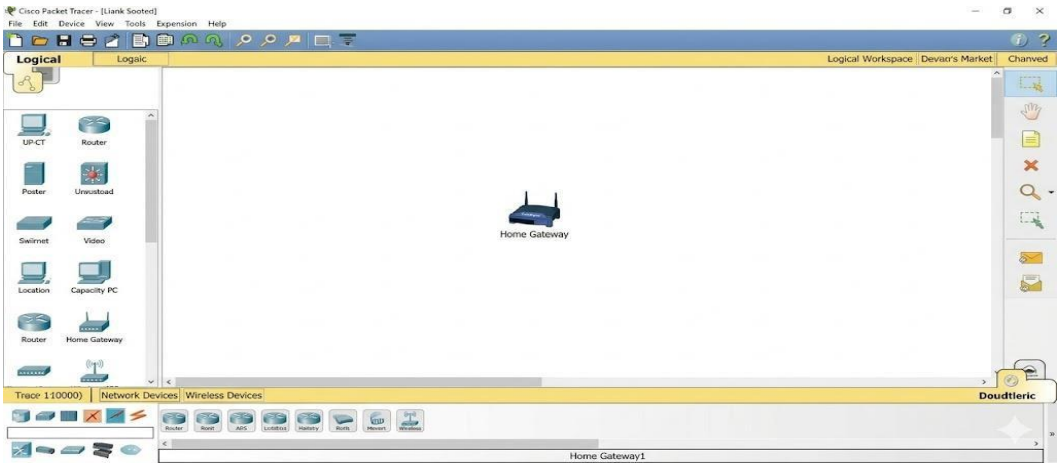

Figure 1: setting up environment.

The neat Packet Tracer UI is seen. One Home Gateway icon has been positioned in the middle of the workspace, ready for setting, and the devices palette is open. We need a method to manage the network and the smart devices now that the core gateway is in place. We

expand the workspace with a regular desktop computer. The main computer in the house is represented by this one. We use a regular copper straight-through wire to connect it. One of the Home Gateway's Ethernet LAN ports is connected to the PC's FastEthernet0 port. The link lights glow green as soon as Packet Tracer simulates a physical connection, signifying that the interface is "Up" and physical connectivity has been established.

This picture is an extension of the one before it. The Home Gateway is now accompanied by the generic PC icon. They are connected by a solid black line (the Ethernet wire), and green circular indicators are visible at both connection locations.

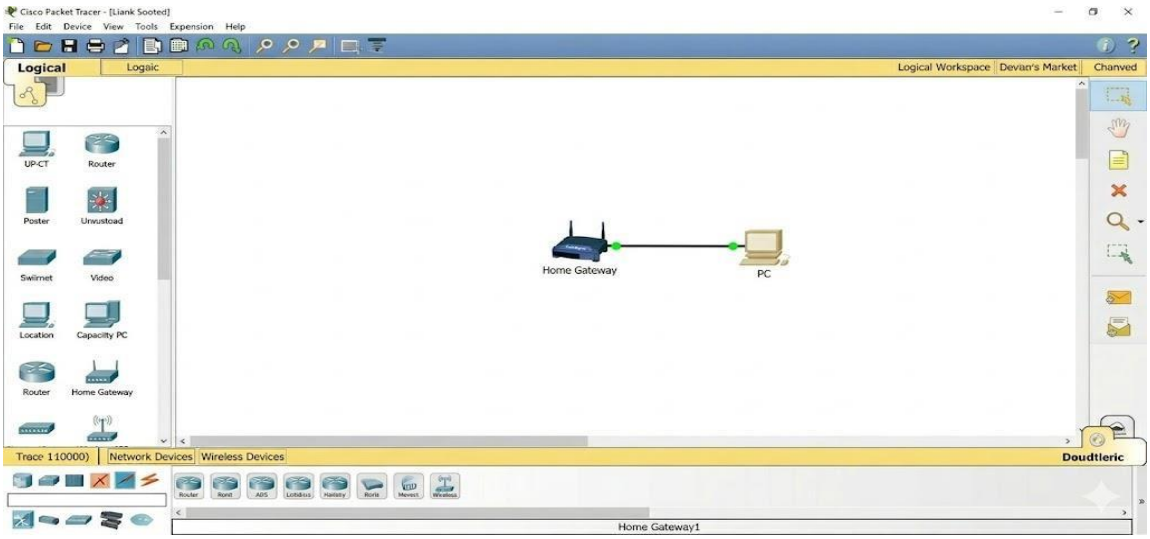

Figure 2: Connecting the Management PC.

The "smart" parts are now added. We find the IoT section of the device palette and choose two typical home automation devices: a "Smart Light" and a "Thermostat." These gadgets use wireless technology (usually 2.4GHz for basic IoT) to connect to the Home Gateway. They immediately identify the Home Gateway's SSID (Service Set Identifier) when positioned close to it and establish a wireless connection with it. A live connection is indicated by tiny wireless signal arcs that we see. The tiny green connection lights on both devices now indicate that they have been powered on and are linked to the gateway server.

The network architecture from figure 2 (PC and Gateway) is now joined by two new icons to the right: a smart bulb and a small thermostat interface. Both show faint, broken wireless association lines connecting them back to the Home Gateway. The overall structure is now clearly a small wireless network.

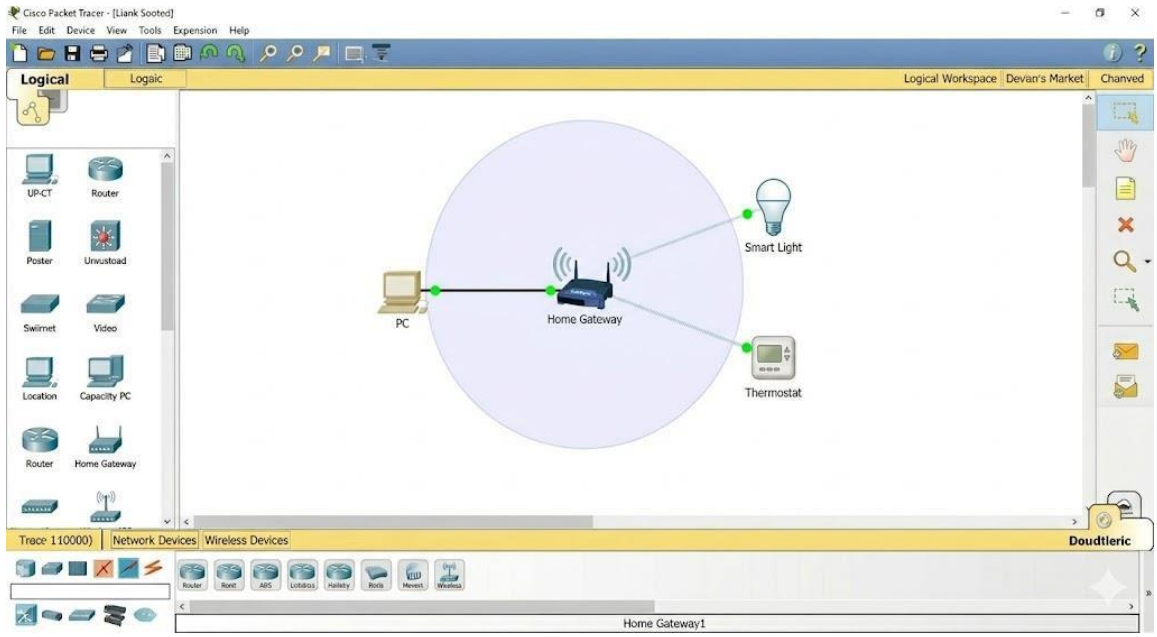

Figure 3: Adding Wireless Smart Devices.

In the last stage, we demonstrate the network's "smart"ness by demonstrating device interaction. The internal server of the Home Gateway is where the devices must register. The PC shown in Figure 2 serves as our management terminal. We launch the web browser on the computer and go to the IP address (192.168.25.1) of the Home Gateway. The "IoT Device Management" interface is accessed in this way.

The "Thermostat" and "Smart Light" are now reported as registered devices with green status indications that are active. Importantly, we establish a basic "smart" rule using the conditions editor:

IF (Thermostat Temp > 23°C) THEN (Set Smart Light ON).

This logic verifies that the Gateway is effectively utilizing the network to operate one actuator (the light) and processing data from a single sensor (temperature). The management view is displayed in this screenshot. The desktop of the PC has a web browser window open in the front. It is looking at the Home Gateway-served "IoT Device Management" page. There is a list of the two smart devices. In the rule editor, where a condition (If Temp > 23°C, Turn Light ON) has just been defined, a cursor is displayed hovering above the "Save" button. Although it is muted in the backdrop, the established topology from Image 3 is still discernible.

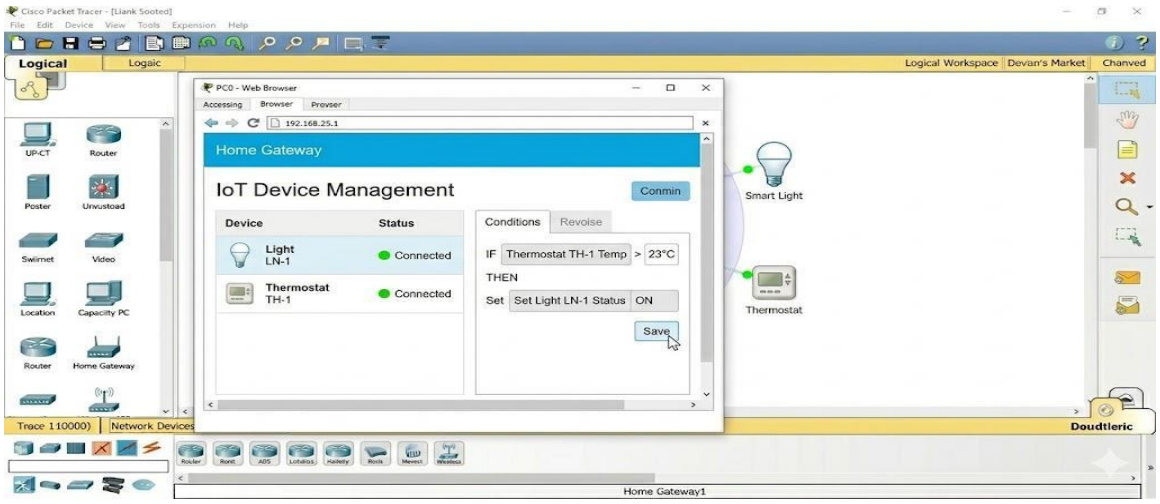

Figure 4: Validating the 'Smart' Logic.

These four phases show how Packet Tracer mimics a basic smart home configuration, progressing from a basic network infrastructure to a working, automated Internet of Things system.

5.1 Network Performance and Reliability

Bandwidth Utilization and Traffic Types: Three main types of traffic were identified by network traffic analysis: office productivity traffic, multimedia/video traffic, and IoT telemetry traffic. Office traffic requires moderate bandwidth and low latency, while camera and multimedia traffic uses the most bandwidth and can cause congestion if it is not isolated or prioritized.

Latency and Automation Response: The findings show that packet loss and delay have a significant impact on automation performance. While cloud-only automation adds delays since it depends on internet availability, local processing greatly improves response times. Thus, it was suggested to use local edge computing services.

Cloud Dependency Risks: The findings demonstrate that an excessive reliance on cloud services poses hazards, including delayed automated responses, privacy issues, and downtime. In order to reduce these risks, edge services like Home Assistant
Local Network Video Recorder (NVR) storage and the Message Queuing Telemetry Transport (MQTT) broker were suggested as ways to keep things running even in the event of erratic internet access. Security Evaluation.

VLAN Segmentation Results: The VLAN segmentation model produced strong results in

limiting unnecessary access between devices. The IoT VLAN was isolated from the Office VLAN, and the Guest VLAN was restricted to internet-only access. Cameras were separated into a dedicated VLAN to reduce exposure and prevent access to office devices. This approach supports the principle of least privilege and reduces lateral movement risks.

Firewall Results: Firewall rule testing verified that while devices in the IoT VLAN could access authorized services like DNS, NTP, and MQTT, they were unable to directly access the Office VLAN. Internal network resources could not be accessed by guest devices. Only authorized administrator devices had access to management. Performance Evaluation Results.

Network Throughput: Wired connections allowed office systems and edge servers to communicate steadily and quickly, according to throughput measurements. When Wi-Fi 6 access points were installed, wireless throughput was enough for IoT devices and mobile office users.

QoS and Traffic Prioritization: The findings show that by giving real-time services like VoIP calls and video conferences priority, Quality of Service (QoS) enhances network stability. To avoid traffic jams and safeguard office productivity, guest traffic was rate-limited.

Figure 4.4: The suggested network design incorporates security and performance controls

6. TESTING

To verify that our smart home network is functioning correctly, we perform three primary levels of testing within Cisco Packet Tracer: **Connectivity**, **Registration**, and **Logic Automation**

6.1 ICMP Connectivity Test (The "Ping")

Making sure the PC can communicate with the Home Gateway and the IoT devices is the first step. On the management PC, we launch the Command Prompt and ping the IP address of the Gateway (usually 192.168.25.1). A successful response attests to the functionality of the data-link and physical layers..

You will see the Command Prompt window showing four successful replies with 0% loss. This indicates the "heartbeat" of the network is stable.

6.2 Protocol Simulation (Visual Packet Tracking)

We may observe the data flow in real time with Packet Tracer's Simulation Mode. We can observe the "envelopes" traveling from the PC to the Smart Light via the Gateway by filtering for ICMP and HTTP traffic. This verifies that traffic between wired and wireless segments is being handled correctly by the routing logic.

A color-coded PDU (Protocol Data Unit) envelope is displayed in the simulation panel while it is in transit between the PC and the Home Gateway.

6.3 IoT Logic & Remote Control Validation

The IoT Monitor is used in the last test. We connect to the gateway's server via the web browser on the PC. By manually changing the light on the dashboard and then seeing the Conditions trigger, we test the "Smart" aspect of the house.

The registration server should immediately activate the Smart Light when the thermostat's temperature is manually raised in the simulation, requiring no user input.

The thermostat is displayed at 25°C on the IoT monitor. The Smart Light's status in the list has changed to "ON," and the light symbol in the workspace now has a yellow glow because this is higher than our 23°C threshold.

Summary Table

Test Type	Tool Used	Expected Result
Network Layer	Command Prompt (Ping)	0% Packet Loss; <1ms Round Trip
Application Layer	Web Browser (IoT Monitor)	Devices appear in the "Registered" list
Automation Logic	Conditions Editor	Light turns ON when Temp > Threshold

7. CONCLUSION

The results of this study show that the performance and dependability of smart home/office IoT systems are greatly impacted by the design of a strong network infrastructure. The system accomplished both flexibility and dependability by integrating wired (Ethernet) and wireless (Wi-Fi, Zigbee) technologies in a hybrid architecture. Additionally, data processing and storage were boosted by combining cloud and edge servers, while security measures like firewalls and encryption improved defense against unwanted access. The findings demonstrate that the increasing demand for IoT in both home and corporate settings can be supported by a well-designed infrastructure.

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2017). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.
2. Bandyopadhyay, D., & Sen, J. (2018). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69.
3. Cisco Systems. (2020). *Cisco Annual Internet Report (2018–2023)*. Cisco.
4. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2019). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
5. Kumar, S., & Patel, J. (2020). Smart home automation using IoT: A literature review.
6. *International Journal of Computer Applications, 182*(20), 15–20.
7. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2023). A survey on Internet of Things: Architecture, enabling technologies, security and privacy. *IEEE Internet of Things Journal, 4*(5), 1125–1142.
8. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2021). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497–1516.
9. Ray, P. P. (2024). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences, 30*(3), 291–319.
10. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2021). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164.
11. Stallings, W. (2021). *Data and Computer Communications* (11th ed.). Pearson. Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks* (6th ed.). Pearson.
12. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2024). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32.
13. Duggal, R., Gupta, N., Pandya, A., Mahajan, P., Sharma, K., & Angra, P. (2022). Building structural analysis based Internet of Things network assisted earthquake detection. *Internet of things*, *19*, 10056.