GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey

Timothy Murkomen *

Department of computer science & software engineering, Jaramogi Oginga Odinga University of Science and Technology Bondo, Kenya.

GSC Advanced Research and Reviews, 2024, 18(03), 234–264

Publication history: Received on 30 January 2024; revised on 10 March 2024; accepted on 13 March 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.18.3.0106

Abstract

TCP/IP is the backbone of modern network communication, connecting devices across the world. TCP/IP at its core is a suite of protocols that enables the transmission of data between computers, facilitating the foundation of the interconnected global network. At the Application Layer of TCP/IP is where the interaction between software applications and the network occurs. The user-centric protocols such as HTTP, SMTP, FTP, POP3, IMAP and DNS facilitate various tasks at this layer such as web browsing, email communication, and file transfer. This comprehensive survey conducted an exploration of the performance, security and privacy issues at the application layer of the TCP/IP. It initiated by providing a background of TCP/IP model, it's architecture and the core characteristics, with major focus on the application layer. This paper aimed to discuss the state-of-the-art of performance, privacy and security concerns in TCP/IP application layer. It also proposed future research areas to equip researchers, practitioners, policy makers and the decision makers with tangible knowledge, offering guidance in navigating the performance, privacy and security concerns in TCP/IP Application Layer. It aimed to discuss the current performance, privacy and security research gaps at the Application Layer of the TCP/IP Model. The findings of this research sheds light on the performance, privacy and security issues while suggesting the countermeasures to strengthen and optimize the overall performance, security and privacy of TCP/IP model at the application layer. The paper finally suggests future directions and research areas at the TCP/IP application layer.

Keywords: TCP/IP; Application Layer; Performance; Privacy; Security; HTTP; HTTPS; FTP; SMTP; POP3; IMAP; DNS; SNMP; Telnet; DHCP

1. Introduction

The TCP/IP comprises of several communication protocols that are designed to operate over the internet and other private networks [1], hence facilitating the key operations and services across these networks [2]-[4]. It also ensures end to end connectivity by establishing and maintaining communications between the communication entities [5]-[7]. Tasks such as data formatting, addressing and packet routing are performed by TCP/IP hence ensuring reliable delivery of information to the intended recipients [8].

Many people utilize the established connections through a diverse array of devices which includes the desktop computers, laptops, mobile phones, and tablets [9], [10]. In regard to the vast adoption, TCP/IP application layer gains huge significance since it is user centric with the network [11]. According to [12], the primary utilization of the internet revolves around effective communication, entertainment, and education. It is paramount to recognize the nature of digital era which is very dynamic, where the TCP/IP protocol suite not only facilitates day-to-day activities but also serves as the backbone for emerging technologies. The ubiquity of devices connected to the internet brings about

* Corresponding author: Timothy Murkomen

diverse challenges and opportunities within the TCP/IP Application Layer, hence it is necessary to have an in-depth understanding of its functionalities, performance, privacy and security issues [13]-[16].

In the recent years, the emergence of cloud computing and Internet of Things (IoT), devices have intensified and strengthened the significance of the TCP/IP application layer [17]-[19]. Over the past ten years, the quantity of IoT devices has surpassed the total global population [20]. It is estimated that by the year 2025, there is an anticipation that the Internet of Things (IoT) will achieve the capability to establish connections between all devices utilized in our day-to-day lives and the digital ecosystem at large [21]. Cloud-based applications rely heavily on efficient data transfer mechanisms to ensure quality user experiences, on the other hand, the multitude of IoT devices add some layers of complexity to the already developed network interactions [22]- [24].

Numerous attacks focus specifically on the application layer hence exploiting vulnerabilities in web servers [25]-[30]. Web servers are openly accessible to the public hence it encounters numerous and frequent interactions from users. The primary objective of malicious personnel is to mimic legitimate and regular traffic as possible, for them to exploit and compromise the application. The most common protocols at the application layer includes the Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) [32], File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP)[33], Domain Name System (DNS) [34]-[38] , Simple Network Management Protocol (SNMP), Telnet , and DHCP (Dynamic Host Configuration Protocol (DHCP). HTTPS is commonly employed to ensure the security of data in transit [39]-[41]. However, potential vulnerabilities exist where the user data may be exposed to the risk of a data breach. This risk arises if the processing code is not adequately isolated from all other components, including the operating system on the host machine.

The need to address performance issues, privacy concerns, and security concerns within the TCP/IP application layer is very important because the application layer serves as the main interface for achieving data interoperability, interacting with various services and systems through the user centric application layer protocols [42], [43].

According to [44], TCP/IP is the fundamental protocol suite that governs communication on the internet. While TCP/IP has been instrumental in enabling global connectivity, it also poses significant privacy and security concerns. One primary issue revolves around packet interception and eavesdropping. TCP/IP packets are transmitted in plaintext, making them vulnerable to interception by malicious actors [45]-[47]. This poses a severe threat to privacy as sensitive information, such as personal data, financial details, or passwords, can be captured and exploited. Moreover, TCP/IP lacks built-in mechanisms for authentication and encryption, further exacerbating security vulnerabilities [48]-[51]. Without proper authentication, malicious entities can masquerade as legitimate users or systems, leading to unauthorized access and data breaches. Additionally, the absence of encryption means that data transmitted over TCP/IP networks can be easily intercepted and tampered with, compromising the integrity and confidentiality of the information exchanged.

Furthermore, TCP/IP-based systems are susceptible to various forms of cyber-attacks, including denial-of-service (DoS) attacks and man-in-the-middle (MitM) attacks. These attacks can disrupt network operations, degrade service quality, or facilitate unauthorized access to sensitive data [52]-[57]. Mitigating these threats requires implementing robust security measures, such as firewalls, intrusion detection systems, and encryption protocols, to safeguard TCP/IP-based communications and protect user privacy. Addressing the privacy and security challenges associated with TCP/IP is imperative to ensure the continued trust and reliability of internet communication networks.

In this study, it is evident that the performance, privacy, and security issues within the TCP/IP application layer are not isolated issues but interconnected aspects, that is, they are holistic in nature. Addressing one aspect inherently affects the other, hence it requires a more robust and holistic approach to navigate the ever-evolving challenges and the dynamic nature of internet communication.

The paper provides a comprehensive analysis of performance, privacy and security issues in TCP/IP application layer Protocols. To achieve this objective, the paper begins by presenting an overview of TCP/IP protocol suite and its architecture with a specific focus on the application layer. The findings of this survey will contribute to the existing body of knowledge by providing researchers, practitioners, decision makers and policy makers with a comprehensive understanding of the state-of-the-art in performance, security and privacy issues at the application layer protocols of the TCP/IP. This therefore informs the development of robust protocols in the TCP/IP application layer. This paper makes the following significant contributions:

- Contextualizing TCP/IP application layer protocols: The paper provides a comprehensive overview of TCP/IP protocol suite with specific focus on the application layer protocols. This includes HTTP, SMTP, FTP, POP3, IMAP,DNS and DHCP protocols.
- Performance, privacy and security issues in the TCP/IP application layer: The core focus of the survey is performance, privacy and security issues in the TCP/IP application layer protocols.
- Privacy and security issues countermeasures at the TCP/IP application layer: The paper also highlights the countermeasures to the performance, privacy and security issues in the TCP/IP application layer.
- Open research gaps and future directions: The paper highlights the open research gaps in privacy and security issues in the TCP/IP application layer.

The rest of this paper is structured as follows: Section I, II and III provides a concise introduction and overview of the TCP/IP application layer, with the key concepts related to the TCP/IP protocol and OSI reference model. The section also highlights the similarities and differences between the TCP/IP and the OSI reference model. Section IV conducts a comprehensive survey of the relevant literature, while Section V outlines the research methodology adopted for this study and covers sub-sections such as the research questions that guides the study. Section VI presents comprehensive analysis and discussions of the study focusing on in-depth exploration various attacks in the application layer protocols. Section VII presents the research gaps and future directions, finally, Section VIII presents the concluding remarks of this survey paper.

1.1. Research Motivation

The motivation behind conducting this survey lies in the increasing reliance on TCP/IP protocols specifically at the application layer. In today's interconnected world, where desktop computers, laptops, mobile phones, and tablets are commonplace, understanding the performance, privacy, and security issues within the TCP/IP application layer is crucial. This is coupled with the high emergence of cloud computing and Internet of Things (IoT) devices, and the fundamental role of TCP/IP plays in the internet. The article aims to shed light on the performance, security and privacy issues at the TCP/IP application layer protocols, its objective being to provide researchers, practitioners, decision makers and policy makers with a comprehensive understanding of the state-of-the-art in performance, security and privacy issues at the TCP/IP application layer in the rapidly evolving digital ecosystem.

2. Overview

2.1. TCP/IP Architecture

The TCP/IP protocol suite stands as an industry-standard for large networks that are interconnected worldwide [58]. In today’s internet, TCP/IP predates the OSI model as it serves as the foundational protocol. Unlike the OSI model's seven layers, the TCP/IP protocol suite consolidates the first three layers into a single layer, application layer and the last two into a unified layer (Network Interface). This distinction results in four layers for TCP/IP: Application Layer, Transport Layer, Internet Layer, and Network Interface Layer [59]. The functions align with the corresponding layers of the OSI model, however, the layer mapping is not one-to-one due to the differences in their architectural development, as depicted in Figure 1.

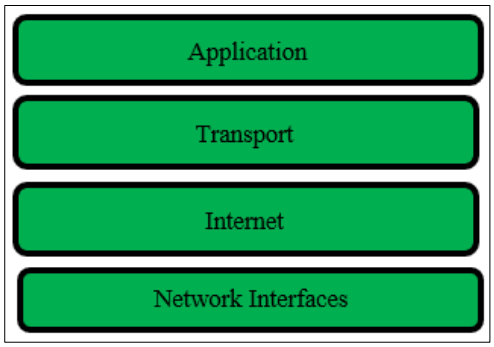

Figure 1 The TCP/IP Architecture

2.2. TCP/IP vs OSI Model

The Open System Interconnection (OSI) Model serves as a logical and conceptual framework defining network communication for systems that aim to interconnect and communicate with each other. OSI Model outlines a systematic

approach to organizing and understanding the complexities of computer packet transfer through the use of different layers of protocols. The OSI Model not only provides a blueprint for logical network structure but also effectively illustrates the process of data transfer between interconnected systems, making it a fundamental guide in the field of networking [60], [61].

2.2.1. Commonalities between the TCP/IP and OSI Models

The two conceptual frameworks have several commonalities as summarized in Table 1 below:

Table 1 The Commonalities of the OSI and TCP/IP Model

S/No	Commonality	Explanation
1	*Logical Models*	Both the TCP/IP and OSI models operate as logical models, providing a structured framework for understanding and implementing network communication processes.
2	*Standard Definition*	Both TCP/IP and OSI model play a critical role in defining standards for networking hence both contributes to the establishment of a robust common ground for communication protocols and devices.
3	*Framework for Implementation*	Both TCP/IP and OSI model offer a comprehensive framework for creating and implementing networking standards and devices. They guide the development of protocols and technologies that facilitate effective communication in computer networks. *Layered Approach:* Both models adopt a layered approach to network communication, breaking down the complex process into distinct layers, each responsible for specific functionalities. This layering enhances modularity and ease of understanding.
4	*Functionality Standards*	In both models, individual layers define specific functionalities and set standards exclusive to that particular functionality. This approach contributes to clarity and facilitates the efficient implementation of diverse networking functionalities.
5	*Interoperability*	Both models support interoperability, allowing manufacturers to produce devices and network components that can coexist and collaborate seamlessly with those from other manufacturers. This interoperability is essential for the diverse range of devices that constitute modern computer networks.
6	*Simplified Troubleshooting*	The division of complex functions into simpler components in both models simplifies the troubleshooting process. This modular approach aids in identifying and resolving issues at specific layers without the need to delve into the entire network structure.
7	*Referencing Existing Standards*	Instead of redefining standards and protocols already established by organizations like IEEE, both models reference and incorporate these existing standards. For instance, Ethernet standards were defined by IEEE before the inception of these models, and both TCP/IP and OSI models leveraged these standards rather than duplicating the effort.

2.2.2. Differences Between OSI Model and TCP/IP Model

The OSI Reference Model and the TCP/IP Model, although both serve as the fundamental frameworks for network communication, they differ in terms of their purposes, approaches, and development origins. The OSI Reference Model is a logical and conceptual model focusing on open system interconnection, providing reliability and addressing errors at each layer. In contrast, the TCP/IP Model mainly guides how computers connect to the internet and transmit data, handling reliability as an end-to-end issue with the transport layer managing error detection and recovery. The OSI Model has a smaller header size (5 bytes) and follows a vertical approach. It is also exclusively connection-oriented in its transport layer. On the other hand, the TCP/IP Model features a larger header size (20 bytes), and adopts a horizontal approach, and supports both connection-oriented and connectionless communication. Developed by ISO and ARPANET, respectively, they contribute to standardizing hardware and establishing connections between various computer types. The differences are summarized in Table 2.

Table 2 The differences between OSI and TCP/IP Model

S/No	Aspect	OSI Model	TCP/IP Model
1	Purpose and Focus	Logical and conceptual model for open system interconnection	Specifies how a computer should connect to the internet and transmit data
2	Reliability	OSI provides reliability as a fundamental aspect	TCP/IP addresses reliability as an end-to-end concern
3	Error Handling	Each layer detects and handles errors	Transport layer is responsible for error detection and recovery
4	Header Size	OSI header size is 5 bytes	TCP/IP header size is 20 bytes
5	Acronym Meaning	OSI stands for Open Systems Interconnection	TCP/IP stands for Transmission Control Protocol
6	Architectural Approach	OSI follows a vertical approach	TCP/IP follows a horizontal approach
7	Connection Orientation	OSI transport layer is only connection-oriented	TCP/IP model supports both connection-oriented and connectionless
8	Development Organization	OSI model developed by ISO (International Standard Organization)	TCP/IP model developed by ARPANET (Advanced Research Project Agency Network)
9	Hardware Standardization vs. Connection Establishment	OSI helps standardize router, switch, motherboard, and other hardware	TCP/IP facilitates connection between different types of computers

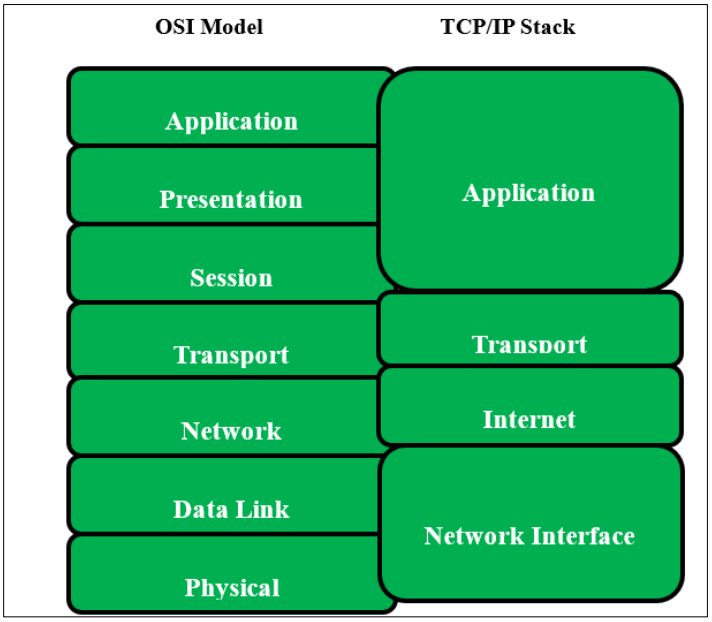

Figure 2 The OSI and TCP/IP Architecture

2.3. TCP/IP Application Layer Protocols

The TCP/IP Model application layer combines the functionalities of the application, presentation, and session layers in the OSI model. This is clearly shown in Figure 2. Application layer engages directly with the users and is responsible for initiating transfer of data onto the network. It utilizes software programs for network communication. The presentation

layer also handles data formatting for proper interpretation by the destination device, including tasks such as data compression, decompression, encryption, and decryption [62],[63].

There are various application layer protocols that facilitate the exchange of user information. Examples of these protocols includes Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) [64], File Transfer Protocol (FTP) [65], Simple Mail Transfer Protocol (SMTP) [66], Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP)[67], Domain Name System (DNS), Simple Network Management Protocol (SNMP), Telnet , and DHCP (Dynamic Host Configuration Protocol (DHCP). HTTPS is commonly employed to ensure the security of data in transit [68], [69]. Each protocol possesses performance, security and privacy issues as discussed in the next part. TCP/IP application layer protocols are summarized in Table 3 below.

Table 3 Summary of common ports in the TCP/IP Application Layer

Protocol	Description	Common Ports
HTTP	Hypertext Transfer Protocol	80
HTTPS	Hypertext Transfer Protocol over SSL	443
FTP	File Transfer Protocol	21
SMTP	Simple Mail Transfer Protocol	25
POP3	Post Office Protocol version 3	110
IMAP	Internet Message Access Protocol	143
DNS	Domain Name System	53
SNMP	Simple Network Management Protocol	161, 162
Telnet	Telnet Protocol	23
DHCP	Dynamic Host Configuration Protocol	67, 68

2.3.1. HTTP & HTTPS

The Hyper Text Transfer Protocol (HTTP) is an application layer protocol that is utilized in the client-server architecture [70]. HTTP facilitates communication between internet web clients hence acting as a request-response protocol, that is between the web browsers and the web servers [71], [72]. When a client initiates a request, the HTTP protocol transfers the request to the server for processing. After the processing, the server generates a response which is then sent back to the client over the network. This is demonstrated in Figure 3.

HTTPS provides robust security measures for data transmission of data over the internet hence ensuring confidentiality and integrity of data [73]-[75]. However, some researchers suggest that HTTPS implementation can lead to increased power consumption [76], [77], which may not be ideal for devices with limited battery life. Researchers also suggest that HTTPS may lack flexibility [78] in some scenarios, hence potentially hindering the performance and functionality. Giant sites such as Facebook and YouTube have widely adopted HTTPS as the standard protocol for secure communication with their users [79]. Therefore, while HTTPS offers strong security benefits, its impact on power consumption and flexibility should be considered when designing internet applications.

The standard HTTP protocol poses a security risk as data transmitted from the server to the browser is not encrypted, leaving it vulnerable to theft. HTTPS protocols helps mitigate this risk by incorporating SSL (Secure Sockets Layer) [80] certificates, or TLS enabling the establishment of a secure encrypted connection between the server and the browser. This encryption prevents potential interception of sensitive data, such as credit card information and passwords, during transmission [81]-[87]. Authentication is also a crucial aspect provided by HTTPS, ensuring that both the server and the client can verify each other's identities [88], [89]. In today's internet landscape where trust and security are paramount, the authentication function offered by HTTPS is very paramount.

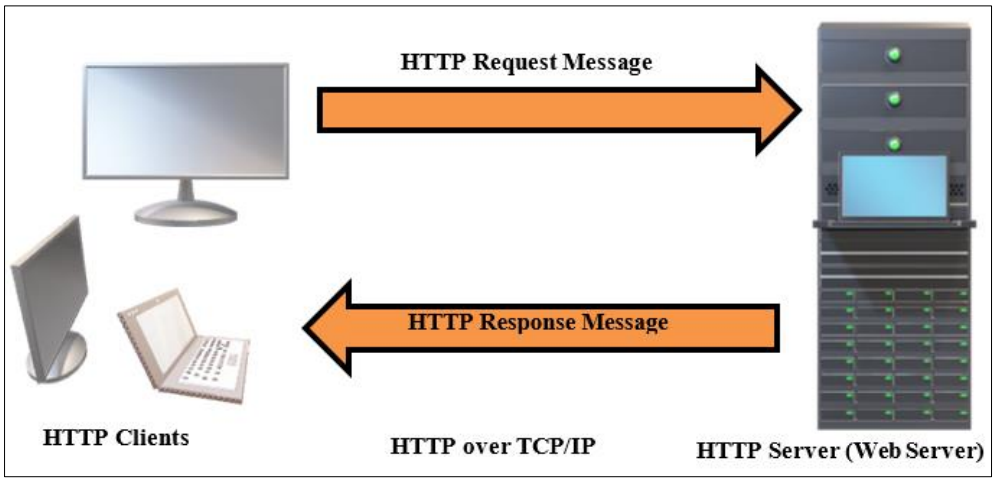

Figure 3 HTTP Request Response

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) provides security measures for data transmission over the internet, ensuring data confidentiality and integrity. The difference between HTTP and HTTPS are shown in Table 4.

HTTPS = HTTP + SSL

Table 4 Sample Differences between http and https

Feature	**HTTP**	**HTTPS**
Protocol	Hypertext Transfer Protocol	Hypertext Transfer Protocol over SSL
Encryption	No encryption, data is transmitted in plaintext	Uses SSL/TLS encryption to secure data transmission.
Security	Not secure, Vulnerable to eavesdropping and data interception.	Provides secure communication, preventing data theft.
URL	Begins with http://	Begins with htttps://
Port	Default Port is 80	Default port is 443
SSL Certificate	Not required	Requires SSL Certificate for encryption
Authentication	No built-in authentication mechanisms	Supports server and client authentication
Usage	Suitable for non-sensitive data transmission	Essential for transmitting sensitive information such as passwords and financial data.

2.3.2. Telnet

Terminal Network (Telnet) is a standard TCP/IP protocol that facilitates the establishment of connections to remote devices [90]. This enables the local terminal to appear as if it is directly connected to the terminal at the remote system. Telnet serves as a communication tool, allowing users to interact with devices located at remote locations. Network administrators commonly utilize Telnet for accessing and managing remote devices by establishing connections through the IP address or hostname of the remote device [91]. Figure 4 below illustrates the Telnet.

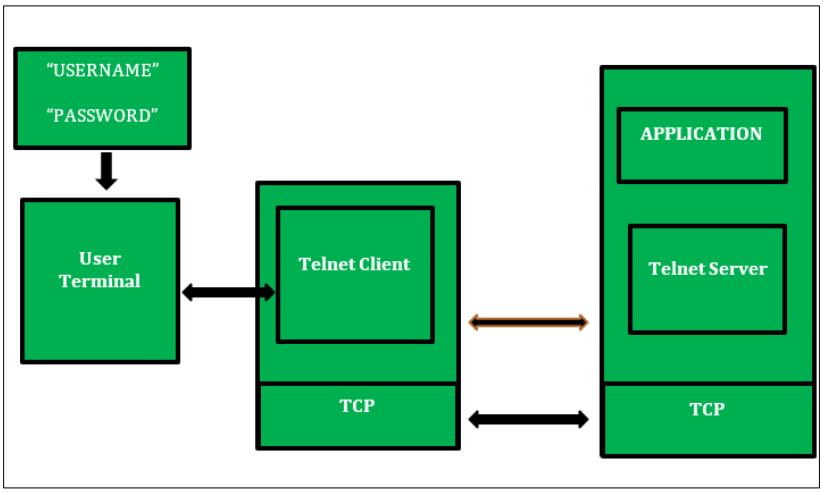

Figure 4 The Telnet Protocol

2.3.3. Secure Shell (SSH)

SSH, also known as Secure Shell enables users to manage and manipulate remote servers on the internet securely [93]. SSH is positioned as a secure alternative to Telnet and it employs cryptography [94] to ensure the encryption and security of all communications. One of its primary features of SSH is the provision of authentication for remote users. SSH employs various encryption techniques, including Symmetric Encryption, which utilizes a shared secret key for both encryption and decryption, ensuring secure communication between sender and receiver. Common ciphers for Symmetric Encryption include DES, AES, and Triple DES. SSH also utilizes Asymmetric Encryption, utilizing distinct public and private keys for encryption and decryption. The public key is used for encryption, while the private key, held exclusively by the receiver, is used for decryption. Notable ciphers for Asymmetric Encryption encompass RSA, Diffie-Hellman, and defence against potential threats like Man-in-the-Middle attacks [95], [96].

2.3.4. SMTP

The Simple Mail Transfer Protocol (SMTP) functions as a Message Transfer Agent (MTA) and operates on port number 25 [97]. In the email communication process, a sender or client requires a client MTA to send emails, while the recipient or server needs a server MTA to receive the mail. SMTP plays a pivotal role on the Internet by defining both the MTA client and MTA server. Its primary purpose is to establish the guidelines for the transfer of data between the MTA client and MTA server through the exchange of commands and responses [98], [99]. In essence, SMTP provides the framework for the seamless transfer of emails across the Internet. Figure 5 illustrates the SMTP protocol.

2.3.5. Post Office Protocol version 3 (POP3)

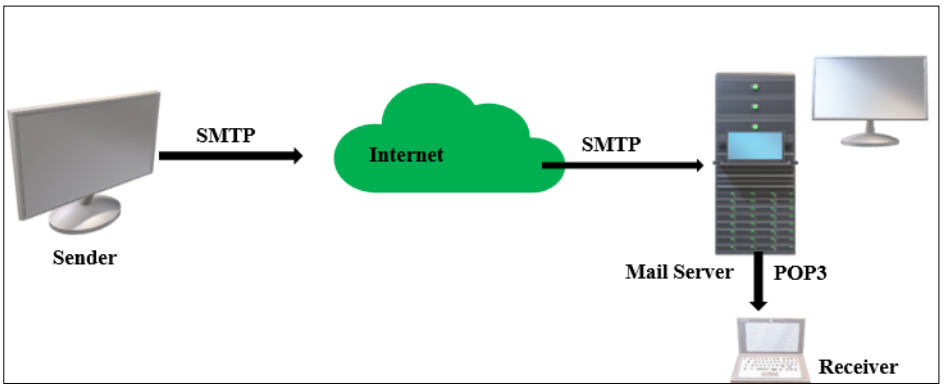

Figure 5 The SMTP Protocol

In the third phase of email retrieval, a pull program becomes essential to extract messages from the mail server and deliver them to the intended recipient. This process employs message access agents (MAA) designed to retrieve data from the mail server [100]. Post Office Protocol version 3 (POP3) serves as one such message access agent, utilizing port

number 110. When a user initiates email access to download messages from the mailbox on the mail server, the client establishes a connection to the server on port 110. Subsequently, the client employs a username and password to gain access to the mailbox, enabling users to retrieve their messages securely [101].

2.3.6. IMAP 4

The IMAP4 (Internet Mail Access Protocol) version 4, operating on Port 993, surpasses POP3 in both capability and complexity. Unlike POP3, which restricts users from creating emails on the server, lacks the provision for separate folders, and doesn't allow users to preview emails before downloading, IMAP4 introduces enhanced features. With IMAP4, users can examine emails before downloading, opt for partial downloads, and exercise additional functionalities like creating, deleting, or renaming mailboxes directly on the mail server. This heightened flexibility and functionality make IMAP4 a more advanced and versatile option compared to the limitations of POP3 [102]-[104]. Figure 6 shows the POP 3 and IMAP protocols.

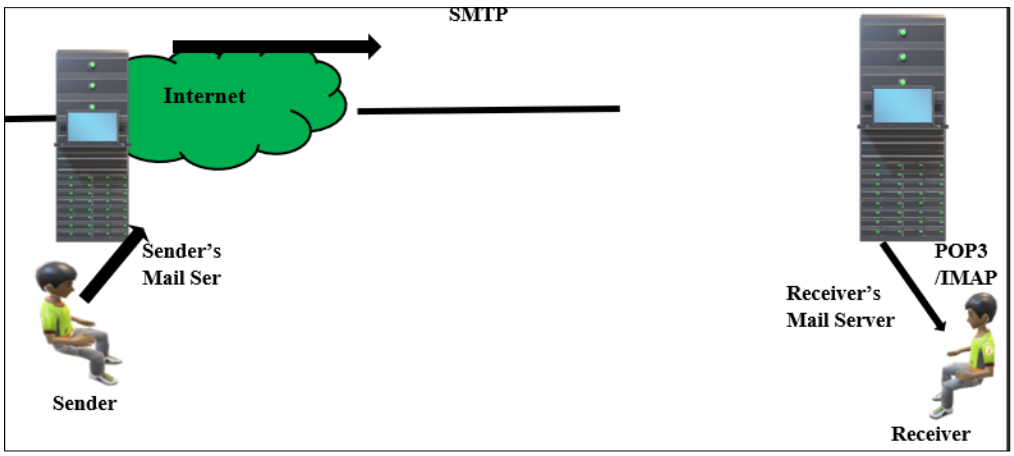

Figure 6 POP3 and IMAP protocols

2.3.7. File Transfer Protocol (FTP)

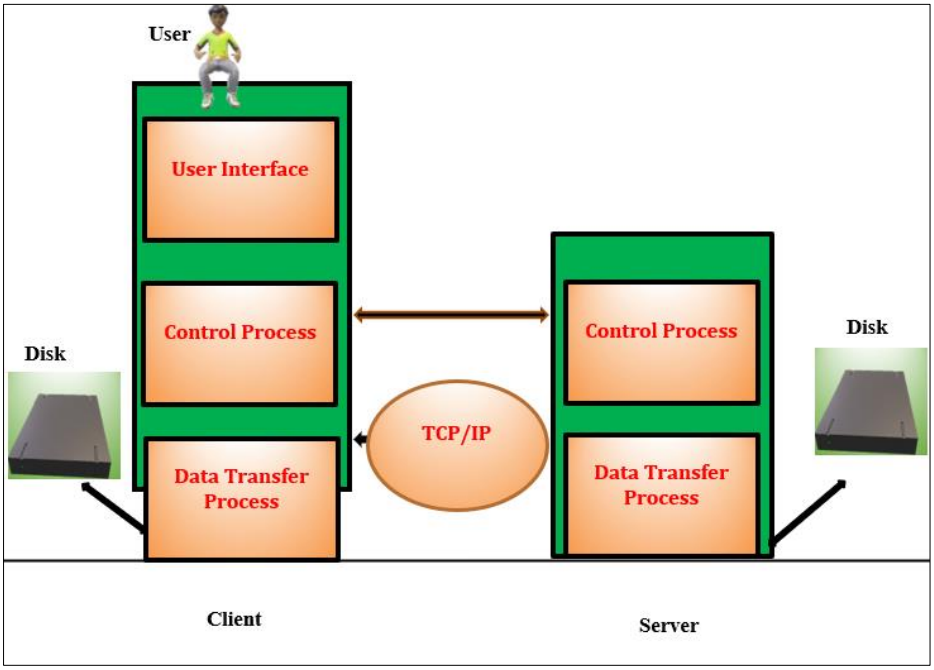

Figure 7 File Transfer Connection

The File Transfer Protocol (FTP) [105] is employed to replicate a file from one host to another, utilizing TCP services for the transfer process. This involves establishing two connections between the hosts – one dedicated to data transfer

with port number 20 and the other handling control information with port number 21.The control processes utilize the control connection, which remains open for the entirety of the FTP session. In parallel, the data transfer processes employ the data connection, specifically opened for the file transfer operation and subsequently closed once the transfer is completed [106], [107]. The fundamental FTP model is illustrated in the Figure 7 while Table 5 presents a summary of the TCP/IP Application Layer Protocols.

Table 5 Summary of the TCP/IP Application Layer Protocols

S/No	Protocol	Description	Use Cases/ Features	Security Aspects	Common Ports
1	HTTP	Hypertext Transfer Protocol	Web browsing, data retrieval, content delivery	SSL/TLS for secure connections	80
2	HTTPS	Hypertext Transfer Protocol over SSL	Secure version of HTTP with SSL/TLS	Encryption, secure data transmission	443
3	FTP	File Transfer Protocol	File transfer between hosts	Authentication, data integrity	21
4	SMTP	Simple Mail Transfer Protocol	Email transmission	Authentication, message integrity	25
5	POP3	Post Office Protocol version 3	Retrieving email from a serve	Secure variants available	110
6	IMAP	Internet Message Access Protocol	Access and manage email on a server	SSL/TLS support, authentication	143
7		Domain Name System	Translates domain names to IP addressed	DNSSEC for security	53
8	SNMP	Simple Network Management Protocol	Network devices monitoring and management	SNMPv3 for secure communication	161, 162
9	Telnet	Telnet Protocol	Remote terminal access	Encrypted alternatives recommended	23
10	DHCP	Dynamic Host Configuration Protocol	Automatic IP address assignment	Security considerations exist	67, 68

3. Related Work

Over the recent years, numerous articles have been conducted in the entire ecosystem of TCP/IP suite. Many researchers have addressed the general performance, privacy and security concerns [108] in the ecosystem of TCP/IP. Authors in [109] investigate vulnerabilities in the TCP/IP header, analysing various attack vectors such as TCP SYN flooding and session hijacking. The primary goal of the paper was to propose effective countermeasures, utilizing an experimental-simulation approach, to enhance TCP/IP header security and assist network designers in implementing robust security measures at this level. Author in [110] investigates and compares the effectiveness of the messaging protocols which includes the MQTT, CoAP, AMQP, and HTTP within IoT systems.

The authors in [111] provided a comprehensive overview and analysis of the various protocols and standards relevant to the Internet of Things (IoT), while the study in [112] compares various IoT application layer protocols through the implementation of a smart parking system. The researchers in [113] compared the application layer protocols for the Internet of Things (IoT) through experimentation. Several surveys have been conducted but focusing on the general TCP/IP protocol suite. The study in [114] Unveils vulnerabilities associated with web attacks and it focuses specifically on Man-In-The-Middle attacks [115] and session hijacking. The paper analyses trends, contributors, and solutions from selected studies spanning the years 2016-2023, shedding light on evolving cyber-security measures needed to address these threats.

Researchers in [32] explored comprehensively recent advancements in IoT application layer protocols and assess the potential research directions at the intersection of IoT and machine learning. The paper provides insights into the

evolving landscape of IoT protocols while identifying opportunities for incorporating machine learning techniques in this context. Authors in [116] provides an in-depth examination of the application layer messaging protocol in the Internet of Things (IoT). It offers an extended review of the messaging protocols within the IoT context. Table 6 shows comparative analysis of the review papers.

Table 6 Comparative Analysis of the Review Papers

Ref	Year	Title	Objective
[114]	(2024)	Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking	The paper explores vulnerabilities associated with web attacks, specifically focusing on Man-In-The-Middle attacks and session hijacking. It also analyses trends, contributors, and solutions from selected studies spanning the years 2016-2023.
[116]	(2023)	An extended review of the application layer messaging protocol of the internet of things.	This article seeks to provide an in-depth examination of the application layer messaging protocol in the Internet of Things (IoT). It aims offers an extended review of messaging protocols within the IoT context.
[117]	(2023)	An approach to application-layer DoS detection	This study aims to address the growing difficulty in countering Denial of Service (DoS) attacks, particularly those targeting application-layer protocols such as HTTP, DNS, and SMTP. It proposes a generalized detection approach for application-layer DoS attacks, utilizing a combination of datasets and machine learning techniques.
[118]	(2022)	Survey on recent advances in IoT application layer protocols and machine learning scope for research directions.	The paper aims to comprehensively explore recent advancements in IoT application layer protocols and assess the potential research directions at the intersection of IoT and machine learning. It also provides insights into the evolving landscape of IoT protocols while identifying opportunities for incorporating machine learning techniques.
[119]	(2021)	A survey on IoT application layer protocols	The research explores evolving IoT technology in computer engineering, emphasizing application layer protocol selection. It defines potential protocols and compares their traffic management efficiency in diverse IoT applications based on experimental results. The paper also aims to streamline protocol selection for effective integration in the dynamic IoT ecosystem.
[32]	(2020)	Security of IoT Application Layer Protocols: Challenges and Findings.	This research conducts a comprehensive survey on the security challenges of application layer protocols in IoT technologies. It focuses on messaging/data sharing and service discovery protocols. It also analyses the main threats, Common Vulnerabilities and Exposures (CVE), and provides in-depth insights into good practices and measures to mitigate security risks.
[110]	(2017)	Choice of effective messaging protocols for IoT systems: MQTT, CaAP, AMQP and HTTP	The article aims to investigate and compare the effectiveness of messaging protocols which includes the MQTT, CoAP, AMQP, and HTTP, within IoT systems. It focuses on providing insights into the strengths and weaknesses of these protocols to assist in making informed choices for optimal messaging in IoT environments.
[120]	(2017)	TCP IP Header Attack Vectors and Countermeasures	This paper investigates vulnerabilities in the TCP/IP header, analysing various attack vectors such as TCP SYN flooding and session hijacking. It suggests the possible countermeasures, utilizing an experimental-simulation approach, to enhance TCP/IP header security
[112]	(2017)	A Comparison of IoT application layer protocols	Aims to compare various IoT application layer protocols through the implementation of a smart parking system. It focuses on

		Through a smart parking implementation	evaluating and contrasting Application Layer protocols within the context of smart parking.
[111]	(2017)	A survey of protocols and standards for internet of things	This survey provides a comprehensive overview and analysis of the various protocols and standards relevant to the Internet of Things (IoT). The paper analyses IoT protocols facilitating a better understanding of the technologies and standards that play a crucial role in IoT applications and implementations.
[113]	(2016)	Comparing application layer protocols for the internet of things via experimentation	Aims to compare application layer protocols for the Internet of Things (IoT) through experimentation.

4. Research Methodology

In this survey paper, we analyse existing literature on TCP/IP Application layer focusing on performance, security and privacy concerns. The research methodology employed in this study involves a comprehensive review of academic papers, conference proceedings, and relevant publications. The paper employs a rigorous selection process hence providing a holistic and up-to-date overview of the current state of research in this domain. The methodology employed in the study comprises three distinct steps:

4.1. String Searching

On 15th January, 2024, a comprehensive search was conducted to identify relevant research papers for our study, resulting in a total of 497 papers. After removing 266 papers due to duplication, 231 papers remained. Subsequently, 119 articles were excluded based on the inclusion and exclusion criteria, leaving 112 articles for further analysis. During the abstract-based screening process, an additional 89 articles were excluded, resulting in 23 articles for in-depth review. After carefully reviewing these articles, four were excluded as they did not align with the scope and objectives of the current research, leaving a final dataset of 19 articles. After reading the full articles, four more were removed, resulting in a total of 15 articles that were ultimately included in the study. Figure 8 shows the selection and screening process.

4.2. Data Sources

The data sources for this research encompassed a selection of renowned academic databases, including IEEE Xplore, Science Direct, Springer, Hindawi, and PLOS. The databases were chosen for their extensive collection of scholarly papers and articles relevant to the study's focus on performance, privacy and security issues in the TCP/IP application layer. Through a systematic search process using specific keywords and Boolean operators such as *("All Metadata": TCP/IP Application Layer)* ***OR*** *("All Metadata": Performance, Security)* ***AND*** *("All Metadata": Privacy Issues)*. The papers were then carefully evaluated based on their titles, abstracts, and keywords to ensure their relevance and alignment with the research questions and objectives. The selected papers from these databases with the corresponding keywords and Boolean Operators are listed in the **Table 7** below:

Table 7 Selected Databases

S/No	Database	No. of Articles	URL	Keywords
1	IEEE	3753	https://www.ieee.org/	("All Metadata": TCP/IP Application Layer) OR ("All Metadata": Performance, Security) AND ("All Metadata": Privacy Issues)
2	Science Direct	2593	https://www.ieee.org/	"Performance, Security and Privacy issues in the TCP/IP Application Layer"
3	Springer	1527	https://www.springer.com/	Performance, Security and Privacy issues in the TCP/IP Application Layer
4	Wiley	19	https://onlinelibrary.wiley.com/	"Performance, Security and Privacy issues in the TCP/IP Application Layer"

5	MDPI	203	https://www.mdpi.com/	"Performance OR Security OR Privacy AND TCP/IP Application Layer"
6	PLOS	274	https://plos.org/	"Performance, Security and Privacy issues in the TCP/IP Application Layer"

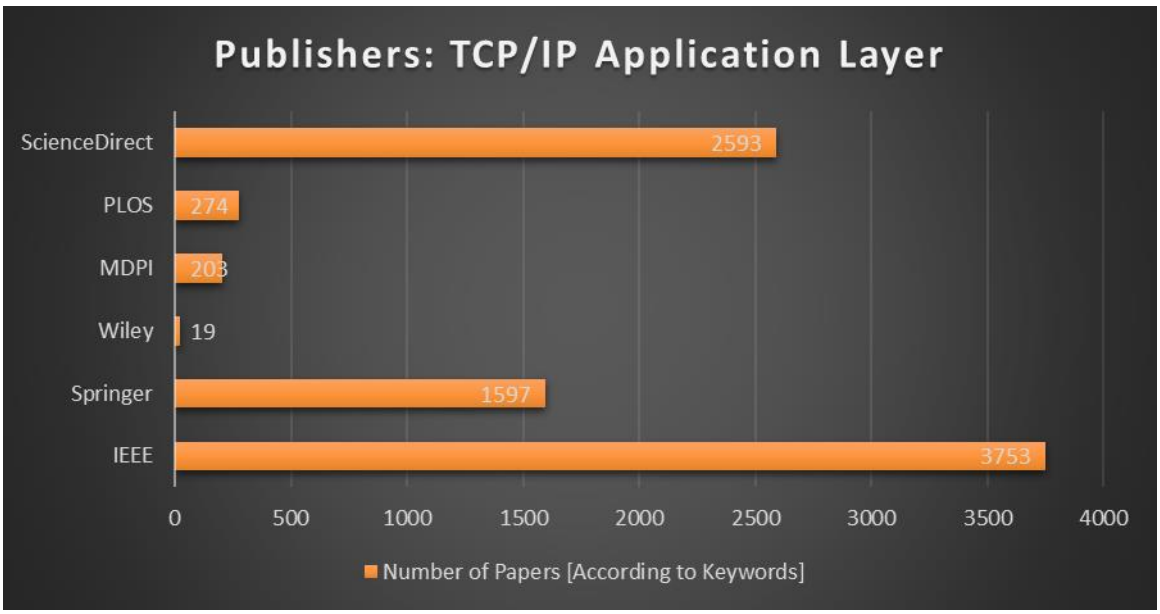

Figure 8 Publishers in the field of TCP/IP Application Layer

4.3. Screening of the papers

This stage involved a rigorous screening of papers identified from the data sources as summarized in Table 4. The screening initiated by assessing the relevance of each paper according to their titles, abstracts, and keywords, ensuring they were aligned with the research area at hand, which focused on the performance, privacy and security issues in the TCP/IP application layer protocols. Papers that met the predefined criteria were subjected to a more in-depth review to determine the suitability for achieving the research objectives and answering the research questions. During this process, research that focused on TCP/IP layer with more aim in performance, security and privacy issues in the application layer were retained for further analysis. In contrast, papers that did not closely align with the research objectives were excluded in the process. This robust screening of papers ensured that not only the highly relevant papers are included in the study, but also valuable papers are included in the study, contributing to the achievement of the research objectives and the credibility of the research findings. The selection and screening process are summarized in Figure 9.

4.4. Research Questions

In this survey, we aim to address five research questions, which includes the current performance issues in the TCP/IP Application layer protocols. It also aims to address the privacy and security concerns that exist with the TCP/IP application layer protocol. The study finally provides the overview of current research gaps and the future research areas that can address the identified concerns in the TCP/IP application layer protocols. The research questions are summarized in Table 8 with the corresponding motivation.

5. Analysis and Discussion of the results

In this sub-section, we present a comprehensive analysis of the outcomes obtained from our research study on performance, privacy, and security issues at the TCP/IP Application layer. The analysis focused extensively on the data collected during the research process, aiming to answer the research questions outlined in Table 8. We examine the results to gain valuable insights into the performance, security, and privacy issues in the TCP/IP application layer. **Table 9** provides a comparative analysis of the review papers.

5.1. RQ 1: Current Performance Issues in the TCP/IP Application Layer

The investigation into current performance issues in the TCP/IP application layer revealed several key areas. Key findings in the study revealed that latency is a prominent concern impacting the responsiveness of user-centric protocols. Bandwidth limitations were identified also as key contributors to slower data transmission, affecting various application layer tasks such as web browsing and file transfers. Others include protocol processing overhead, concurrent connections handling, resource utilization and data parsing and formatting.

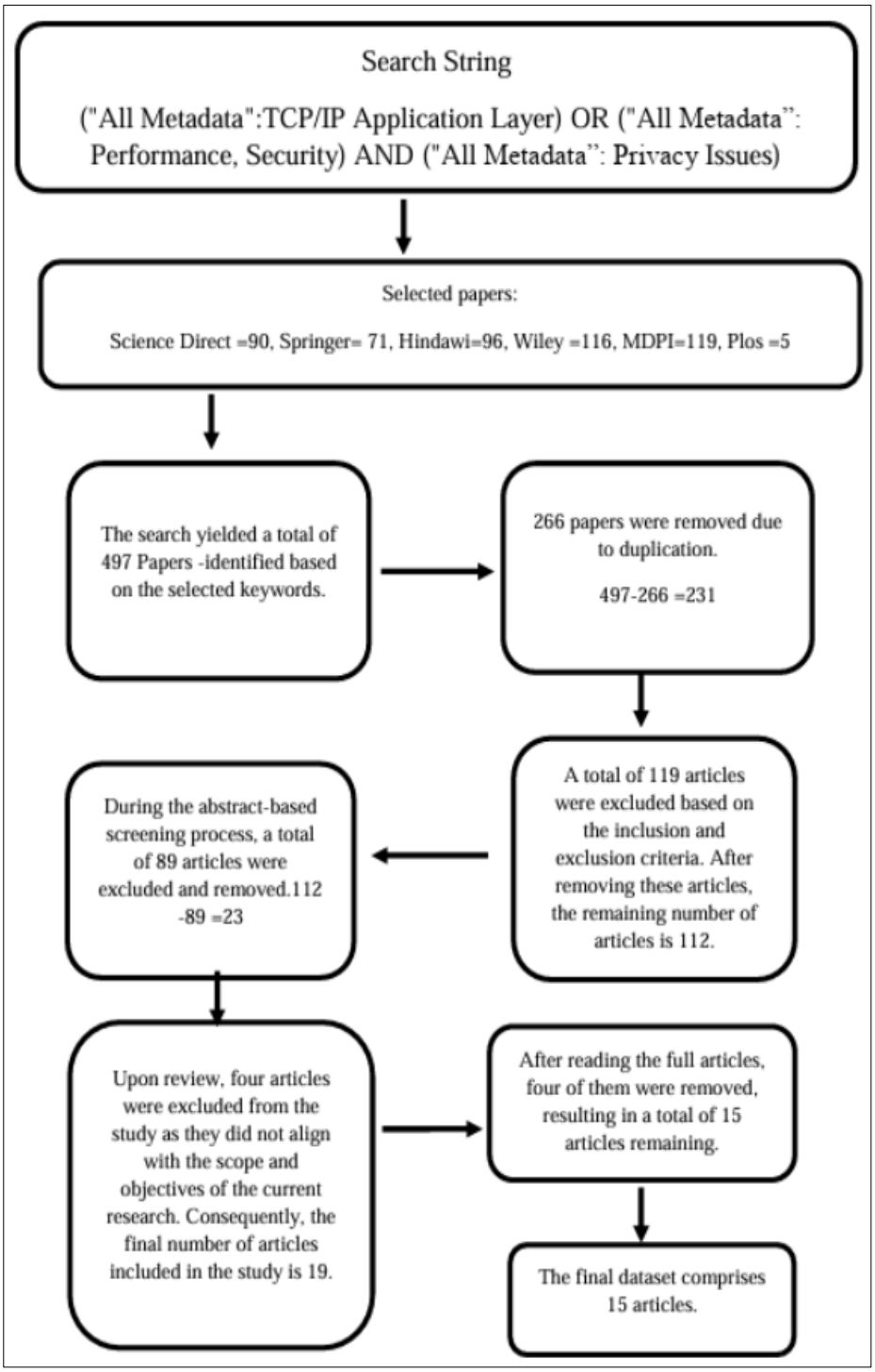

Figure 9 The selection and screening process

Latency: Latency is a prominent concern impacting the responsiveness of user-centric protocols. Latency in TCP/IP networks, often referred to as the time it takes for a data packet to travel from its source to its destination, is a critical

performance metric that affects the user experience and the efficiency of networked applications [121], [122]. Factors contributing to latency include the physical distance between communicating nodes, the number of hops (intermediate devices like routers and switches) data packets must traverse, the quality and capacity of the network connections, and the congestion levels on the network. TCP/IP's connection establishment process, involving the three-way handshake, and its congestion control mechanisms, designed to ensure network stability by adjusting the rate of data transmission based on network traffic conditions, can also introduce additional latency [123]-[126]. Reducing latency in TCP/IP networks is crucial for time-sensitive applications such as online gaming, real-time communications, and financial transactions, where delays can have significant impacts on usability and performance.

Bandwidth limitations: Bandwidth limitations were identified also as key contributors to slower data transmission, affecting various application layer tasks such as web browsing and file transfers. Bandwidth limitations in TCP/IP networks refer to the maximum rate at which data can be transferred over a network connection, significantly influencing the performance and throughput of networked applications [127]. These limitations are dictated by various factors including the physical media's capacity (such as fiber optic, cable, or wireless), the quality of network hardware (routers, switches, and modems), network topology, and the protocols used for data transmission.

TCP/IP's inherent control mechanisms, such as flow control and congestion avoidance, while essential for maintaining network stability and preventing packet loss, can also throttle the data transmission rate, especially in high-latency environments or during peak traffic times [128], [129].

Table 8 Research questions

	Research Question	**Motivation**
RQ 1	What are the current performance issues in the TCP/IP Application Layer?	Understanding the existing challenges will help in identifying areas that require improvement for better application layer performance.
RQ 2	What privacy concerns exist within the TCP/IP Application Layer?	Exploring privacy issues will contribute to enhancing user-centric protocols and addressing potential vulnerabilities in data transmission.
RQ 3	What are the prevalent security issues in the TCP/IP Application Layer?	Identifying security concerns will aid in developing effective countermeasures to protect against threats and vulnerabilities at the application layer.
RQ 4	What are the existing research gaps in TCP/IP Application Layer performance, privacy, and security?	Recognizing research gaps will guide future studies, helping researchers focus on areas where additional investigation is needed.
RQ 5	What future research areas can address the identified issues in TCP/IP Application Layer?	Proposing future research areas will provide a roadmap for researchers and policymakers to guide efforts towards improving TCP/IP application layer concerns.

Additionally, the overhead introduced by the TCP/IP headers further reduces the effective bandwidth available for application data. As a result, optimizing TCP/IP configurations, employing quality of service (QoS) policies, and upgrading network infrastructure are critical steps for mitigating bandwidth limitations and improving the overall efficiency of data transmission over TCP/IP networks [130].

Protocol Processing Overhead: The processing overhead associated with application layer protocols, such as HTTP, SMTP, or FTP, can impact performance. According to [131], protocol processing overhead in TCP/IP networks refers to the computational and time resources required to process the TCP/IP protocol stack layers, including data encapsulation/de-capsulation, header analysis, and error checking. This overhead can significantly impact network performance, particularly on devices with limited processing capabilities or in scenarios involving high-speed data transmission [132]. Each layer of the TCP/IP model (application, transport, internet, and link) adds its own set of headers to the data packet, increasing the overall packet size and requiring additional processing at each hop along the packet's journey. Moreover, tasks such as the three-way handshake for establishing a TCP connection, the calculation of checksums for error detection, and the dynamic adjustment of transmission rates to manage congestion control, all contribute to the processing workload. This not only affects the latency and throughput of the network but also consumes valuable system resources [133], highlighting the importance of efficient protocol design and the need for hardware capable of handling high levels of network traffic with minimal delays.

Concurrent Connections Handling: The ability of the application layer to efficiently manage and handle multiple concurrent connections can affect performance. Concurrent connections handling in TCP/IP networks is a critical aspect that determines the ability of a network to support multiple simultaneous communication sessions between devices [134]. This capability is essential for maintaining the performance and reliability of web servers, databases, and other networked services that must manage numerous client connections at once. TCP/IP handles concurrent connections through the use of unique combinations of source and destination IP addresses and ports, allowing each connection to be uniquely identified and managed independently [135, [136]. However, the handling of a large number of concurrent connections poses challenges, including increased memory and CPU usage, potential bottlenecks in network equipment, and the need for efficient connection and session management strategies to prevent congestion and ensure fair resource allocation among all active connections. Optimizations such as connection pooling, load balancing, and the use of more efficient protocols like QUIC over traditional TCP can help mitigate these challenges, enhancing the network's ability to handle high volumes of concurrent connections effectively.

Data Parsing and Formatting: Applications often need to parse incoming data and format outgoing data according to specific protocols or standards. Data parsing and formatting in TCP/IP networks are crucial processes that involve the organization, interpretation, and conversion of data as it traverses through the various layers of the TCP/IP protocol stack [137], [138]. Each layer in the stack has its own specific format for headers and payloads, necessitating that data be parsed (i.e., analysed and structured) and formatted (adapted to a specific structure) appropriately as it is encapsulated for transmission or de-capsulated upon reception. This ensures that the data can be correctly interpreted and processed by sending and receiving devices [139]. For example, at the application layer, data might need to be formatted according to the rules of HTTP, FTP, or SMTP protocols, while at the transport layer, TCP or UDP headers are added to manage flow and error control. Efficient [140] parsing and formatting are essential for the seamless interoperability of network services and applications, but they also introduce overhead that can impact performance, making it a balancing act to ensure data integrity and protocol compliance without unduly affecting network speed and efficiency.

Resource Utilization: Application layer processes may consume significant system resources, such as CPU, memory, and network bandwidth [141]. Inefficient resource utilization can lead to performance degradation, especially in resource-constrained environments.

Scalability: The ability of application layer protocols and services to scale horizontally to accommodate increasing loads is crucial for maintaining performance under high demand [142].

These findings emphasize the need for optimization strategies to strengthen the overall performance of the TCP/IP application layer protocols. Table 9 below summarizes the current performance issues in the TCP/IP application layer.

Table 9 Current performance issues in the TCP/IP Application Layer protocols

S/No	Performance Issue	Illustration	Action
1	Latency	Delays in response time for user requests	Implementing caching mechanisms Optimizing network routing
2	Bandwidth Limitations	Restriction in data transfer speed	Employing data compression techniques. Optimizing content delivery networks
3	Protocol Processing Overhead	High CPU usage for parsing application layer protocols	Utilizing efficient parsing algorithms Implementing protocol-specific optimizations
4	Concurrent Connections Handling	Inefficient management of multiple simultaneous connections	Implementing connection pooling Optimizing connection handling mechanisms
5	Data Parsing and Formatting	Inefficient processing of incoming/outgoing data according to protocols	Optimizing parsing and formatting algorithms

6	Resource Utilization	Excessive consumption of system resources	Implementing resource usage monitoring Optimizing memory and CPU utilization
7	Scalability	Inability to handle increasing loads	Implementing horizontal scaling techniques Optimizing load balancing mechanisms

5.2. RQ 2 and RQ 3 : Security and Privacy Concerns within the TCP/IP Application Layer

The identification of security issues of the TCP/IP Application layer exposed various threats including the Man-in-the-Middle attacks, session hijacking, and unauthorized access Privacy concerns also exposed vulnerabilities in user-centric protocols within the TCP/IP application layer protocols. The security and privacy concerns in TCP/IP application layer protocols are discussed in the next session and summarized in Figure 10.

5.2.1. Performance, Security and Privacy Issues, With the Corresponding Countermeasures

Hyper Text Transfer Protocol (HTTP) and Web Applications in Browsers: In our daily internet communications, web browsers play a pivotal role, serving as the primary interface for interaction. The default communication protocol employed by web browsers is HTTP, facilitating the transfer of files constituting web pages from servers. However, this method involves plain text transfers, making it susceptible to intruders who can easily intercept and read the data packets [143], [144].

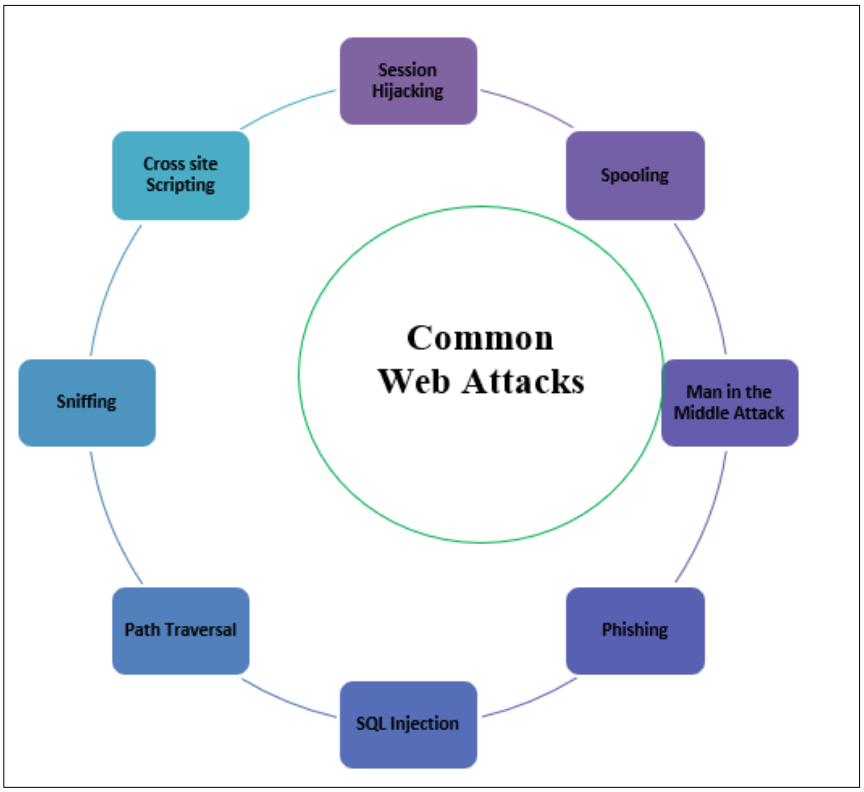

Figure 10 Common web-based attacks

To address this security concern, web browser developers have shifted to using HTTPS (Hyper Text Transfer Protocol Secure) instead of traditional HTTP. HTTPS incorporates a security protocol known as Secure Socket Layer (SSL), which ensures the encryption of data during transmission between the web server and the browser or web client. SSL utilizes public-key encryption to exchange a symmetric key between the client and the server, and this symmetric key is then employed to encrypt the entire HTTP transaction, encompassing both the request and the response. By implementing SSL within HTTP, the data becomes indecipherable to potential attackers attempting to eavesdrop through packet capturing tools. This security measure enables data to traverse even less secure networks while still maintaining its integrity and confidentiality. Figure 10 illustrates the common web-based attacks.

5.3. Security Concerns in Web Applications and Browsers

Caching Issues: Web browsers store temporary files from visited web pages in a cache on the user's machine for quick access [145] –[149]. This cache may include sensitive data like images, passwords, and usernames. If a user's computer is compromised, an attacker could access this information without authentication [150], raising privacy concerns. Regularly clearing the cache and disabling auto-saving of passwords in the browser can mitigate these risks.

Session Hijacking: Session hijacking [151] occurs when an attacker steals an HTTP session by intercepting and capturing packets using a packet sniffer [152]-[156]. Successful hijacking grants the attacker full access to the session, redirecting communication from the client to the web server to the attacker. Weak authentication during session initiation makes hijacking possible. Strengthening authentication measures is crucial to prevent such attacks [157]. Figure 11 and 12 show active and passive session hijacking states respectively.

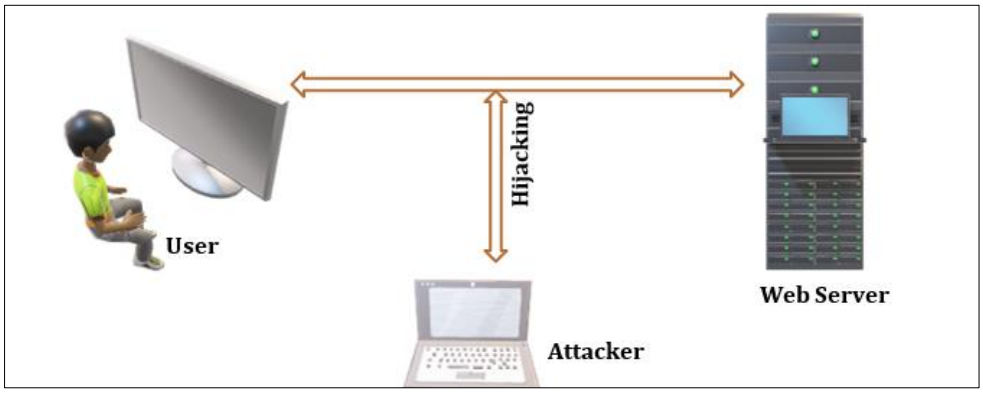

Figure 11 Active session hijacking state

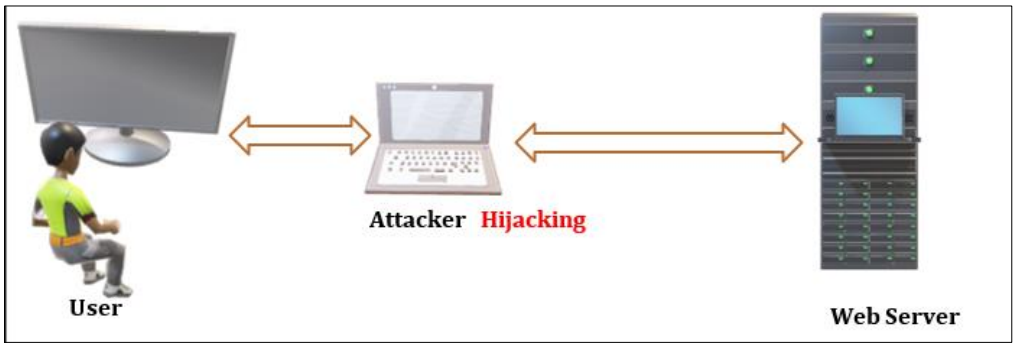

Figure 12 Passive session hijacking state

Cookie Poisoning: Cookies store session information to maintain user states and avoid repetitive logins. However, attackers may modify or steal cookies on a user's machine, compromising personal information [158], [159]. If an attacker gains access to a cookie containing login credentials, they can use it without further authentication. This poses a risk of unauthorized access and potential identity theft. Web Application Firewalls (WAF) play a crucial role in detecting and blocking cookie poisoning attacks by inspecting HTTP sessions and identifying parameters set in cookies issued by the web server [160], [161].

Replay Attack: A replay attack is a type of cyber-attack where an unauthorized user intercepts and retransmits data to the server [162]-[164]. In this scenario, the attacker doesn't just capture the data but can also modify it, leading to potentially different results than what the original sender intended [165]-[169]. Additionally, the attacker may spoof the client's IP address, redirecting their machine to an unintended destination. To mitigate replay attacks, it's crucial for web browsers to implement effective session tracking mechanisms that can discern legitimate from replayed traffic. Figure 13 shows a typical replay attack.

Cross-Site Scripting: Cross-Site Scripting (XSS) [170] is an attack where a malicious actor injects harmful code into a web application or browser, and this code is then executed on the client side [171].The primary objective of this attack is to hijack a user's session by stealing session tokens and cookies [172]-[176].

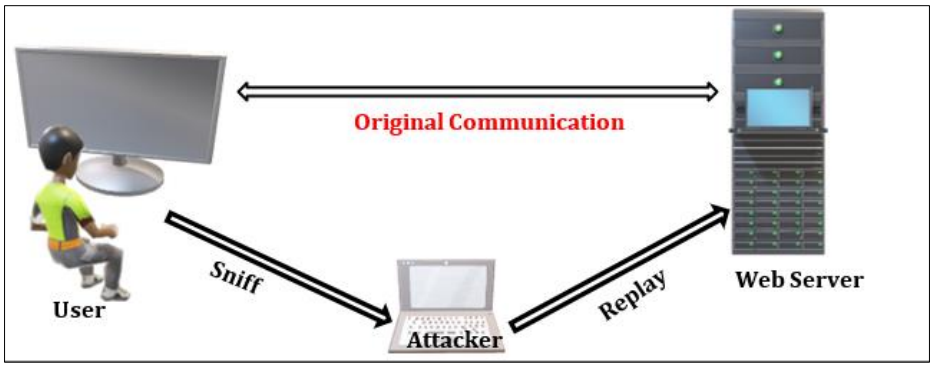

Figure 13 Replay attack

One way to defend against XSS attacks is to disable scripts from running on the website, but this approach may limit some features. Another strategy involves strengthening security controls, especially when dealing with cookie-based user authentication. Figure 14 shows the cross-site scripting (XSS).

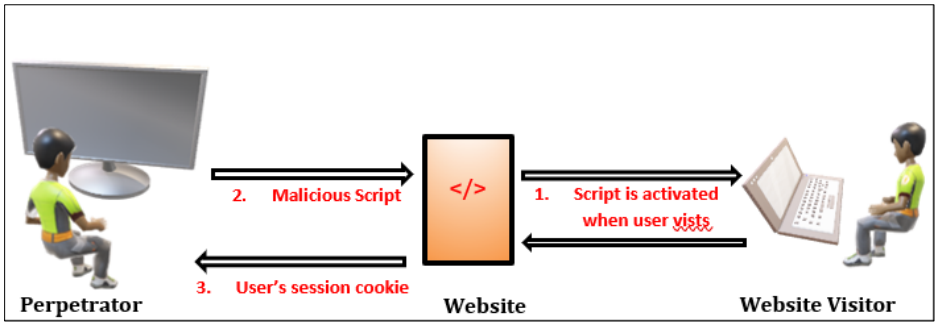

Figure 14 Cross-site scripting

Domain Name System: The Domain Name System (DNS) is a critical component of the internet that translates human-readable domain names into IP addresses [177]. Attackers may attempt to manipulate DNS records, leading to incorrect IP addresses and redirecting legitimate traffic to malicious servers. There are two common methods employed by attackers: protocol attacks and attacks on the DNS server.

DNS Protocol Attacks: DNS protocol attacks exploit vulnerabilities in the way DNS functions on a network [178]. Three prevalent types are DNS cache poisoning, DNS spoofing, and DNS ID hijacking. DNS cache poisoning involves manipulating the information stored in the DNS cache, providing incorrect name-to-IP mappings and diverting requests to malicious sites [179]. DNS spoofing entails faking the IP address of a computer to misdirect requests. DNS ID hijacking involves impersonating [180] a DNS server and responding to requests, leading to misdirection. Implementing patches and keeping DNS server operating systems up-to-date is essential in preventing these attacks, and DNS Security Extensions (DNSSEC) can add an extra layer of protection. Figure 15 demonstrates a DNS protocol attack.

Dynamic Host Configuration Protocol (DHCP): The Dynamic Host Configuration Protocol (DHCP) automatically assigns temporary IP addresses to client machines on an IP network [181]. As shown in Figure 16, an attacker can misuse this by launching a DHCP starvation attack, overwhelming the DHCP server with false requests and depleting its pool of available IP addresses [182]-[185].

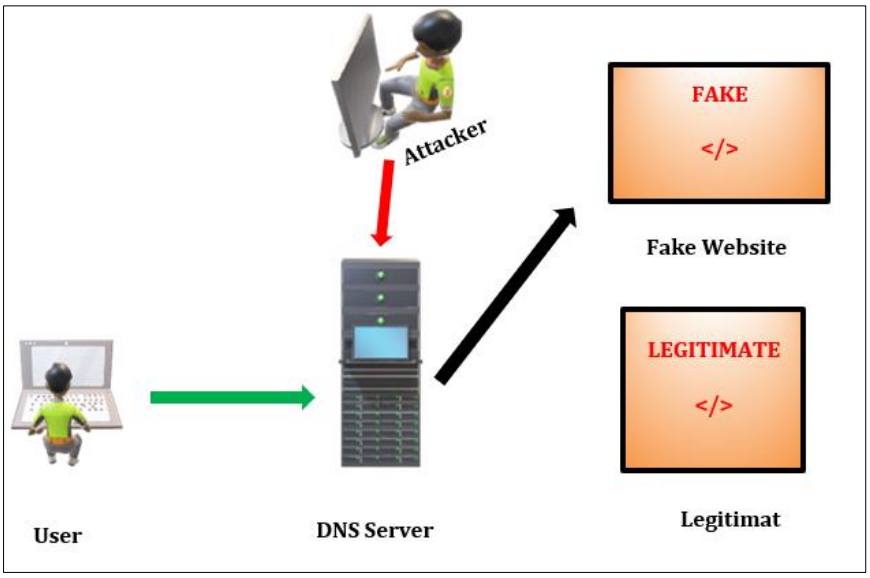

Figure 15 Sample DNS protocol attack

This results in a denial-of-service situation where legitimate users are unable to access the network. To prevent DHCP starvation, port security can be implemented, allowing only a specified number of MAC addresses per port, ensuring that the DHCP server can efficiently manage IP address allocations. Table 10 presents a summary of the common attacks at the application layer protocols.

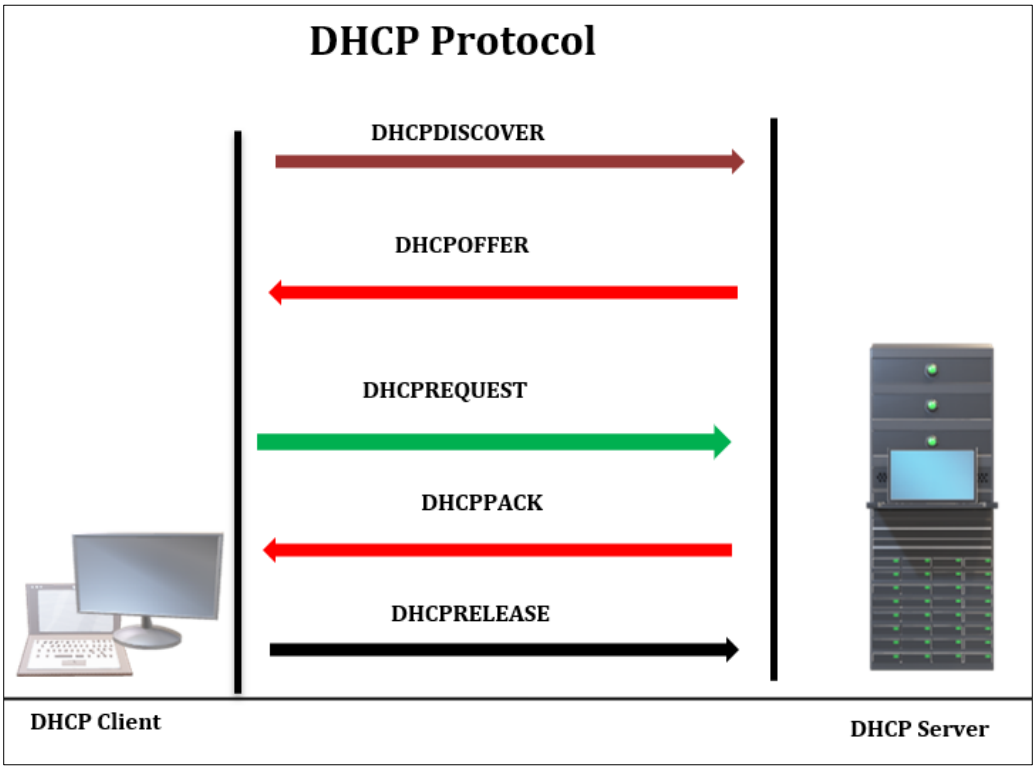

Figure 16 Sample DHCP Server and Client

Table 10 Summary of the common attacks at the application layer protocols.

S.No	Application Layer Protocol	Common Types of Attacks
1	HTTP	Cross-Site Scripting (XSS), SQL Injection HTTP Flood
2	HTTPS	SSL Stripping Session Hijacking
3	FTP	FTP Bounce Attack, FTP Injection
4	SMTP	Email Spoofing, Phishing
5	Telnet	Telnet Bruteforce, Man-In-The-Middle
6	DHCP	DHCP Spoofing DHCP Starvation
7	DNS	DNS Spoofing, DNS Cache Poisoning
8	IMAP	IMAP Brute Force, Email Spoofing
9	POP3	POP3 Bruteforce, Email Spoofing

6. Research Gaps and Future research areas

6.1. Research Gaps

Following the extensive review, our study identified research gaps within the TCP/IP application layer protocols with much focus on the performance, privacy and security concerns. While researchers have proposed numerous security measures to optimize the performance and enhance security and privacy in the application level protocols, significant privacy challenges in this layer remain unaddressed. In this study, limited studies were found addressing emerging technologies such as Internet of Things (IoT) and Machine Learning integration at the application layer. The need for standardized benchmarks for assessing performance, security and privacy metrics was also identified. Closing these research gaps will provide a more holistic understanding of the TCP/IP application layer landscape.

These gaps highlight the areas that require further investigation and attention to achieve optimized performance, robust and secure communication at the application level protocols. The research gaps that were identified and are detailed in Table 11.

Table 11 Summary of the Identified Research Gaps

Research Gap	Discussion
Privacy Challenges	Despite efforts to enhance security and privacy, significant privacy challenges persist within the TCP/IP application layer, warranting further investigation
Emerging Technologies Integration	Limited studies address the integration of emerging technologies such as Internet of Things (IoT) and Machine Learning at the application layer.
Standardized Benchmarks	There is a need for standardized benchmarks to assess performance, security, and privacy metrics consistently across TCP/IP application layer protocols.

6.2. Future Directions

Moving forward, future research in TCP/IP application layer protocol should focus on several key directions considering the identified issues to guide efforts towards robust improvement. Exploring the integration of emerging technologies such as the Internet of Things (IoT) and Machine Learning (ML). Advancements in cryptographic techniques and privacy-preserving mechanisms will be imperative to address evolving performance, privacy and security concerns in the TCP/IP application layer. Additionally, exploring innovative privacy-preserving protocols and utilizing adaptive security measures to counter evolving threats is also an area of future research. This will assist researchers and policymakers, decision makers to navigate the ever-evolving landscape of TCP/IP Application layer.

7. Conclusion

In conclusion, this survey explored the performance, privacy and security issues in the TCP/IP application layer. It explores the TCP/IP architecture and user-centric protocols at the application layer highlighting the performance, privacy and security issues in each protocol. The identified research gaps and proposed future areas of investigation serve as a roadmap for researchers, practitioners, decision makers and policymakers to address and mitigate these concerns effectively. Moving forward, prioritizing the development and implementation of robust protocols will be essential in strengthening the overall performance, security, and privacy of the TCP/IP model at the Application Layer hence ensuring a resilient and secure network environment for all stakeholders.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares no competing interests that might be perceived to influence the results and/or discussion reported in this paper.

Availability of Data and Materials

Data and materials used in this survey paper are either publicly available or referenced appropriately.

References

[1] Bellovin SM. Security problems in the TCP/IP protocol suite. ACM SIGCOMM Computer Communication Review. 1989 Apr 1;19(2):32-48.

[2] Zhao K, Zhang Q. Network protocol architectures for future deep-space internetworking. Science China Information Sciences. 2018 Apr; 61:1-6.

[3] Al-Khurafi OB, Al-Ahmad MA. Survey of web application vulnerability attacks. In2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT) 2015 Dec 8 (pp. 154-158). IEEE.

[4] Hossain MS, Paul A, Islam MH, Atiquzzaman M. Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. Netw. Protoc. Algorithms. 2018;10(1):83-108.

[5] Elewaily DI, Ali HA, Saleh AI, Abdelsalam MM. Delay/Disruption-Tolerant Networking-based the Integrated Deep-Space Relay Network: State-of-the-Art. Ad Hoc Networks. 2024 Jan 1; 152:103307.

[6] Hapanchak VS, Costa A, Pereira J, Nicolau MJ. An intelligent path management in heterogeneous vehicular networks. Vehicular Communications. 2024 Feb 1; 45:100690.

[7] Khashan OA, Khafajah NM, Alomoush W, Alshinwan M. Innovative energy-efficient proxy Re-encryption for secure data exchange in Wireless sensor networks. IEEE Access. 2024 Jan 31.

[8] Rahouma KH, Abdul-Karim MS, Nasr KS. TCP/IP Network Layers and Their Protocols (A Survey). InInternet of Things—Applications and Future: Proceedings of ITAF 2019 2020 (pp. 287-323). Springer Singapore.

[9] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[10] Bardhi E, Conti M, Lazzeretti R, Losiouk E. Security and Privacy of IP-ICN Coexistence: A Comprehensive Survey. IEEE Communications Surveys & Tutorials. 2023 Jul 13.

[11] Shaneel N. Improving Network Performance: An Evaluation of TCP/UDP on Networks. Department of Computing UNITEC Institute of Technology Auckland, New Zealand. 2014.

[12] Saleh AA, Simmons JM. Technology and architecture to enable the explosive growth of the internet. IEEE Communications Magazine. 2011 Jan 6;49(1):126-32.

[13] Anjum A, Agbaje P, Mitra A, Oseghale E, Nwafor E, Olufowobi H. Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication. Future Generation Computer Systems. 2023 Sep 27.

[14] Tang Q, Yu FR, Xie R, Boukerche A, Huang T, Liu Y. Internet of intelligence: A survey on the enabling technologies, applications, and challenges. IEEE Communications Surveys & Tutorials. 2022 May 16;24(3):1394-434.

[15] Kaur B, Dadkhah S, Shoeleh F, Neto EC, Xiong P, Iqbal S, Lamontagne P, Ray S, Ghorbani AA. Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet of Things. 2023 Apr 6:100780.

[16] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[17] Khaled AE, Helal S. Interoperable communication framework for bridging RESTful and topic-based communication in IoT. Future Generation Computer Systems. 2019 Mar 1;92:628-43.

[18] Corotinschi G, Găitan VG. Enabling IoT connectivity for Modbus networks by using IoT edge gateways. In2018 International Conference on Development and Application Systems (DAS) 2018 May 24 (pp. 175-179). IEEE.

[19] Görges M, Dumont GA, Petersen CL, Ansermino JM. Using machine-to-machine/“Internet of Things” communication to simplify medical device information exchange. In2014 International Conference on the Internet of Things (IOT) 2014 Oct 6 (pp. 49-54). IEEE.

[20] Karagiannis V, Chatzimisios P, Vazquez-Gallego F, Alonso-Zarate J. A survey on application layer protocols for the internet of things. Transaction on IoT and Cloud computing. 2015 Jan 1;3(1):11-7.

[21] Guner A, Kurtel K, Celikkan U. A message broker based architecture for context aware IoT application development. In2017 International Conference on Computer Science and Engineering (UBMK) 2017 Oct 5 (pp. 233-238). IEEE.

[22] Prabhu R, Rajesh S. A Effective Retrieval and Task Scheduling on Cloud Data Storage. Journal of Critical Reviews. 2020;7(8).

[23] Bajaj K, Sharma B, Singh R. Implementation analysis of IoT-based offloading frameworks on cloud/edge computing for sensor generated big data. Complex & Intelligent Systems. 2022 Oct;8(5):3641-58.

[24] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[25] Praseed A, Thilagam PS. DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. IEEE Communications Surveys & Tutorials. 2018 Sep 16;21(1):661-85.

[26] Arafat MY, Alam MM, Alam MF. A practical approach and mitigation techniques on application layer DDoS attack in web server. International Journal of Computer Applications. 2015;131(1):13-20.

[27] Jiang M, Wang C, Luo X, Miu M, Chen T. Characterizing the impacts of application layer DDoS attacks. In2017 IEEE International Conference on Web Services (ICWS) 2017 Jun 25 (pp. 500-507). IEEE.

[28] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[29] Singh K, Singh P, Kumar K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. Computers & security. 2017 Mar 1;65:344-72.

[30] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[31] Trevisan M, Soro F, Mellia M, Drago I, Morla R. Does domain name encryption increase users' privacy?. ACM SIGCOMM Computer Communication Review. 2020 Jul 22;50(3):16-22.

[32] Donta PK, Srirama SN, Amgoth T, Annavarapu CS. Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. Digital Communications and Networks. 2022 Oct 1;8(5):727-44.

[33] Karamollahi M, Williamson C. Characterization of IMAPS email traffic. In2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS) 2019 Oct 21 (pp. 214-220). IEEE.

[34] Wang Y, Zhou A, Liao S, Zheng R, Hu R, Zhang L. A comprehensive survey on DNS tunnel detection. Computer Networks. 2021 Oct 9;197:108322.

[35] Furfaro A, Pace P, Parise A. Facing DDoS bandwidth flooding attacks. Simulation Modelling Practice and Theory. 2020 Jan 1;98:101984.

[36] Rajendran B, Shetty P. Domain name system (dns) security: Attacks identification and protection methods. InProceedings of the International Conference on Security and Management (SAM) 2018 (pp. 27-33). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[37] Khormali A, Park J, Alasmary H, Anwar A, Saad M, Mohaisen D. Domain name system security and privacy: A contemporary survey. Computer Networks. 2021 Feb 11;185:107699.

[38] Li X, Xu W, Liu B, Zhang M, Li Z, Zhang J, Chang D, Zheng X, Wang C, Chen J, Duan H. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In2024 IEEE Symposium on Security and Privacy (SP) 2023 Oct 17 (pp. 46-46). IEEE Computer Society.

[39] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[40] Casanova LF, Lin PC. Generalized classification of DNS over HTTPS traffic with deep learning. In2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) 2021 Dec 14 (pp. 1903-1907). IEEE.

[41] Behnke M, Briner N, Cullen D, Schwerdtfeger K, Warren J, Basnet R, Doleck T. Feature engineering and machine learning model comparison for malicious activity detection in the dns-over-https protocol. IEEE Access. 2021 Sep 16;9:129902-16.

[42] Olamidipupo SA, Danas K. Review of interoperability techniques in data acquisition of wireless ECG devices. IOSR J. Mob. Comput. Appl. 2015;2(2):42-2394.

[43] Mavrogiorgou A, Kiourtis A, Perakis K, Pitsios S, Kyriazis D. IoT in healthcare: Achieving interoperability of high-quality data acquired by IoT medical devices. Sensors. 2019 Apr 27;19(9):1978.

[44] Ma Z. The Investigation of Communications Protocol. In2023 International Conference on Data Science, Advanced Algorithm and Intelligent Computing (DAI 2023) 2024 Feb 14 (pp. 576-582). Atlantis Press.

[45] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[46] Haseeb-Ur-Rehman RM, Aman AH, Hasan MK, Ariffin KA, Namoun A, Tufail A, Kim KH. High-Speed Network DDoS Attack Detection: A Survey. Sensors. 2023 Aug 1;23(15):6850.

[47] Alsabbagh W, Kim C, Langendörfer P. Silent Sabotage: A Stealthy Control Logic Injection in IIoT Systems. InSubmitted at the 5th Silicon Valley Cybersecurity Conference (SVCC 2024) 2024 Jun 17.

[48] Tariq U, Ahmed I, Bashir AK, Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors. 2023 Apr 19;23(8):4117.

[49] Al-Shareeda MA, Manickam S, Laghari SA, Jaisan A. Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications. Sustainability. 2022 Nov 29;14(23):15900.

[50] Sadiku MN, Akujuobi CM. The Internet. InFundamentals of Computer Networks 2022 Aug 30 (pp. 51-69). Cham: Springer International Publishing.

[51] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[52] Kharitonov A, Zimmermann A. WiP: Distributed Intrusion Detection System for TCP/IP-Based Connections in Industrial Environments Using Self-organizing Maps. InApplied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21–24, 2021, Proceedings 2021 (pp. 231-251). Springer International Publishing.

[53] Holguin I, Errapotu SM. Mitigating Common Cyber Vulnerabilities in DNP3 with Transport Layer Security. In2023 North American Power Symposium (NAPS) 2023 Oct 15 (pp. 1-6). IEEE.

[54] Alsabbagh W, Amogbonjaye S, Urrego D, Langendörfer P. A Stealthy False Command Injection Attack on Modbus based SCADA Systems. In2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) 2023 Jan 8 (pp. 1-9). IEEE.

[55] Zeghida H, Boulaiche M, Chikh R. Securing MQTT protocol for IoT environment using IDS based on ensemble learning. International Journal of Information Security. 2023 Mar 24:1-2.

[56] Csatár J, Péter G, Holczer T. Holistic attack methods against power systems using the IEC 60870-5-104 protocol. Infocommunications Journal. 2023;15(3):42-53.

[57] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[58] Pawar AB, Jawale MA, William P, Sonawane BS. Efficacy of TCP/IP Over ATM Architecture Using Network Slicing in 5G Environment. InSmart Data Intelligence: Proceedings of ICSMDI 2022 2022 Aug 18 (pp. 79-93). Singapore: Springer Nature Singapore.

[59] Kanellopoulos D, Sharma VK, Panagiotakopoulos T, Kameas A. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. Electronics. 2023 May 31;12(11):2490.

[60] Ravali P. A comparative evaluation of OSI and TCP/IP models. Int. J. Sci. Res. 2013;4(7):2319-7064.

[61] Martinović M, Lovaković D, Ćosić T. Network Security Issues in Regard to OSI Reference Model Layers. InProceedings of TEAM 2014 6 th International Scientific and Expert Conference of the International TEAM Society 10–11 th November 2014, Kecskemét, Hungary 2014 (p. 105).

[62] Tömösközi M, Reisslein M, Fitzek FH. Packet header compression: A principle-based survey of standards and recent research studies. IEEE Communications Surveys & Tutorials. 2022 Jan 19;24(1):698-740.

[63] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[64] Tran KT, Pham AX, Nguyen NP, Dang PT. Analysis and Performance Comparison of IoT Message Transfer Protocols Applying in Real Photovoltaic System. International Journal of Networked and Distributed Computing. 2024 Feb 23:1-3.

[65] Monnin M, Sussman LL. Turnstile File Transfer: A Unidirectional System for Medium-Security Isolated Clusters. Journal of Cybersecurity Education, Research and Practice. 2023;2024(1):12.

[66] Sharp R. Network Security. InIntroduction to Cybersecurity: A Multidisciplinary Challenge 2023 Oct 13 (pp. 171-233). Cham: Springer Nature Switzerland.

[67] Buitrago López A, Pastor-Galindo J, Gómez Mármol F. Updated exploration of the Tor network: advertising, availability and protocols of onion services. Wireless Networks. 2024 Feb 25:1-5.

[68] Manthiramoorthy C, Khan KM. Comparing several encrypted cloud storage platforms. International Journal of Mathematics, Statistics, and Computer Science. 2024;2:44-62.

[69] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[70] Wei P, Hong Z, Shi M. Performance analysis of HTTP and FTP based on OPNET. In2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS) 2016 Jun 26 (pp. 1-4). IEEE.

[71] Katis T, Kaskalis T. Autonomous robotic platform for comprehensive environmental monitoring and mapping: Design, implementation, and integration. InAIP Conference Proceedings 2024 Feb 21 (Vol. 3063, No. 1). AIP Publishing.

[72] Bhoi SK, Ghugar U, Dash S, Nayak R, Bagal DK. Exploring The Security Landscape: A Comprehensive Analysis Of Vulnerabilities, Challenges, And Findings In Internet Of Things (Iot) Application Layer Protocols. Migration Letters. 2024 Feb 17;21(S6):1326-42.

[73] Zahid R, Altaf A, Ahmad T, Iqbal F, Vera YA, Flores MA, Ashraf I. Secure data management life cycle for government big-data ecosystem: Design and development perspective. Systems. 2023 Jul 25;11(8):380.

[74] Dawood M, Tu S, Xiao C, Alasmary H, Waqas M, Rehman SU. Cyberattacks and security of cloud computing: a complete guideline. Symmetry. 2023 Oct 26;15(11):1981.

[75] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[76] Gupta V, Wurm M. The energy cost of ssl in deeply embedded systems. Technical report Sun Microsystems, TR-2008-173, June 2008.

[77] Naylor D, Finamore A, Leontiadis I, Grunenberger Y, Mellia M, Munafò M, Papagiannaki K, Steenkiste P. The cost of the" s" in https. InProceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies 2014 Dec 2 (pp. 133-140).

[78] Kamel M, Boudaoud K, Resondry S, Riveill M. A low-energy consuming and user-centric security management architecture adapted to mobile environments. In12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops 2011 May 23 (pp. 722-725). IEEE.

[79] Cao Z, Xiong G, Zhao Y, Li Z, Guo L. A survey on encrypted traffic classification. InApplications and Techniques in Information Security: 5th International Conference, ATIS 2014, Melbourne, VIC, Australia, November 26-28, 2014. Proceedings 5 2014 (pp. 73-81). Springer Berlin Heidelberg.

[80] Kizza JM. Computer network security protocols. InGuide to Computer Network Security 2024 Jan 20 (pp. 409-441). Cham: Springer International Publishing.

[81] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70

[82] Taherdoost H. E-Business Security and Control. InE-Business Essentials: Building a Successful Online Enterprise 2023 Sep 5 (pp. 105-135). Cham: Springer Nature Switzerland.

[83] Albshaier L, Almarri S, Hafizur Rahman MM. A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. Computers. 2024 Jan 17;13(1):27.

[84] Daah C, Qureshi A, Awan I, Konur S. Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. Electronics. 2024 Feb 23;13(5):865.

[85] Hartanto F, Budiman B, Gwei E, Gunawan AA, Edbert IS. An Experiment to Prevent Malicious Actors from Compromising Private Digital Assets Over a Public Network. Engineering, MAthematics and Computer Science Journal (EMACS). 2024 Jan 31;6(1):7-11.

[86] Shankar SP, Gudadinni SM, Mohta R. A Comprehensive Study of Cyber Threats in the Banking Industry. InStrengthening Industrial Cybersecurity to Protect Business Intelligence 2024 (pp. 244-269). IGI Global.

[87] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[88] Rao PM, Deebak BD. A Comprehensive Survey on Authentication and Secure Key Management in Internet of Things: Challenges, Countermeasures, and Future Directions. Ad Hoc Networks. 2023 Mar 23:103159.

[89] Ghaffari F, Bertin E, Crespi N, Hatin J. Distributed ledger technologies for authentication and access control in networking applications: A comprehensive survey. Computer Science Review. 2023 Nov 1;50:100590.

[90] Surti M, Shah V, Makadiya Y, Shah K, Padhya M. Exploring Cyber Security Issues in the Internet of Healthcare Things (IoHT) with Potential Improvements. InInformation and Communication Technology for Competitive Strategies (ICTCS 2022) Intelligent Strategies for ICT 2023 May 16 (pp. 569-585). Singapore: Springer Nature Singapore.

[91] Sasaki T, Fujita A, Ganán CH, van Eeten M, Yoshioka K, Matsumoto T. Exposed infrastructures: Discovery, attacks and remediation of insecure ics remote management devices. In2022 IEEE Symposium on Security and Privacy (SP) 2022 May 22 (pp. 2379-2396). IEEE.

[92] Basholli F, Daberdini A. Security in telecommunication networks and systems. InInternational Interdisciplinary Conference" The role of Technology in the Shaping of Society 2022 (Vol. 72).

[93] Preetha M, Dhabliya D, Lone ZA, Pandey S, Acharjya K, Gowrishankar J. An Assessment of the Security Benefits of Secure Shell (SSH) in Wireless Networks. In2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) 2023 Dec 29 (pp. 1-6). IEEE.

[94] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[95] Glăvan D, Răcuciu C, Moinescu R, Eftimie S. Man in the middle attack on HTTPS protocol. Scientific Bulletin" Mircea cel Batran" Naval Academy. 2020;23(1):199A-201.

[96] Michelena A, Aveleira-Mata J, Jove E, Bayón-Gutiérrez M, Novais P, Romero OF, Calvo-Rolle JL, Aláiz-Moretón H. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems. 2024 Feb;41(2):e13263.

[97] Kambourakis G, Gil GD, Sanchez I. What email servers can tell to Johnny: an empirical study of provider-to-provider email security. IEEE Access. 2020 Jul 14;8:130066-81.

[98] Liu E, Akiwate G, Jonker M, Mirian A, Savage S, Voelker GM. Who's got your mail? characterizing mail service provider usage. InProceedings of the 21st ACM Internet Measurement Conference 2021 Nov 2 (pp. 122-136).

[99] Gavrilovic N, Ciric V. Design and evaluation of proof of work based anti-spam solution. In2020 Zooming Innovation in Consumer Technologies Conference (ZINC) 2020 May 26 (pp. 286-289). IEEE.

[100] Gellens R, Newman C, Yao J, Fujiwara K. Post Office Protocol Version 3 (POP3) Support for UTF-8. 2013 Mar.

[101] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[102] Vijayalakshmi N, Sivajothi E, Vivekanandan DP. efficiency and limitation of secure protocol in email services. International Journal of Engineering Sciences and Research Technology, pp-539-544. 2012 Nov.

[103] Banday MT. Effectiveness and limitations of e-mail security protocols. International Journal of Distributed and Parallel Systems (IJDPS) Vol. 2011 May;2.

[104] Mohamed G, Mohideen M, Banu S. E-Mail Phishing–An open threat to everyone. International Journal of Scientific and Research Publication. 2014;4(2):1-4.

[105] Singh SP, Goyal N. Security configuration and performance analysis of ftp server. International Journal of communication and computer Technologies. 2014;2(2):106-9.

[106] Ding J. A File Transfer Method Based on Modbus Protocol. In2023 8th International Conference on Power and Renewable Energy (ICPRE) 2023 Sep 22 (pp. 2029-2033). IEEE.

[107] Mohamed NN, Mohd Yussoff Y, Mat Isa MA, Hashim H. Extending hybrid approach to secure Trivial File Transfer Protocol in M2M communication: a comparative analysis. Telecommunication Systems. 2019 Apr 15;70:511-23.

[108] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[109] Osanaiye OA, Dlodlo M. TCP/IP header classification for detecting spoofed DDoS attack in Cloud environment. InIEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON) 2015 Sep 8 (pp. 1-6). IEEE.

[110] Naik N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In2017 IEEE international systems engineering symposium (ISSE) 2017 Oct 11 (pp. 1-7). IEEE.

[111] Salman T, Jain R. A survey of protocols and standards for internet of things. arXiv preprint arXiv:1903.11549. 2019 Feb 10.

[112] Kayal P, Perros H. A comparison of IoT application layer protocols through a smart parking implementation. In2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN) 2017 Mar 7 (pp. 331-336). IEEE.

[113] Mijovic S, Shehu E, Buratti C. Comparing application layer protocols for the Internet of Things via experimentation. In2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI) 2016 Sep 7 (pp. 1-5). IEEE.

[114] Muzammil MB, Bilal M, Ajmal S, Shongwe SC, Ghadi YY. Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. IEEE Access. 2024 Jan 5.

[115] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland

[116] Bhowmik R, Riaz MH. An extended review of the application layer messaging protocol of the internet of things. Bulletin of Electrical Engineering and Informatics. 2023 Jun 15;12(5):3124-33.

[117] Kemp C, Calvert C, Khoshgoftaar TM, Leevy JL. An approach to application-layer DoS detection. Journal of Big Data. 2023 Feb 13;10(1):22.

[118] Nebbione G, Calzarossa MC. Security of IoT application layer protocols: Challenges and findings. Future Internet. 2020 Mar 17;12(3):55.

[119] Hamid HG, Alisa ZT. A survey on IoT application layer protocols. Indonesian Journal of Electrical Engineering and Computer Science. 2021 Mar;21(3):1663-72.

[120] Nyangaresi VO, Ogara SO, Abeka SO. TCP IP header attack vectors and countermeasures. American Journal of Science Engineering and Technology, 2, 39–49.

[121] Abdullah S. Enhancing the TCP Newreno Fast RecoveryAlgorithm on 5G Networks. Journal of Computing and Communication. 2024 Jan 31;3(1):33-43.

[122] Maschi F, Alonso G. Strega: An HTTP Server for FPGAs. ACM Transactions on Reconfigurable Technology and Systems. 2024 Jan 27;17(1):1-27.

[123] Kushwaha SK, Jain SK. NMFLRED: Neuro-Multilevel-Fuzzy Logic RED Approach for Congestion Control in TCP/IP Differentiated Services. International Journal of Intelligent Systems and Applications in Engineering. 2024;12(2):674-85.

[124] Boeding M, Scalise P, Hempel M, Sharif H, Lopez Jr J. Toward Wireless Smart Grid Communications: An Evaluation of Protocol Latencies in an Open-Source 5G Testbed. Energies. 2024 Jan 11;17(2):373.

[125] Mishra S, Jain VK, Gyoda K, Jain S. An efficient content replacement policy to retain essential content in information-centric networking based internet of things network. Ad Hoc Networks. 2024 Mar 15;155:103389.

[126] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[127] Dai L, Qi H, Chen W, Lu X. High-Speed Data Communication with Advanced Networks in Large Language Model Training. IEEE Micro. 2024 Jan 30.

[128] Ni Z, You J, Li Y. An ICN-Based On-Path Computing Resource Scheduling Architecture with User Preference Awareness for Computing Network. Electronics. 2024 Feb 29;13(5):933.

[129] Botirov SR. Analysis of the characteristics of cloud infrastructure based on traditional technologies and SDN technologies. InArtificial Intelligence, Blockchain, Computing and Security Volume 2 2024 (pp. 700-705). CRC Press.

[130] Liu H, Ni H, Han R. A Link Status-Based Multipath Scheduling Scheme on Network Nodes. Electronics. 2024 Feb 1;13(3):608.

[131] Aruna R, Kushwah VS, Praveen SP, Pradhan R, Chinchawade AJ, Asaad RR, Kumar RL. Coalescing novel QoS routing with fault tolerance for improving QoS parameters in wireless Ad-Hoc network using craft protocol. Wireless Networks. 2023 Oct 4:1-25.

[132] Glazkov R, Moltchanov D, Srikanteswara S, Samuylov A, Arrobo G, Zhang Y, Feng H, Himayat N, Spoczynski M, Koucheryavy Y. Provisioning of Fog Computing over Named-Data Networking in Dynamic Wireless Mesh Systems. Sensors. 2024 Feb 8;24(4):1120.

[133] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[134] Djaker AB, Kechar B, Afifi H, Moungla H. Maximum Concurrent Flow Solutions for Improved Routing in IoT Future Networks. Arabian Journal for Science and Engineering. 2023 Aug;48(8):10079-98.

[135] Pan Y, Rossow C. TCP Spoofing: Reliable Payload Transmission Past the Spoofed TCP Handshake. In2024 IEEE Symposium on Security and Privacy (SP) 2024 Feb 1 (pp. 179-179). IEEE Computer Society.

[136] Börger E, Gervasi V. Mixed Synchronous/Asynchronous Control Structures. InStructures of Computing: A Guide to Practice-Oriented Theory 2024 Mar 2 (pp. 151-179). Cham: Springer International Publishing.

[137] Singh SP, Chakrabarti S, Shukla D, Terzija V. Development and implementation of a MATLAB-based phasor data concentrator for synchrophasor applications. International Journal of Electrical Power & Energy Systems. 2024 Jan 1;155:109637.

[138] Ghazo AT, Kumar R. ANDVI: Automated Network Device and Vulnerability Identification in SCADA/ICS by Passive Monitoring. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2024 Jan 15.

[139] Găitan VG, Zagan I. Modbus Extension Server Implementation for BIoT-Enabled Smart Switch Embedded System Device. Sensors. 2024 Jan 12;24(2):475.

[140] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[141] Liu N, Gao S, Hou X, Liang T, He G, Zhang H, Das SK. An ICN-Based Secure Task Cooperation in Challenging Wireless Edge Networks. IEEE Transactions on Network and Service Management. 2024 Jan 2.

[142] Dhadhania A, Bhatia J, Mehta R, Tanwar S, Sharma R, Verma A. Unleashing the power of SDN and GNN for network anomaly detection: State-of-the-art, challenges, and future directions. Security and Privacy. 2024 Jan;7(1):e337.

[143] Kampourakis V, Kambourakis G, Chatzoglou E, Zaroliagis C. Revisiting man-in-the-middle attacks against HTTPS. Network Security. 2022 Mar;2022(3).

[144] Khare R, Lawrence S. Upgrading to TLS within HTTP/1.1. 2000 May.

[145] Cuesta B, Ros A, Gomez ME, Robles A, Duato J. Increasing the effectiveness of directory caches by avoiding the tracking of noncoherent memory blocks. IEEE Transactions on Computers. 2011 Dec 20;62(3):482-95.

[146] Kowarschik M, Weiß C. An overview of cache optimization techniques and cache-aware numerical algorithms. Algorithms for memory hierarchies: advanced lectures. 2003 Feb 28:213-32.

[147] Álvarez JD, Risco-Martín JL, Colmenar JM. Multi-objective optimization of energy consumption and execution time in a single level cache memory for embedded systems. Journal of Systems and Software. 2016 Jan 1;111:200-12..

[148] Fang Z, Zhao L, Jiang X, Lu SL, Iyer R, Li T, Lee SE. Reducing cache and TLB power by exploiting memory region and privilege level semantics. Journal of Systems Architecture. 2013 Jun 1;59(6):279-95.

[149] Maniotis P, Gitzenis S, Tassiulas L, Pleros N. An optically-enabled chip–multiprocessor architecture using a single-level shared optical cache memory. Optical Switching and Networking. 2016 Nov 1;22:54-68.

[150] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[151] Kamal P. State of the art survey on session hijacking. Global Journal of Computer Science and Technology. 2016 Mar;16(1):39-49.

[152] Rupal DR, Satasiya D, Kumar H, Agrawal A. Detection and prevention of ARP poisoning in dynamic IP configuration. In2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) 2016 May 20 (pp. 1240-1244). IEEE.

[153] Balogh Z, Koprda Š, Francisti J. LAN security analysis and design. In2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT) 2018 Oct 17 (pp. 1-6). IEEE.

[154] Elamaran V, Arunkumar N, Babu GV, Balaji VS, Gomez J, Figueroa C, Ramirez-González G. Exploring DNS, HTTP, and ICMP response time computations on brain signal/image databases using a packet sniffer tool. IEEE Access. 2018 Sep 16;6:59672-8.

[155] Levi M, Hazan I. User profiling using sequential mining over web elements. In2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS) 2019 Sep 23 (pp. 1-6). IEEE.

[156] Araujo F, Taylor T, Zhang J, Stoecklin M. Cross-stack threat sensing for cyber security and resilience. In2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) 2018 Jun 25 (pp. 18-21). IEEE.

[157] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[158] Dalipi F, Yayilgan SY. Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) 2016 Aug 22 (pp. 63-68). IEEE.

[159] Papadogiannakis E, Papadopoulos P, Kourtellis N, Markatos EP. User tracking in the post-cookie era: How websites bypass gdpr consent to track users. InProceedings of the web conference 2021 2021 Apr 19 (pp. 2130-2141).

[160] Jegatheesan S. Cookies Invading Our Privacy for Marketing Advertising and Security Issues. arXiv preprint arXiv:1305.2306. 2013 May 10..

[161] Bless C, Dötlinger L, Kaltschmid M, Reiter M, Kurteva A, Roa-Valverde AJ, Fensel A. Raising awareness of data sharing consent through knowledge graph visualisation. InFurther with Knowledge Graphs 2021 (Vol. 53, pp. 44-57).

[162] Mallikarachchi D, Wong K, Lim JM. A message verification scheme based on physical layer-enabled data hiding for flying ad hoc network. Multimedia Tools and Applications. 2024 Feb 23:1-21.

[163] Alyahya S, Khan WU, Ahmed S, Marwat SN, Habib S. Cyber secure framework for smart agriculture: Robust and tamper-resistant authentication scheme for IoT devices. Electronics. 2022 Mar 21;11(6):963.

[164] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[165] Malladi S, Alves-Foss J, Heckendorn RB. On preventing replay attacks on security protocols. InProc. International Conference on Security and Management 2002 Jun (Vol. 6).

[166] Le A, Loo J, Chai KK, Aiash M. A specification-based IDS for detecting attacks on RPL-based network topology. Information. 2016 May 12;7(2):25.

[167] Verma A, Ranga V. Comment on “DIO Suppression Attack Against Routing in the Internet of Things”. Authorea Preprints. 2023 Oct 30.

[168] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019 Nov 13;22(1):616-44.

[169] Bang AO, Rao UP, Kaliyar P, Conti M. Assessment of routing attacks and mitigation techniques with RPL control messages: A survey. ACM Computing Surveys (CSUR). 2022 Jan 18;55(2):1-36.

[170] Alqarni AA, Alsharif N, Khan NA, Georgieva L, Pardade E, Alzahrani MY. MNN-XSS: Modular Neural Network Based Approach for XSS Attack Detection. Computers, Materials & Continua. 2022 Feb 1;70(2).

[171] Nithya V, Pandian SL, Malarvizhi C. A survey on detection and prevention of cross-site scripting attack. International Journal of Security and Its Applications. 2015 Mar 1;9(3):139-52.

[172] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[173] Abaimov S, Bianchi G. CODDLE: Code-injection detection with deep learning. IEEE Access. 2019 Sep 13;7:128617-27.

[174] Akay B, Karaboga D, Akay R. A comprehensive survey on optimizing deep learning models by metaheuristics. Artificial Intelligence Review. 2022 Feb 1:1-66.

[175] Akrout R, Alata E, Kaaniche M, Nicomette V. An automated black box approach for web vulnerability identification and attack scenario generation. Journal of the Brazilian Computer Society. 2014 Dec;20:1-6.

[176] Hoffman P, McManus P. DNS queries over HTTPS (DoH). Internet Engineering Task Force (IETF). 2018 Oct.

[177] Aggarwal A, Kumar M. An ensemble framework for detection of DNS-Over-HTTPS (DOH) traffic. Multimedia Tools and Applications. 2023 Sep 25:1-28.

[178] Kim TH, Reeves D. A survey of domain name system vulnerabilities and attacks. Journal of Surveillance, Security and Safety. 2020 Sep;1(1):34-60.

[179] Li X, Xu W, Liu B, Zhang M, Li Z, Zhang J, Chang D, Zheng X, Wang C, Chen J, Duan H. TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets. In2024 IEEE Symposium on Security and Privacy (SP) 2023 Oct 17 (pp. 46-46). IEEE Computer Society.

[180] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[181] Ramprasad R, Narayanan J, Balaji D, Kishor S. A DHCP Based Approach To IP Address Management And Allocation In A Network Using VLSM. In2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) 2023 Mar 17 (Vol. 1, pp. 882-887). IEEE.

[182] Tripathi N, Hubballi N. Exploiting DHCP server-side IP address conflict detection: A DHCP starvation attack. In2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS) 2015 Dec 15 (pp. 1-3). IEEE.

[183] De Graaf K, Liddy J, Raison P, Scano JC, Wadhwa S, inventors; Juniper Networks Inc, assignee. Dynamic host configuration protocol (DHCP) authentication using challenge handshake authentication protocol (CHAP) challenge. United States patent US 8,555,347. 2013 Oct 8.

[184] Ju H, Han J. DHCP message authentication with an effective key management. International Journal of Computer and Information Engineering. 2007 Aug 28;1(8):1199-202.

[185] Komori T, Saito T. The secure DHCP system with user authentication. In27th Annual IEEE Conference on Local Computer Networks, 2002. Proceedings. LCN 2002. 2002 Nov 6 (pp. 123-131). IEEE.