Journal of Modern Engineering and Technology Vol: 1, No 1, 2025, Page: 1-15

Review Article

A Review of TCP/IP Applications: From Web Services to the Internet of Things (IoT)

Firas Basim Al Hilali*

Naif Arab University for Security Sciences, Riyadh 14812, Saudi Arabia
Corresponding Email: 202500758@student.nauss.edu.sa

Received: 17 August 2025 **Revised:** 27 September 2025 **Accepted:** 24 October 2025

Abstract: This review article discusses the evolution of TCP/IP applications from conventional web services to modern IoT ecosystems. This study examines how classic protocols like HTTP, FTP, and SMTP influenced the web for communication and how lightweight protocols like MQTT, CoAP, and 6LoWPAN emerged to support the restrictions of IoT devices. The two domains have been compared in terms of communication paradigms, security requirements, scalability concerns, and service quality. Furthermore, protocol enhancements have been highlighted in this study, such as the use of IPv6, QUIC, DTLS, and the integration with edge computing. It points out issues that heterogeneous networks are facing nowadays, such as latency, energy efficiency, device authentication, and congestion control. Finally, it discusses future directions for researchers and practitioners on safe TCP/IP extensions, AI-driven network optimization, and 5G-enabled IoT.

Keywords: TCP/IP, Web Services, IoT Communication, HTTP, IPv6, Network Security, REST API, IoT Protocols

1. INTRODUCTION

The TCP/IP suite is the basic communication architecture on which modern digital networks are implemented [1–3]. It enabled transparent data exchange among distributed systems and supported major applications, such as web services, email, file transfer, and cloud-based communication. It has now been significantly adapted to the demands of billions of devices in IoT scenarios that are characterized by low processing power, narrow bandwidth, and energy-related resource limitations. This, therefore, introduces a new era from the typical client-server web communication to heterogeneous, decentralized, and resource-aware IoT environments [4, 5].

In web-enabled applications, TCP/IP allows the usage of standardized protocols such as HTTP/HTTPS, SMTP, DNS, and RESTful services in order for communication over the internet to be dependable, secure, and scalable [6-8]. These applications depend on strong mechanisms at the transport layer, high bandwidth, and clearly defined security protocols such as SSL/TLS. In any case, the classic model of TCP/IP was not designed to handle special features of IoT traffic-frequent small data transmissions, intermittent connectivity, and constrained hardware. Consequently, the system of IoT has introduced lightweight communication protocols such as MQTT, CoAP, and 6LoWPAN. Operating within the TCP\IP framework, they nonetheless address some limitations of embedded devices [9, 10].

Even with these improvements, a variety of problems in TCP/IP applications in both web services and IoT ecosystems remain to be tackled. These include, among many others, latency, congestion control, device authentication, energy efficiency, and interoperability between heterogeneous networks. Man-in-the-middle attacks, data leaks, and other conventional web-related vulnerabilities have given way to IoT-specific security dangers, including device takeover, botnet development, and shoddy encryption. In this regard, academic developers and network engineers need to understand exactly how TCP/IP is implemented, optimized, and secured in both the online and IoT domains.

This essay examines TCP/IP's uses, ranging from traditional web services to Internet of Things communication methods. The following lists this work's principal contributions:

- Analyzing the evolution of TCP/IP from web-centric systems to IoT-based communication environments.
- Comparing the architectures, performances, and constraints of traditional web protocols with IoT-focused protocols: HTTP, FTP, SMTP, MQTT, CoAP, and 6LoWPAN.
- Identify security issues, performance limitations, and scalability challenges in both domains.

Embracing the latest trends that include IPv6, QUIC, 5G-enabled IoT, edge computing, and AI-driven network optimization.

The rest of the paper is organized as follows. Section 2 deals with related works, Section 3 show the basics of the TCP/IP protocol suite, while Section 4 addresses TCP/IP applications in web services. Section 5 delves into TCP/IP adaptations in IoT communications. Section 6 presents security challenges, Section 7 discusses performance and scalability issues, while Section 8 deals with emerging technologies and future directions. Section 9 concludes the paper.

2. RELATED WORK

TCP/IP protocol suite development and its utilization in web services and IoT contexts have been a subject of interest in much research works. One of the early prominent surveys on the Internet of Things (IoT) was contributed by Atzori et al. [11], which insisted on underlining TCP/IP networking concepts as the basis for IoT communications and highlighted that the main challenges were addressing, scalability, and interoperability. Along these lines, Gubbi et al. [12] noted the necessity of using RESTful web services along with lightweight protocols at the device level when discussing cloud computing and integration with IoT over TCP/IP networks.

Fielding and Taylor presented in [13] how HTTP and REST architectures are layered on top of TCP/IP in order to support scalable, stateless web services. Finally, Berners-Lee et al. formalized in [14] the base of modern Web communication, HTTP/1.1, while Dierks and Rescorla standardized in [15] TLS due to the increasing security concerns, enabling secure HTTP (HTTPS) communication over TCP/IP networks.

As the IoT technologies evolved, enhanced application layer protocols were proposed. MQTT represents a lightweight publish-subscribe protocol over TCP/IP that was proposed by Banks and Gupta [16] for low-bandwidth Internet of Things devices. To reduce latency and complexity in such resource-constrained networks, Bormann et al. [17] developed the constrained Application Protocol, known as CoAP, utilizing UDP rather than TCP. In addition, Kushalnagar et al. [18] developed 6LoWPAN, which is designed to carry IPv6 packets efficiently over low-power wireless networks.

Performance, scalability, and security-related issues of TCP/IP-based IoT systems have been addressed in recent research. Work by Al-Fuqaha et al. examined various standards of IoT communication and analyzed TCP limitations in the presence of high latency in wireless links. Sicari et al. described major security risks in IoT networks, including device hijacking, denial of service, and weak encryption. Other relatively recent research topics cover QUIC, edge computing, and AI-driven TCP/IP network optimization for enhancing network throughput, reducing congestion, and enabling smart routing of data.

In summary, while there is literature that has examined TCP/IP in either web systems or separately in IoT, only a few works comprehensively compare the two domains. This paper bridges this gap by reviewing the applications of TCP/IP from traditional web services to modern IoT communication models through analysis of protocols and performance constraints with emerging enhancements in a unified manner.

3. FUNDAMENTALS OF THE TCP/IP PROTOCOL SUITE

The fundamental networking architecture used to link devices via the internet and private networks is called TCP/IP (Transmission Control Protocol/Internet Protocol). By standardizing data formatting, addressing, transmission, routing, and reception, it establishes a layered communication framework that guarantees compatibility across disparate systems [21, 22]. The four-layer TCP/IP architecture is depicted in Figure 1, showing how data moves from web or Internet of Things apps to physical network.

3.1 TCP/IP Layered Architecture

Each of the four functional layers that make up TCP/IP is in charge of particular communication tasks [22]:

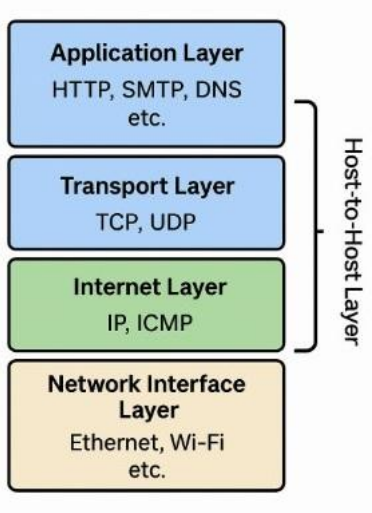

Figure 1. TCP/IP Architecture Model

Table 1. Four functional layers

Layer	Function	Example Protocols
Application Layer	Provides network services to end-users and applications	HTTP, HTTPS, FTP, SMTP, DNS, MQTT, CoAP
Transport Layer	Ensures reliable or fast data delivery between hosts	TCP, UDP
Internet Layer	Handles logical addressing and routing of packets	IP (IPv4, IPv6), ICMP, ARP
Network Access Layer	Manages physical transmission over network media	Ethernet, Wi-Fi, PPP, MAC

3.2 Key Protocols in the TCP/IP Suite [22]

- TCP (Transmission Control Protocol: Ensures reliable, connection-oriented delivery of data with features such as error detection, retransmission, and flow control.
- UDP (User Datagram Protocol): A connectionless protocol that allows for quicker transmission, without error recovery; utilized in streaming, gaming, and DNS requests.
- IP (Internet Protocol): Performs packet routing and addressing. IPv6 is a fundamental requirement for IoT because of the huge address space.
- DNS (Domain Name System): Translates user-friendly domain names, such as google.com, into IP addresses.
- HTTP/HTTPS: Web communication protocols widely used in web browsers and also by RESTful API services.

3.3 TCP/IP in Web Services vs IoT Systems

Both IoT applications and traditional web services rely on TCP/IP, but they use multiple protocols based on device capabilities, data requirements, and system limitations [23, 24].

Table 2. Comparison of TCP/IP-Based Protocols in Web vs IoT Applications

Feature	Web Services (HTTP-Based)	IoT Systems (MQTT/CoAP-Based)
Primary Protocols	HTTP, HTTPS, FTP, SMTP, WebSocket	MQTT, CoAP, 6LoWPAN, AMQP
Transport Layer	TCP (reliable, heavy)	MQTT → TCP, CoAP → UDP
Communication Model	Request–response (client/server)	Publish–subscribe (MQTT), Request–response (CoAP)
Security	SSL/TLS, HTTPS, OAuth	DTLS (for CoAP), Lightweight encryption, TLS for MQTT
Data Size	Large (HTML, XML, JSON)	Small sensor data (bytes to kilobytes)
Device Resources	PCs, servers (high power)	Microcontrollers, sensors (low power)
Network Type	High bandwidth, stable connection	Low bandwidth, intermittent, wireless
Addressing	IPv4/IPv6	IPv6, 6LoWPAN (IPv6 over Low-Power Networks)
Latency Tolerance	Medium	Low latency (real-time IoT control)
Energy Consumption	Not critical	Must be extremely low

3.4 Adaptation of TCP/IP for IoT Systems

The very limited and wireless nature of IoT contexts was not intended for the TCP/IP protocol, which was first created for computers and dependable networks. Because IoT devices frequently run on low-energy sources and have limited memory and processing power, conventional protocols like HTTP are too cumbersome and ineffective. IoT networks also have low bandwidth, sporadic connectivity, and the need to send small data packets often. If traditional TCP/IP protocols are employed without modification, these factors increase latency and energy consumption.

These issues were addressed by the introduction of lightweight protocols within the TCP/IP framework. CoAP works over UDP to provide a lightweight alternative for HTTP suitable for resource-constrained devices, whereas MQTT enables efficient, low-bandwidth, and minimal-processing-cost publish-subscribe models over TCP. These adaptations make IoT systems maintain compatibility with TCP/IP while keeping power consumption low, latency as low as possible, and providing better scalability [25].

4. TCP/IP IN WEB SERVICES

For dependable communication between clients and servers over the internet, web services mostly rely on the TCP/IP protocol stack. Web-based applications, including websites, APIs, email systems, and cloud platforms, rely on TCP/IP for end-to-end connectivity, data integrity, routing, addressing, and session management [26].

4.1 Role of TCP/IP in Web Communication

In traditional web configurations, a client (browser or application) sends a request to a server through the HTTP/HTTPS protocol over TCP. TCP ensures that data is delivered reliably and in the correct order through three-way handshakes, acknowledgments, retransmission, flow management, and congestion control. Due to this, it can be used for applications where completeness and accuracy of the data are crucial. Some widely used web protocols based on TCP/IP are listed in Table 3 [27].

Table 3. Common TCP/IP-Based Web Protocols

Protocol	Layer (TCP/IP Model)	Function
HTTP / HTTPS	Application	Transfers web pages and API data; HTTPS adds SSL/TLS security
FTP	Application	Used for file upload and download
SMTP / IMAP / POP3	Application	Email sending and retrieval
DNS	Application	Resolves domain names to IP addresses
TCP	Transport	Provides reliable, connection-oriented data delivery
IP (IPv4/IPv6)	Internet	Handles routing and addressing of data packets

The most popular of them for web services is HTTP/HTTPS. By guaranteeing confidentiality, integrity, and authentication, HTTPS incorporates SSL/TLS encryption to secure communication.

4.2 Web Service Architectures Supported by TCP/IP

There are two primary forms of web services built on TCP/IP:

- SOAP-Based Web Services (Simple Object Access Protocol): Use XML messaging over HTTP or SMTP, suitable for highly structured enterprise applications.
- RESTful Web Services (Representational State Transfer): Use HTTP methods (GET, POST, PUT, DELETE) and typically exchange data in JSON or XML, making them lightweight and ideal for web APIs.

4.3 Security in TCP/IP-Based Web Services

Because of risks such data eavesdropping, spoofing, and session hijacking, security is essential in online communication [28]. Use of TCP/IP web services:

- HTTPS (HTTP over SSL/TLS) for encryption
- Digital certificates for authentication
- OAuth / JWT for user and API access control
- Firewalls and Intrusion Detection Systems (IDS) for network protection
- Security is mostly provided at the application layer via HTTPS and encryption protocols, even if TCP/IP offers fundamental integrity and routing.

4.4 Limitations in Web Service Environments

Despite its reliability in web systems, the following are challenges posed to TCP/IP:

- High communication overhead due to TCP handshakes and HTTP headers
- Latency in real-time applications such as video streaming or gaming
- Scalability issues under heavy traffic (DDoS attacks)
- Not optimized for low-power or limited-resource devices, unlike IoT protocols such as MQTT

5. TCP/IP IN IOT COMMUNICATION MODELS

Coupled with the use of TCP/IP as its fundamental networking architecture, IoT jointly integrates billions of connected sensors, actuators, and embedded devices into the global internet. In contrast to typical web systems, the IoT devices are bound by stringent limitations, including little memory, low computing power, small data packet sizes, low bandwidth, and battery-powered operations. This has therefore brought about the development of lightweight communication protocols that adjust TCP/IP for resource-constrained contexts due to the straight usage of conventional TCP/IP protocols such as HTTP, which is very wasteful for IoT [27, 28].

IoT communication typically consists of short, intermittent data transfers, often in real time, where reliability and energy efficiency are more important than high data throughput. Protocols such as CoAP (Constrained Application Protocol) and MQTT (Message Queuing Telemetry Transport) were devised in the TCP/IP framework to satisfy this [29, 30]. Operating over TCP, MQTT uses a publish-subscribe model through a central broker to provide reliable message delivery using various QoS levels with minimal bandwidth consumption. A publish-subscribe communication architecture is used by MQTT, a lightweight messaging protocol that operates over TCP. Devices (publishers) send messages to a broker, and only subscribers to that subject receive the data. In terms of time, place, and execution, this separates the sender and recipient. Figure 2 illustrates the MQTT publish–subscribe architecture.

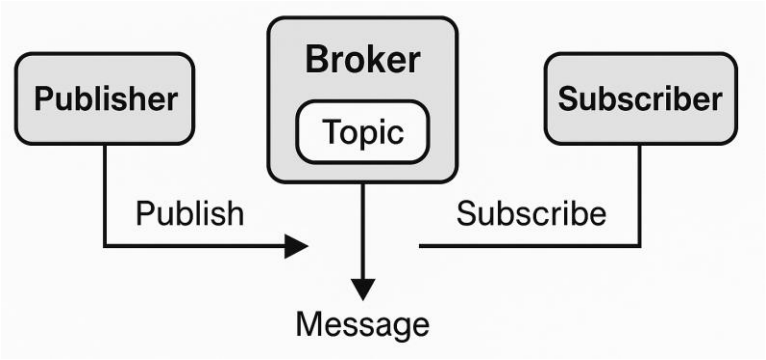

Figure 2. MQTT Publish–Subscribe Communication Model

CoAP, on the other hand, runs over UDP and follows a simplified request–response model similar to HTTP but with a greatly reduced header and lower latency, optimal for low-power wireless networks, figure 3. CoAP Request–Response Communication Model. In addition,

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) supports IPv6 packet compression and transmission over IEEE 802.15.4 networks, allowing end-to-end addressing while minimizing overhead. Using the TCP/IP architecture, figure 4 depicts the end-to-end data flow in an IoT context, demonstrating how IoT devices connect to the cloud over the internet via a local gateway.

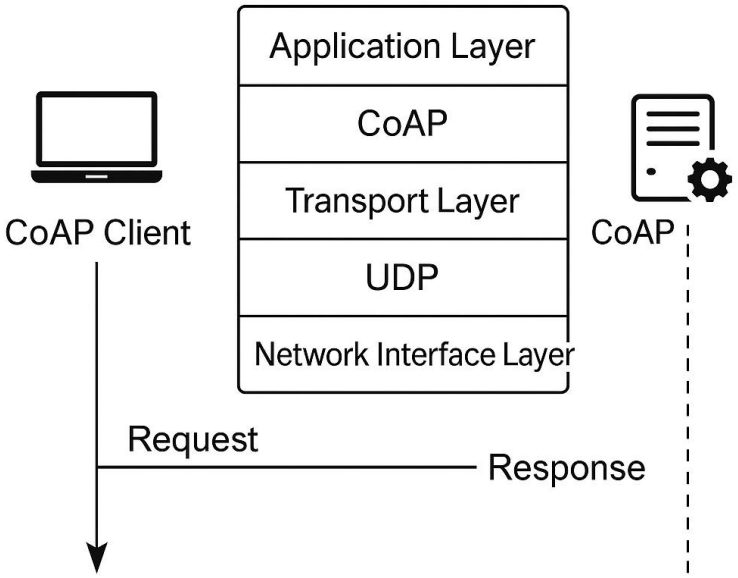

Figure 3. CoAP Request–Response communication model

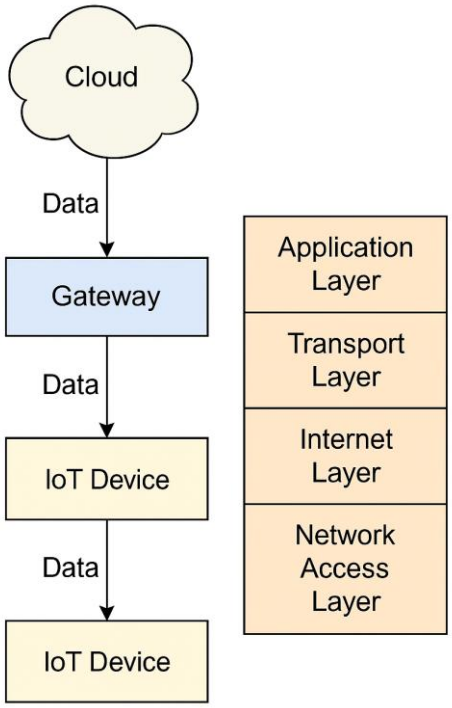

Figure 4. End-to-End IoT communication over TCP/IP

IPv6 adoption is essential for the Internet of Things, given that IPv4 addresses are running out and billions of devices need to be uniquely identified. Security in IoT using TCP/IP remains difficult because many devices are unable to handle complex encryption techniques. Lightweight security techniques employ TLS for MQTT and DTLS for CoAP, aimed at guaranteeing confidentiality, integrity, and authentication in order to lessen this. Even with these modifications, TCP/IP in the Internet of Things still faces issues such as packet loss in erratic wireless networks, delay in TCP handshakes, energy consumption during retransmissions, and scalability issues in large deployments [31]. Figure 5 illustrates how IoT communication uses lightweight, asynchronous mechanisms like MQTT (publish–subscribe) and CoAP (request–response) that operate over TCP or UDP for efficiency in limited environments, whereas traditional web communication uses a client–server model using HTTP/HTTPS over TCP.

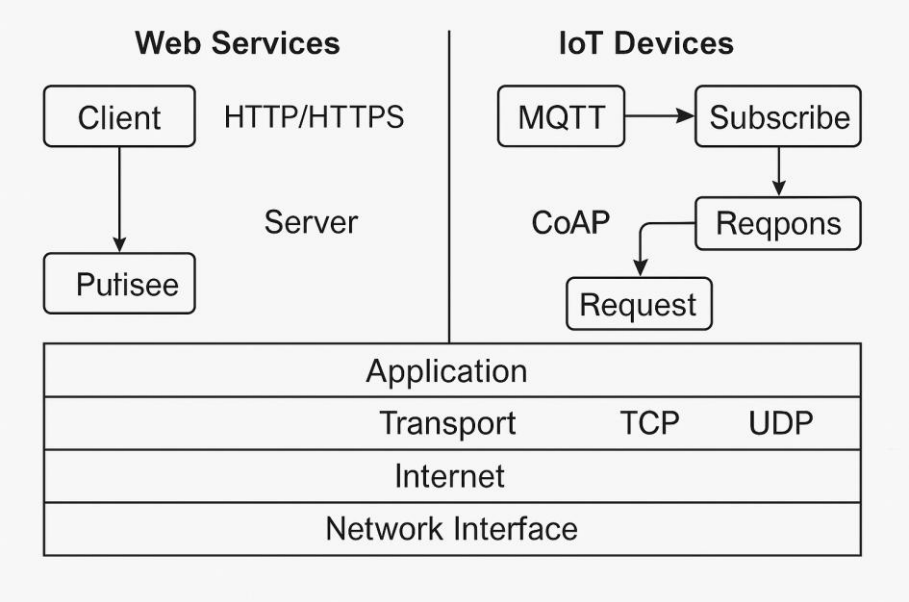

Figure 5. Comparison of Web Services and IoT Communication over TCP/IP Architecture

Table 4. Comparison of TCP/IP Protocols in Web Services vs IoT Applications

Feature	Web Services (HTTP/HTTPS)	IoT Communication (MQTT / CoAP / 6LoWPAN)
Communication Model	Client–Server (Request/Response)	MQTT: Publish–Subscribe / CoAP: Request–Response
Transport Layer	TCP	MQTT → TCP / CoAP → UDP
Data Size	Large (HTML, JSON, XML)	Very small sensor data
Device Type	PCs, Servers, Smartphones	Low-power sensors, microcontrollers
Network Type	Stable, high bandwidth	Low-power, wireless, unstable links
Energy Consumption	Not critical	Must be very low
Addressing	IPv4 and IPv6	IPv6 and 6LoWPAN
Security Mechanism	HTTPS (TLS/SSL), OAuth	TLS for MQTT, DTLS for CoAP
Reliability	High (guaranteed delivery)	Selective: MQTT QoS, CoAP Confirmable
Use Case	Web browsing, REST APIs, email	Smart homes, industrial IoT, sensor monitoring

6. SECURITY CHALLENGES IN TCP/IP FOR WEB AND IOT APPLICATIONS

A big challenge for both the current IoT applications and traditional web services, the security of TCP/IP-based communication is one of the key factors. In fact, TCP/IP was not necessarily built around robust security, but rather to provide basic data transport capabilities. Ensuring confidentiality, integrity, availability, and authentication of data in Web of Things and IoT systems, additional security protocols like SSL/TLS or DTLS, or even encryption frameworks, have to be used. However, due to differences in computational power, in connectivity, and with respect to specific deployment situations, security concerns within traditional online scenarios and IoT are clearly different [32].

Man-in-the-middle attacks, SQL injection, session hijacking, DNS spoofing, phishing, and cross-site scripting are believed to be some of the most common security risks in online services. Today, these issues have been resolved with robust authentication methods such as OAuth or JWT, protection provided by firewalls, intrusion detection systems, and HTTPS (HTTP over SSL/TLS). These systems can afford encryption, certificates, and security monitoring tools without significant performance constraints as they work under conditions of high bandwidth and sufficient processing resources. Although TCP guarantees dependable transmission, higher-layer protocols should be used to encrypt communications.

In contrast, IoT systems have to address more complex and important issues: low computing power of devices, risks in wireless communication, and physical accessibility of sensors and actuators. These adversaries can exploit a weak or default password of the device, unencrypted communication, or even firmware vulnerabilities, or physically tamper with the device. Threats in IoT devices include device spoofing, botnet formation, such as the Mirai attack, denial of service on constrained networks, data tampering, and unauthorized access. Encryption via TLS and DTLS is supported by MQTT and CoAP. However, due to their heavy cryptographic operations, many low-cost IoT devices cannot perform them efficiently. Moreover, large-scale IoT networks do not use centralized security management and normally operate without attended environments [33].

Table 5. Security Challenges in Web vs IoT TCP/IP Applications

Aspect	Web Services	IoT Applications
Main Threats	MITM, SQL Injection, Session Hijacking, DNS Spoofing	Device Hijacking, Botnets, Firmware Attacks, DoS, Data Tampering
Security Protocols	HTTPS (TLS/SSL), OAuth, JWT	TLS (for MQTT), DTLS (for CoAP), Lightweight Encryption
Device Capabilities	High computing power, storage, constant power supply	Low CPU, limited memory, battery-powered devices
Network Environment	Stable, high-bandwidth wired/wireless networks	Low-power, lossy, and intermittent wireless networks
Encryption Overhead	Acceptable due to strong hardware	May cause latency, energy drain, or failure
Physical Access Risk	Low (servers in secure data centers)	High (devices deployed in open/public spaces)
Attack Detection	IDS/IPS, firewalls, SIEM tools	Minimal device-level monitoring, decentralized security
Addressing	Mostly IPv4/IPv6 secured networks	Often IPv6/6LoWPAN, vulnerable local networks

7. PERFORMANCE AND SCALABILITY CHALLENGES IN TCP/IP FOR WEB AND IOT APPLICATIONS

Web services and IoT networks rely on the performance and scalability of TCP/IP-based communication systems. However, there is a big difference in requirements and challenges between these two domains. In conventional web environment settings, TCP/IP is optimized for high-bandwidth stable networks where performance bottlenecks are created by network congestion, latency, server overload, and large-scale user access. Effectively, TCP is applied at web applications for flow management and congestion control through reliable delivery of data like web pages, APIs, emails, and multimedia. Although it provides very high dependability, retransmission, acknowledgement delays, and connection establishment-three-way handshake-all contribute to latency. With increased user demand, various techniques including load balancing, CDNs, server clustering, and cloud architecture can all achieve scalability.

However, IoT networks face performance issues owing to resource constraints, frequent disconnections, energy constraints, and handling a large number of devices sending small-sized data packets. Because of its overhead, retransmission techniques, and handshaking procedures, TCP is not suitable for the IoT. Lightweight protocols-MQTT over TCP and CoAP over UDP-are preferred because they reduce latency and battery consumption. Addressing, routing, and data aggregation issues make it challenging to scale IoT networks to millions of devices. Even with IPv6 and 6LoWPAN helping to increase addressability, congestion and packet conflicts may still occur in wireless communication during dense network installations. Another major performance challenge concerns QoS in both web and IoT systems. While web applications require high throughput and low latency for services such as video streaming, cloud computing, and e-commerce, IoT applications can bear low throughput but must have small packets delivered timely and efficiently, especially in critical fields like healthcare, smart grids, and industrial automation. Energy efficiency is also a very important aspect in IoT; therefore, repeated retransmissions and long TCP sessions also drain battery-operated devices. Moreover, IoT real-time systems can hardly be realized under the minimum delays typical of traditional TCP/IP mechanisms. Given the above challenges, several emerging technologies such as edge computing and fog networks, QUIC protocol integration, 5G, and AI-based congestion control are used either to replace or enhance classical TCP/IP functionality, thus making systems more responsive and scalable [35].

Table 6. Performance and Scalability: Web Services vs IoT Systems

Aspect	Web Services	IoT Applications
Data Transmission	Large files, web pages, multimedia	Small, periodic sensor data
Transport Protocol	Mostly TCP	MQTT (TCP), CoAP (UDP)
Latency Issues	Connection setup delay, congestion	Real-time delay sensitivity, wireless instability
Scalability	Solved using CDNs, cloud servers, load balancing	Millions of devices, address management (IPv6/6LoWPAN)
Energy Consumption	Not critical (servers, PCs)	Critical (battery-powered devices)
Network Type	High-speed, stable networks	Low-power, lossy, intermittent
Congestion Control	TCP congestion algorithms, buffering	Limited buffering, packet loss, collisions

QoS Requirements	High throughput, low latency for streaming and web access	Low latency, high reliability, low energy use
Resource Constraints	High processing and memory availability	Very limited memory, CPU, and power
Optimization Approaches	CDN, caching, parallel connections, HTTP/2, QUIC	MQTT, CoAP, edge computing, data aggregation, duty cycling

8. EMERGING TRENDS AND FUTURE DIRECTIONS IN TCP/IP FOR WEB AND IOT SYSTEMS

With the evolution of communication technologies, TCP/IP has continued to adapt to meet the growing demands of speed, reliability, scalability, and security across both Web and IoT environments. Though the traditional architecture of TCP/IP remains the backbone of the Internet, a number of challenges related to performance limitations, latency, massive device connectivity, and requirements for intelligent networking have fostered the development of new supporting protocols and technologies [36].

This, in turn, will provide a much-needed replacement for the depletion of IPv4, including a larger address space, and enabling billions of IoT devices to communicate directly. Another extension for IPv6 enables interoperability and scalability for even limited IoT devices: 6LoWPAN. QUIC was designed by Google and standardized by the IETF for addressing latency and overhead issues of TCP. QUIC operates over UDP with its embedded encryption, fast connection establishment, and enhanced congestion control, thus making it suitable for real-time IoT connectivity and high-speed web applications [36].

Another major trend is the integration of IoT and 5G networks. Due to 5G's high bandwidth, very low latency, and mMTC characteristics, real-time applications like industrial automation, remote surgery, and driverless cars will be able to use TCP/IP-based protocols effectively. However, IoT devices produce a huge volume of data, and utilising cloud computing for processing data solely is not practical. To reduce latency and improve security by reducing exposure to centralized servers, edge and fog computing-based architectures have emerged that process data closer to devices [37, 40].

Moreover, AI and ML are being used in TCP/IP networks to make them more autonomous and self-optimizing. AI-based systems can predict network congestion, change routing paths dynamically, detect anomalies or cyber-attacks, and optimize energy consumption of IoT devices. Lightweight encryption, blockchain-based authentication, and zero-trust architectures are further evolving the security protocols for enhanced resilience and trust in both web and IoT systems. Future research on TCP/IP will continue to be aimed at secure end-to-end communication of billions of heterogeneous devices, autonomous management, real-time performance, and energy efficiency. These will continue to ensure flexibility, scalability, and continuous support of intelligent transport, smart cities, next-generation web technologies, and industrial IoT ecosystems [38–40].

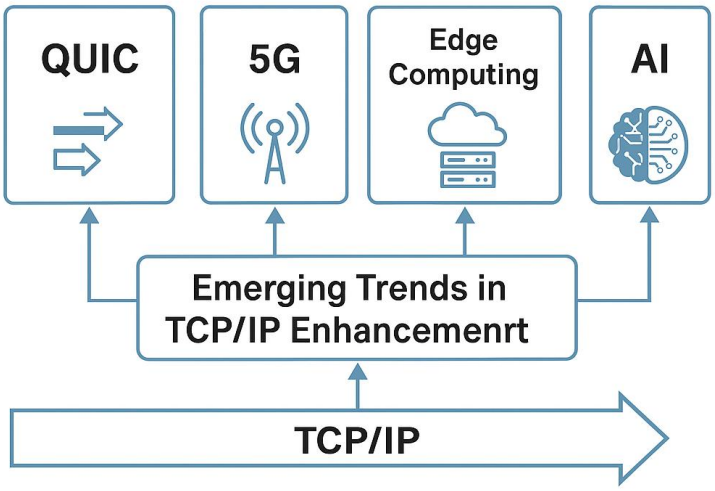

Figure 6. Future Trends in TCP/IP Evolution

9. CONCLUSION

TCP/IP remains the fundamental communication infrastructure of the internet, effectively supporting web services such as HTTP, HTTPS, FTP, and SMTP. On the other hand, with the development of the Internet of Things, some requirements that TCP/IP was not designed for, such as low-power devices, small data transfer, and massive device connections, emerged. In order to meet the demands of the Internet of Things, some lightweight protocols, including MQTT, CoAP, and 6LoWPAN, were developed within the TCP/IP framework. Performance, scalability, and security issues still affect online and Internet of Things applications. Latency and cyber-attacks are issues faced by web-based systems while limitations of device resources, unstable wireless links, and lack of protection are some issues faced by IoT systems. IPv6, QUIC, 5G, edge computing, and AI-based network management are some of the emerging technologies that further improve TCP/IP in terms of performance and versatility. To sum up, TCP/IP is evolving but not being replaced. Energy efficiency, low-latency communication, light-weight security, and intelligent autonomous networking are foreseen as accommodation for large-scale IoT systems and online services, and will be the main areas of future research.

10. REFERENCES

1- T. Murkomen, "Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey," GSC Advanced Research and Reviews, vol. 18, pp. 234-264, 2024.
2- K. Yasukata, "IIP: an integratable TCP/IP stack," ACM SIGCOMM Computer Communication Review, vol. 54, pp. 21-28, 2024.
3- S.-A. Drăgușin, N. Bizon, R.-M. Teodorescu, D. Toma, R.-N. Boștinaru, and G. Anghel, "Communication Protocols in Embedded Systems for Automotive Applications: Comparative Analysis and Implementation Through Virtual Instruments," in 2025 17th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2025, pp. 1-8.
4- H. Yang, H. Liu, X. Yuan, K. Wu, W. Ni, J. A. Zhang, et al., "Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and

Federated Learning in Advanced Networked Systems," Applied Sciences, vol. 15, p. 6587, 2025.
5- A. Gupta and V. K. Chaurasiya, "Adaptive Low-Latency Split Federated Learning with Dynamic Model Partitioning in Resource-Constrained Healthcare IoT," IEEE Transactions on Green Communications and Networking, 2025.
6- M. M. Alani, "Tcp/ip model," in Guide to OSI and TCP/IP models, ed: Springer, 2014, pp. 19-50.
7- R. A. A. P. Soepeno, "Comprehensive Network Analysis Through a Single Main Network Architecture," 2023.
8- J. Wijenbergh, V. Moonsamy, R. van Rijsdijk-Deij, and D. Kuijsters, "Performance comparison of DNS over HTTPS to Unencrypted DNS," PhD dissertation, 2019.
9- K. R. Fall and W. R. Stevens, Tcp/ip illustrated vol. 1: Addison-Wesley Professional, 2012.
10- G. Fisk, M. Fisk, C. Papadopoulos, and J. Neil, "Eliminating steganography in Internet traffic with active wardens," in International workshop on information hiding, 2002, pp. 18-35.
11- L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
12- J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
13- R. T. Fielding and R. N. Taylor, “Principled design of the modern Web architecture,” ACM Transactions on Internet Technology (TOIT), vol. 2, no. 2, pp. 115–150, 2002.
14- T. Berners-Lee, R. Fielding, and H. Frystyk, “Hypertext Transfer Protocol – HTTP/1.0,” IETF RFC 1945, May 1996.
15- T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” IETF RFC 5246, Aug. 2008.
16- A. Banks and R. Gupta, “MQTT version 3.1.1,” OASIS Standard, Oct. 2014.
17- Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP),” IETF RFC 7252, June 2014.
18- N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): Overview, assumptions, problem statement,” IETF RFC 4919, Aug. 2007.
19- A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
20- S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.
21- R. Rojas-Cessa, "Experiments on Computer Networks: Quickly Knowing the Protocols in the TCP/IP Suite," arXiv preprint arXiv:2308.01713, 2023.
22- V. Korpela, "Profinetin ja TCP/IP-tekniikan vertailu," 2022.
23- Z.-A. Chen, T.-Z. Wang, J.-K. She, K.-Y. Qian, and Z.-A. Zeng, "An Intelligent Control Simulation Platform for Nuclear Power Plants Using TCP/IP Real-Time Communication Framework," in International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant, 2024, pp. 585-599.
24- M. Ahsan, M. J. Awan, A. Yasin, S. A. Bahaj, and H. M. F. Shehzad, "Performace evaluation of TCP cubic, compound TCP and NewReno under Windows 20H1, via

802.11 n Link to LTE Core Network," Annals of the Romanian Society for Cell Biology, vol. 25, pp. 5357-5369, 2021.
25- V. P. Singh, M. N. Kumar, M. A. K. Misra, and P. Kuncha, IoT Communication protocols vol. 1: GCS PUBLISHERS, 2023.
26- C. M. Kozierok, The TCP/IP guide: a comprehensive, illustrated Internet protocols reference: No Starch Press, 2005.
27- P. B. Nath and M. M. Uddin, "Tcp-ip model in data communication and networking," American Journal of Engineering Research, vol. 4, pp. 102-107, 2015.
28- N. Gopalan and B. S. Selvan, TCP/IP ILLUSTRATED: PHI Learning Pvt. Ltd., 2008.
29- Y. Chen, "Performance of Message Queue Telemetry Transport Protocol and Constrained Application Protocol in Wireless Sensor Networks," 2017.
30- R. S. Phatak, "A Survey of Communication Protocols in IoT: MQTT, COAP, and Beyond," International Journal of Computer Technology and Electronics Communication, vol. 8, pp. 11013-11018, 2025.
31- F. Samad, A. Abbasi, Z. A. Memon, A. Aziz, and A. Rahman, "The future of internet: IPv6 fulfilling the routing needs in internet of things," International Journal of Future Generation Communication and Networking, vol. 11, pp. 13-22, 2018.
32- W. Shang, Y. Yu, R. Droms, and L. Zhang, "Challenges in IoT networking via TCP/IP architecture," NDN Project, vol. 2, 2016.
33- S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Computer Communication Review, vol. 19, pp. 32-48, 1989.
34- Z. B. Babovic, J. Protic, and V. Milutinovic, "Web performance evaluation for internet of things applications," IEEE Access, vol. 4, pp. 6974-6992, 2016.
35- S. Abourriche, A. Zyane, and A. Ghammaz, "Adaptation of Loss Recovery Mechanisms for improving Scalability and Quality of Service in IoT Networks," in 2023 IEEE International Conference on Advances in Data-Driven Analytics And Intelligent Systems (ADACIS), 2023, pp. 1-6.
36- G. Tselentis, "Towards the future Internet: emerging trends from European research," 2010.
37- M. Aledhari, R. Razzak, B. Qolomany, A. Al-Fuqaha, and F. Saeed, "Biomedical IoT: enabling technologies, architectural elements, challenges, and future directions," IEEE Access, vol. 10, pp. 31306-31339, 2022.
38- K. A. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147-157, 2019.
39- M. Țălu, "Security and privacy in the IIoT: threats, possible security countermeasures, and future challenges," Computing&AI Connect, vol. 2, pp. 1-10, 2025.
40- M. Rawat and G. Singal, "Surveying Technology Fusion in IoT Networks for IDS: Exploring Datasets, Tools, Challenges, and Research Prospects," ACM Transactions on Intelligent Systems and Technology, 2025.