World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Survey on evolving threats in TCP/IP header attacks: Emerging trends and future directions

Winnie Owoko *

Department of Computer Science and Software Engineering, Jaramogi Odinga Oginga University of Science and Technology, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(02), 454–475

Publication history: Received on 02 March 2024; revised on 13 April 2024; accepted on 16 April 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.2.0127

Abstract

The TCP/IP protocol suite, a cornerstone of modern networking, faces escalating threats from evolving attack vectors targeting its headers. This survey explores emerging trends in TCP/IP header attacks, assessing their potential impact and outlining future directions for defense strategies. By scrutinizing recent research and real-world incidents, the paper aims to offer insights into the evolving threat landscape and provide recommendations for enhancing network security. Key areas of investigation include the historical evolution of TCP/IP header vulnerabilities, the adaptation of attackers' techniques over time, and the development of novel defense mechanisms to counteract these threats. The survey underscores the critical importance of understanding TCP/IP header attacks in contemporary cybersecurity and highlights the necessity for proactive measures to safeguard network infrastructures. By addressing the challenges posed by evolving TCP/IP header attacks and identifying areas for further research and development, this survey contributes to the ongoing efforts to strengthen network defenses and mitigate the risks associated with cyber threats targeting TCP/IP protocols.

Keywords: TCP/IP headers; Network security; Emerging threats; Attack vectors; Defense strategies.

1. Introduction

The TCP/IP protocol suite, also known as the Internet Protocol Suite, is a fundamental collection of networking protocols that facilitate the transfer of data packets across computer networks [1]. At its core, TCP/IP comprises various protocols, with Transmission Control Protocol (TCP) and Internet Protocol (IP) serving as the foundational components [2]. IP addresses and routes network packets, akin to road networks connecting cities, while TCP, a connection-oriented protocol, ensures reliable data packet delivery between systems [3]-[6]. This suite plays a pivotal role in modern networking by providing a standardized framework for communication and data exchange over the internet. Understanding TCP/IP is crucial for network administrators and engineers as it forms the backbone of internet communication, enabling seamless data transmission [7] and connectivity across diverse devices and systems.

The concept of TCP/IP header attacks plays a significant role in contemporary cybersecurity as cyber attackers exploit vulnerabilities in the TCP/IP protocol suite to launch sophisticated attacks. According to [8], TCP/IP header attacks have become a prevalent method for cybercriminals to manipulate packet headers and bypass network security measures. These attacks target the header fields of TCP/IP packets, allowing attackers to spoof IP addresses, perform packet injection, and conduct other malicious activities. As highlighted in [9], understanding these attacks is crucial for developing effective defense mechanisms to protect network infrastructures from potential threats. By analyzing and detecting anomalies in TCP/IP headers, security professionals can enhance their incident response capabilities and mitigate the risks posed by such attacks in today's interconnected digital landscape [10]-[12].

* Corresponding author: Winnie Owoko

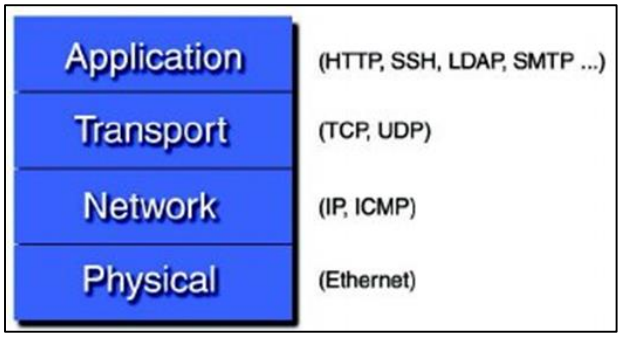

Figure 1 TCP/IP Protocol Suite

As explained in [13], threats in TCP/IP header attacks pose significant risks to network security, primarily due to their ability to manipulate crucial information within network packets. These attacks exploit vulnerabilities in the TCP/IP protocol stack, allowing malicious actors to intercept, modify [14], or fabricate packet headers, leading to various security breaches. One common threat is the TCP/IP sequence number prediction attack, where attackers exploit the predictable nature of sequence numbers to hijack established connections or launch session hijacking attacks, compromising data confidentiality and integrity. Another significant threat is the TCP SYN flood attack, where attackers flood a target server with a barrage of spoofed SYN packets, exhausting its resources and rendering it unable to process legitimate requests [15]-[19]. This form of Denial of Service (DoS) attack disrupts network services, causing downtime and financial losses for organizations. Additionally, TCP/IP header attacks can be leveraged to conduct reconnaissance, evade intrusion detection systems, and initiate advanced persistent threats, making them a persistent and evolving concern for network security professionals. Mitigating these threats requires implementing robust security measures [20], such as packet filtering, encryption, intrusion detection systems, and regular security audits, to safeguard against potential vulnerabilities in the TCP/IP protocol stack.

2. Contributions

The study aims to provide an in-depth exploration of the evolving landscape of TCP/IP header attacks, drawing upon the insights and research findings presented in the references. By synthesizing the historical evolution of TCP/IP vulnerabilities and the adaptation of attackers' techniques over time, the study will analyze the impact of these attacks on network security and the implications for organizations. Through a comprehensive examination of case studies and real-world examples of TCP/IP header attacks, the study will elucidate the practical consequences faced by entities targeted by cyber threats exploiting TCP/IP vulnerabilities. Furthermore, the study will delve into the significance of understanding TCP/IP header attacks in contemporary cybersecurity and the critical role of proactive defense strategies in safeguarding network infrastructures. By analyzing the attack techniques employed by cybercriminals, such as IP spoofing, TCP sequence number prediction, and packet injection, the study aim to shed light on the sophisticated methods used to compromise network integrity and data confidentiality. Additionally, the study will explore the challenges posed by covert channel data exfiltration and ARP spoofing, emphasizing the need for robust defense mechanisms to counteract these threats effectively. Moreover, the study will discuss the evolution of cyber-attacks targeting TCP/IP headers, highlighting the persistent nature of vulnerabilities in the TCP/IP protocol suite. By examining the historical context of TCP/IP header attacks, including incidents like the Morris worm and the exploitation of covert channels for data exfiltration, the study will underscore the ongoing challenges faced by cybersecurity professionals in mitigating these risks. Through a detailed analysis of the impact of TCP/IP header attacks on organizations and networks, the study provides valuable insights into the practical implications of these threats and the imperative need for continuous research and development in TCP/IP header security.

3. Evolution of TCP/IP header attacks

TCP/IP header attacks have a rich historical background marked by notable incidents and vulnerabilities that have shaped the cybersecurity landscape. Figure 2 and Figure 3 show the TCP and IP headers respectively. Recent research in [21] emphasizes the inherent security flaws in the TCP/IP protocol suite, dating back to the early days of the Internet with incidents like the Morris worm. This worm demonstrated the protocol's susceptibility to exploitation due to its design parameters that prioritized reliability over security. Building on this foundation, author in [22] showcased the weaknesses in TCP/IP headers for covert channel data exfiltration, highlighting the ongoing challenges in securing these critical components of network communication. The study further underscores the continued relevance of TCP/IP header attacks in contemporary cyber threats, with hackers leveraging techniques such as address spoofing and TCP

sequence number prediction to compromise network integrity. These historical insights underscore the persistent nature of TCP/IP vulnerabilities and the need for proactive defense mechanisms to safeguard against evolving cyber risks. Table 1 presents a structured overview of key historical incidents and vulnerabilities in TCP/IP header attacks.

Over time, cyber attackers have continuously evolved their attack techniques to exploit new vulnerabilities and circumvent existing defenses, posing significant challenges to cybersecurity professionals [23]-[25].

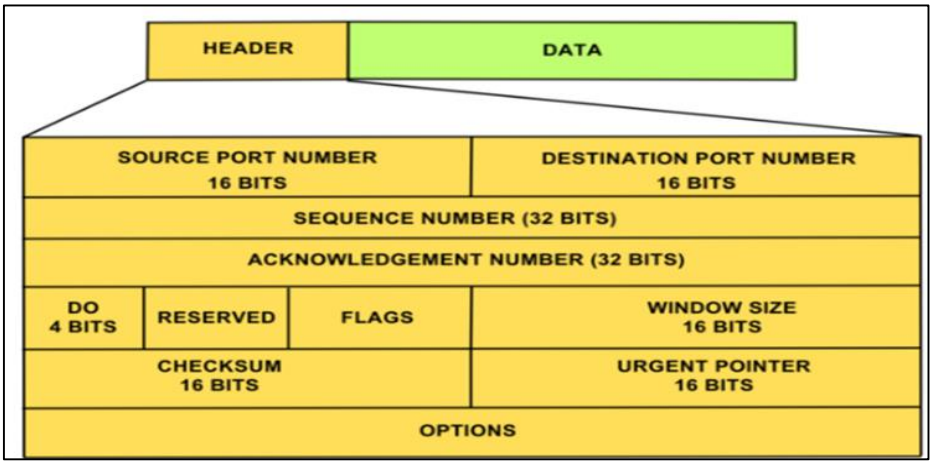

Figure 2 TCP header

Research in [13], highlights the evolution of cyber attacks, demonstrating how methods of spreading attacks have changed, including the exploitation of vulnerabilities in hardware, software, and networks. This evolution is further exemplified by the rise of new attack tools that enable cybercriminals to access sensitive data, encrypt computer data, and launch DDoS attacks [26], costing billions of dollars annually [27]-[29]. Additionally, the study in [21] emphasizes the persistent nature of TCP/IP vulnerabilities, with attackers leveraging techniques like address spoofing and TCP sequence number prediction to compromise network security.

Figure 3 IP header

Furthermore, recent advancements in attack patterns and evasion techniques have rendered traditional defense mechanisms ineffective, necessitating innovative solutions to combat sophisticated cyber threats. By leveraging technologies such as machine learning, deep learning, and blockchain, organizations can enhance their ability to detect malware, intrusion attempts, and other advanced persistent threats [29]-[32].

According to [33], the evolution of TCP/IP header attacks mirrors the advancements in networking technology and the increasing sophistication of cyber threats. Initially, TCP/IP header attacks were relatively simple, often involving basic techniques like IP spoofing or SYN flooding. These attacks primarily targeted vulnerabilities in the TCP/IP protocol stack, exploiting weaknesses in packet header fields to disrupt network communications or compromise system integrity [34]-[37]. As network security measures improved, attackers adapted by developing more sophisticated methods to evade detection and bypass security controls. One significant evolution in TCP/IP header attacks is the emergence of stealthier techniques such as TCP sequence number prediction and session hijacking. Attackers leverage the predictable nature of TCP sequence numbers to intercept and manipulate network connections [38], enabling them

to eavesdrop on communication sessions or inject malicious payloads into data streams without arousing suspicion. These attacks pose serious threats to data confidentiality and integrity, as attackers can silently compromise sensitive information or compromise critical systems without leaving obvious traces.

Table 1 Historical overview of significant incidents and vulnerabilities related to TCP/IP header attacks

Incident/Vulnerability	Description	Year	Effect	Attack Technique	Examples
Morris Worm	Self-replicating program exploiting TCP/IP vulnerabilities, causing widespread disruptions	1988	Highlighted security flaws in TCP/IP implementations	Self-replicating malware	Morris Worm
IP Spoofing	Manipulation of source IP address in TCP/IP headers to impersonate trusted entities(9)	1994	Used in DDoS attacks, man-in-the-middle attacks	Spoofing source IP address	DDoS attacks, man-in-the-middle attacks
TCP Sequence Number Prediction [39]	Predicting TCP sequence numbers to hijack connections, inject data, or bypass security mechanisms	Early 2000s	Used in session hijacking, data manipulation	Predicting TCP sequence numbers	Session hijacking, data manipulation
Packet Injection [40]	Unauthorized injection of packets into networks to disrupt communication or launch attacks	2005	Disrupts communication, intercepts data, launches attacks	Injecting unauthorized packets	Packet injection attacks
Covert Channel Data Exfiltration [41]	Exploiting covert channels in TCP/IP headers to exfiltrate data stealthily without detection	1970s & 80s	Bypasses traditional security measures, exfiltrates data covertly	Encoding data in network traffic	Covert channel data exfiltration
ARP Spoofing [42]	Manipulating ARP protocol to associate rogue MAC address with legitimate IP address	late 1990s and early 2000s	Intercepts network traffic, launches man-in-the-middle attacks, eavesdrops on communications	Spoofing ARP protocol	ARP spoofing attacks
Denial of Service (DoS) Attacks [43]	Overwhelming network resources to cause downtime and deny access to legitimate users	-	Floods networks with malicious traffic, causes downtime and performance issues	Flooding network resources	DoS attacks

Furthermore, the proliferation of distributed denial-of-service (DDoS) attacks [44] has fueled the evolution of TCP/IP header attacks into more scalable and destructive forms. Modern DDoS attacks often utilize sophisticated botnets composed of compromised devices worldwide to launch massive floods of malicious traffic at targeted networks or servers [45]-[50]. By spoofing source IP addresses and manipulating TCP/IP header fields, attackers can amplify the impact of their attacks while obscuring their origins, making it difficult for defenders to mitigate the onslaught effectively. Another notable evolution in TCP/IP header attacks is the integration of advanced evasion techniques to bypass network security mechanisms such as intrusion detection and prevention systems (IDS/IPS). Attackers employ various obfuscation methods to camouflage malicious payloads within network packets, making them appear benign or undetectable to traditional security controls [51]-[54]. By exploiting vulnerabilities in protocol implementations or leveraging protocol ambiguities, attackers can evade detection and successfully penetrate network defenses, exacerbating the challenge of defending against TCP/IP header attacks. In response to the evolving threat landscape, cybersecurity professionals have adopted a proactive approach to defend against TCP/IP header attacks, emphasizing the implementation of comprehensive security measures and the continuous monitoring of network traffic for suspicious activities. This includes deploying next-generation firewalls [55], intrusion detection and prevention systems, advanced threat analytics, and encryption technologies [56] to mitigate the risk of TCP/IP header attacks effectively. Additionally, ongoing research and collaboration within the cybersecurity community are essential to stay ahead of emerging threats and develop robust countermeasures to safeguard critical infrastructure and data assets from evolving TCP/IP header attacks.

4. Emerging trends in TCP/IP header attacks

Previous research emphasize the persistent vulnerabilities within the TCP/IP protocol suite, where attackers exploit header fields to manipulate packet data and launch sophisticated attacks. In a different study, authors in [57] showcases real-world incidents demonstrating the rise of ransomware attacks targeting IoT devices, illustrating the practical implications of TCP/IP header vulnerabilities. These diverse perspectives from various studies collectively highlight the critical need for cybersecurity professionals to stay informed about emerging threats and implement proactive measures to mitigate the impact of TCP/IP header attacks on network security. Novel attack vectors in the realm of cybersecurity continue to evolve, presenting new challenges for defenders. One such trend involves attacks targeting specific protocol fields, where adversaries exploit vulnerabilities in the design or implementation of network protocols to disrupt communication or gain unauthorized access [58]-[60]. By manipulating certain fields within protocol headers, attackers can inject malicious code, alter data packets, or bypass security mechanisms, leading to potential service disruptions or information leakage [61]. Additionally, the use of advanced evasion techniques further complicates defense strategies, as attackers employ sophisticated methods to obfuscate malicious payloads and evade detection by security systems [62]. These techniques may involve fragmentation of packets, encryption [63] of malicious payloads, or manipulation of network traffic patterns to bypass traditional security controls. As attackers continue to innovate and adapt their tactics, defenders must remain vigilant and proactive in identifying and mitigating these emerging threats to safeguard network infrastructure and data assets.

According to [64], emerging trends in TCP/IP header attacks showcase the adaptability and innovation of cybercriminals in exploiting vulnerabilities within network protocols. One notable trend is the increasing use of encryption to obfuscate malicious activities within network traffic [65]-[68]. While encryption enhances data confidentiality and integrity [69], it also provides a veil for attackers to hide malicious payloads within encrypted packets, making it challenging for traditional security controls to detect and mitigate TCP/IP header attacks effectively. As encryption adoption continues to rise across networks, attackers are leveraging this trend to evade detection and launch stealthier attacks, underscoring the importance of advanced threat detection and decryption capabilities. Another emerging trend in TCP/IP header attacks is the exploitation of Internet of Things (IoT) devices and cloud infrastructure [70], [71]. With the proliferation of IoT devices and the migration of critical services to cloud platforms, attackers are targeting vulnerabilities in TCP/IP implementations within these environments to orchestrate large-scale attacks. IoT devices, often characterized by limited processing power and lax security measures, serve as attractive targets for botnet recruitment and amplification attacks, enabling attackers to launch distributed denial-of-service (DDoS) attacks with unprecedented scale and impact. Similarly, vulnerabilities in cloud-based networking services and virtualized environments provide fertile ground for TCP/IP header attacks, highlighting the need for robust security measures and proactive threat intelligence to defend against emerging threats [72]-[75].

Moreover, the convergence of technologies such as 5G networks and edge computing introduces new attack vectors and challenges for network security. As 5G networks promise ultra-low latency and high-speed connectivity [76], they also introduce complexities in network architectures and protocols, creating opportunities for attackers to exploit vulnerabilities in TCP/IP header fields to compromise network integrity or disrupt critical services. Edge computing, which involves processing data closer to the source of generation, further complicates the threat landscape by

decentralizing network resources and widening the attack surface [77]-[80]. Attackers are increasingly targeting edge devices and services to exploit vulnerabilities in TCP/IP implementations and launch sophisticated attacks, necessitating enhanced security measures and threat intelligence to mitigate emerging risks effectively. Furthermore, the rise of artificial intelligence (AI) and machine learning (ML) technologies [81] is reshaping the landscape of TCP/IP header attacks, both as a defensive tool and an offensive weapon. While AI-driven security solutions offer promising capabilities in detecting and mitigating TCP/IP header attacks, adversaries are also leveraging AI and ML techniques to enhance the sophistication and efficacy of their attacks [82]-[86]. From generating polymorphic malware to evading detection through adversarial examples, attackers are harnessing the power of AI to automate and optimize their attack strategies, posing unprecedented challenges for defenders. As AI-driven attacks become more prevalent, organizations must invest in AI-powered security solutions and cultivate cybersecurity talent proficient in AI and ML [87] to stay ahead of evolving threats in TCP/IP header attacks.

In a nutshell, emerging trends in TCP/IP header attacks underscore the dynamic nature of cybersecurity threats and the need for continuous innovation in defensive strategies. From encryption and IoT vulnerabilities to 5G networks and AI-driven attacks, the evolving threat landscape presents complex challenges for organizations seeking to protect their networks and data assets [88]-[91]. By adopting a proactive approach to security, leveraging advanced technologies, and fostering collaboration within the cybersecurity community, organizations can enhance their resilience against emerging threats in TCP/IP header attacks and safeguard their digital infrastructure in an increasingly interconnected world.

5. Impact of emerging threats

Emerging TCP/IP header attacks pose a significant threat to network security and stability, potentially leading to severe consequences for organizations and users. By targeting specific fields within TCP/IP headers, attackers can exploit vulnerabilities in network protocols to launch sophisticated attacks that compromise data integrity, confidentiality, and availability [92], [93]. For instance, attacks such as IP spoofing [94], and packet replay [95], [96] can deceive network devices into accepting malicious packets as legitimate, leading to unauthorized access or data manipulation. These attacks can disrupt network operations, degrade service quality, and expose sensitive information to unauthorized parties. Furthermore, the manipulation of TCP/IP headers can bypass traditional security mechanisms, making it challenging for defenders to detect and mitigate such threats effectively [97]-[99]. As a result, organizations must implement robust security measures [100], such as connection auditing, encryption, and intrusion detection systems, to defend against emerging TCP/IP header attacks and safeguard the integrity and resilience of their network infrastructure. Previous research studies have highlighted the severe consequences of cyber threats for organizations and network infrastructure. According to a study on Denial of Service attacks [101]-[103] the empirical analysis of such attacks aims to develop best practices for designing DoS-resilient network protocols. Figure e gives an illustration of a typical DoS attack. Understanding the motivations of cyber attackers is crucial, as detailed in a review on cyber incidents targeting critical infrastructures [104], [105]. This study emphasizes the growing sophistication of adversaries and the need for robust defenses. The selection criteria for identifying publications on cyber attacks include reports of historical incidents and studies on attack detection and prevention, indicating the diverse range of threats [106] faced by organizations. Major Cyber attacks on critical infrastructures have been compiled to identify vulnerabilities and typical victims and attackers, underscoring the importance of proactive security measures. A comprehensive analysis on cyber security discusses common risks and threats, providing solutions to prevent them [107], emphasizing the necessity for organizations to prioritize cybersecurity measures. This collective body of research underscores the critical importance of addressing cyber threats to safeguard organizational assets and network infrastructure.

According to [108], the impact of emerging threats in TCP/IP is multifaceted and pervasive, affecting not only individual users but also entire industries and critical infrastructure. One of the most significant impacts is on data privacy and integrity. Emerging threats in TCP/IP, such as sophisticated packet manipulation techniques and header attacks, compromise the confidentiality and integrity of data transmitted over networks [109]-[111]. This jeopardizes sensitive information, including personal and financial data, leading to breaches, identity theft, and financial losses. Moreover, the potential for data manipulation [112] poses risks to the trustworthiness of digital transactions and undermines confidence in online communications. Another critical impact is on network availability and reliability. Emerging TCP/IP threats, such as distributed denial-of-service (DDoS) attacks leveraging TCP/IP vulnerabilities, can overwhelm network resources, causing service disruptions and downtime [113], [114]. These attacks target critical infrastructure, including financial institutions, healthcare systems, and government agencies, impacting the delivery of essential services and affecting millions of users [115]. The resulting economic losses, operational disruptions, and reputational damage underscore the importance of robust network defenses and proactive mitigation strategies to ensure network availability and resilience in the face of emerging TCP/IP threats.

Furthermore, emerging threats in TCP/IP have implications for national security and geopolitical stability. Cyberattacks exploiting TCP/IP vulnerabilities, such as those targeting government networks, critical infrastructure, and defense systems, can have far-reaching consequences, including espionage, sabotage, and geopolitical tensions [116]-[118]. Adversaries may exploit TCP/IP weaknesses to infiltrate government networks, steal classified information, or disrupt critical services, posing significant risks to national security and sovereignty [119]. As nations increasingly rely on interconnected digital infrastructure, addressing emerging TCP/IP threats becomes a priority for governments to safeguard against cyber threats and protect national interests.

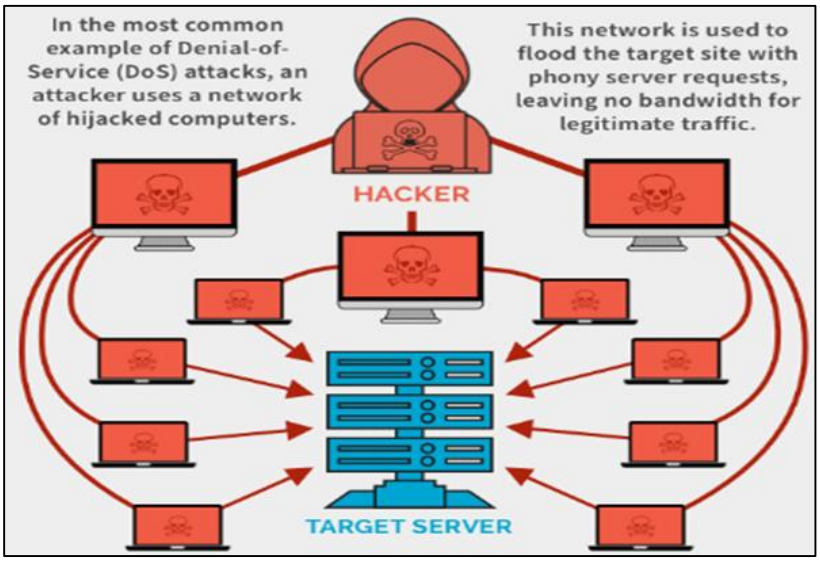

Figure 4 Denial of service attack

The proliferation of TCP/IP threats also poses challenges for regulatory compliance and cybersecurity governance. Regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose strict requirements on organizations to protect the privacy and security of personal data [120]-[122]. However, emerging TCP/IP threats raise compliance concerns as organizations struggle to mitigate evolving risks and secure their networks effectively. Compliance failures not only result in regulatory penalties but also erode consumer trust and damage corporate reputation [123], underscoring the importance of proactive risk management and compliance measures in addressing emerging TCP/IP threats.

In summary, the impact of emerging threats in TCP/IP extends across various domains, including data privacy, network availability, national security, regulatory compliance, and cybersecurity governance [124], [125]. Addressing these threats requires a comprehensive approach that combines technical solutions, regulatory compliance measures, and international cooperation. By enhancing network defenses, strengthening cybersecurity governance frameworks, and promoting collaboration among stakeholders, organizations and governments can mitigate the impact of emerging TCP/IP threats and ensure the resilience and security of digital infrastructure in an increasingly interconnected world.

6. Future directions for TCP/IP defense strategies

Exploring potential directions for enhancing defense strategies against evolving TCP/IP header attacks is essential in maintaining network security. Researchers have identified vulnerabilities in TCP/IP headers, highlighting attack vectors such as TCP SYN flooding and session hijacking [126]. Figure 5 and Figure 6 shows typical TCP SYN flooding and session hijacking attacks respectively. It is crucial to implement robust countermeasures to strengthen TCP/IP header security and support network administrators in safeguarding their systems [127], [128]. Furthermore, the adoption of secure key distribution schemes and encryption protocols has been recommended to enhance data confidentiality and integrity in TCP/IP networks [129]. The deployment of intrusion detection systems, intrusion prevention systems, and firewall solutions is vital for detecting and mitigating threats [130] targeting TCP/IP headers [131]. Understanding network traffic patterns and utilizing anomaly detection techniques can further enhance defense mechanisms against evolving TCP/IP header attacks [132], [133]. Continuous research into security solutions, including access control mechanisms and network authentication services, is necessary to address emerging threats to the TCP/IP protocol suite [134], [135]. Anomaly detection techniques play a crucial role in identifying irregular patterns in network traffic that may indicate

potential security threats [136], [137]. By leveraging machine learning algorithms, researchers can enhance the accuracy of anomaly detection systems and improve the ability to detect sophisticated cyber attacks [138].

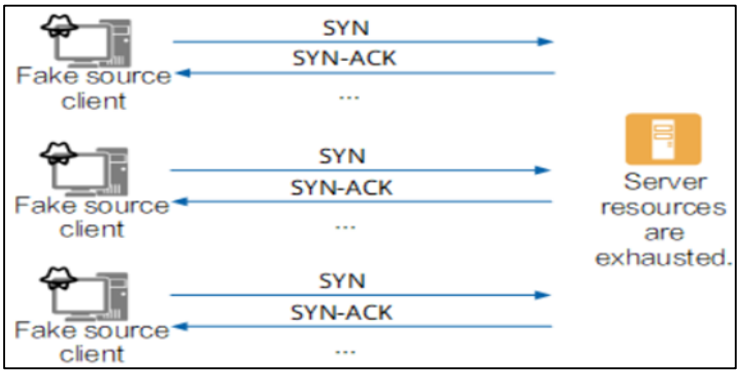

Figure 5 TCP SYN flooding attack

Additionally, advancements in protocol enhancements, such as improving the security features of TCP/IP headers and implementing secure communication protocols, are essential to mitigate vulnerabilities and strengthen overall network security. Research in these areas is vital for staying ahead of evolving cyber threats and ensuring the resilience of network infrastructures in the face of increasingly sophisticated attacks.

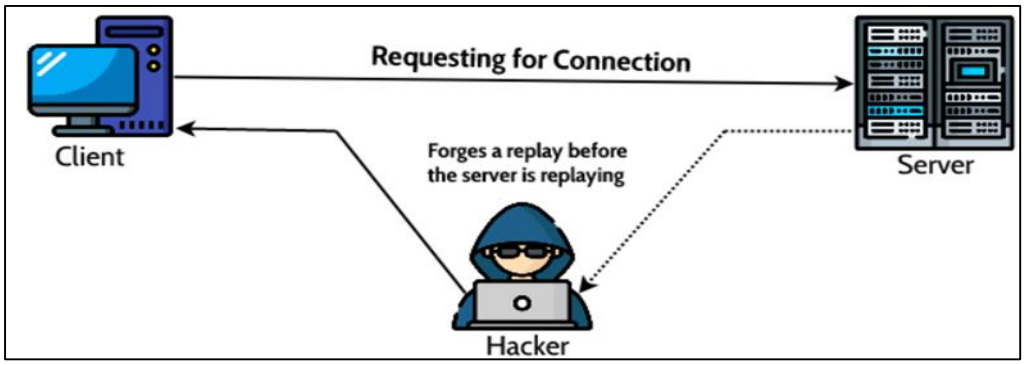

Figure 6 Session hijacking attack

According to [139], TCP/IP defense strategies must embrace a proactive and adaptive approach to counter evolving threats effectively. One key direction is the integration of artificial intelligence (AI) and machine learning (ML) technologies into security solutions. As shown in Figure 7, AI and ML algorithms [140] can analyze network traffic patterns, detect anomalies indicative of TCP/IP attacks, and automate response actions in real-time. By continuously learning from new threats and adapting their defenses, AI-powered security solutions can enhance network resilience and minimize the impact of TCP/IP attacks.

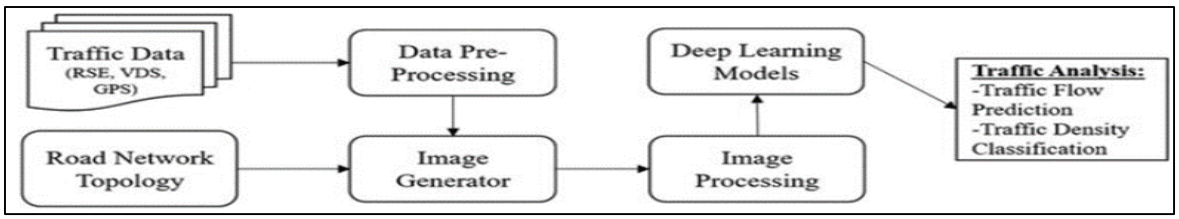

Figure 7 ML assisted traffic analysis

Furthermore, the adoption of Zero Trust architecture represents a promising future direction for TCP/IP defense strategies [141]. Zero Trust assumes that no entity, whether inside or outside the network, can be trusted and requires strict verification of every user and device attempting to access resources [142]- [145]. By implementing granular access controls, network segmentation, and continuous monitoring, Zero Trust architectures limit the attack surface and prevent lateral movement by attackers, mitigating the risks posed by TCP/IP vulnerabilities and insider threats.

Additionally, the development of secure-by-design protocols [146] and standards is essential for strengthening TCP/IP defense strategies in the future. This involves integrating security mechanisms into the design and implementation of TCP/IP protocols to prevent common attack vectors, such as spoofing, injection, and evasion techniques [147], [148]. By adopting secure-by-design principles, protocol developers can minimize the likelihood of vulnerabilities in TCP/IP implementations and reduce the potential impact of attacks on network infrastructure and communication systems. Moreover, collaboration and information sharing among stakeholders will be crucial for advancing TCP/IP defense strategies in the future. Cybersecurity threats are increasingly sophisticated and dynamic, requiring coordinated efforts from governments, industry partners, and the cybersecurity community to identify emerging threats, share threat intelligence, and develop effective mitigation strategies [149], [150]. By fostering collaboration and information sharing initiatives, stakeholders can leverage collective knowledge and resources to stay ahead of evolving TCP/IP threats and enhance overall network security. Finally, the convergence of cybersecurity with emerging technologies such as quantum computing and blockchain presents both opportunities and challenges for TCP/IP defense strategies [151]. Figure 8 shows how blockchain can be amalgamated with ML for securing TCP-based connections.

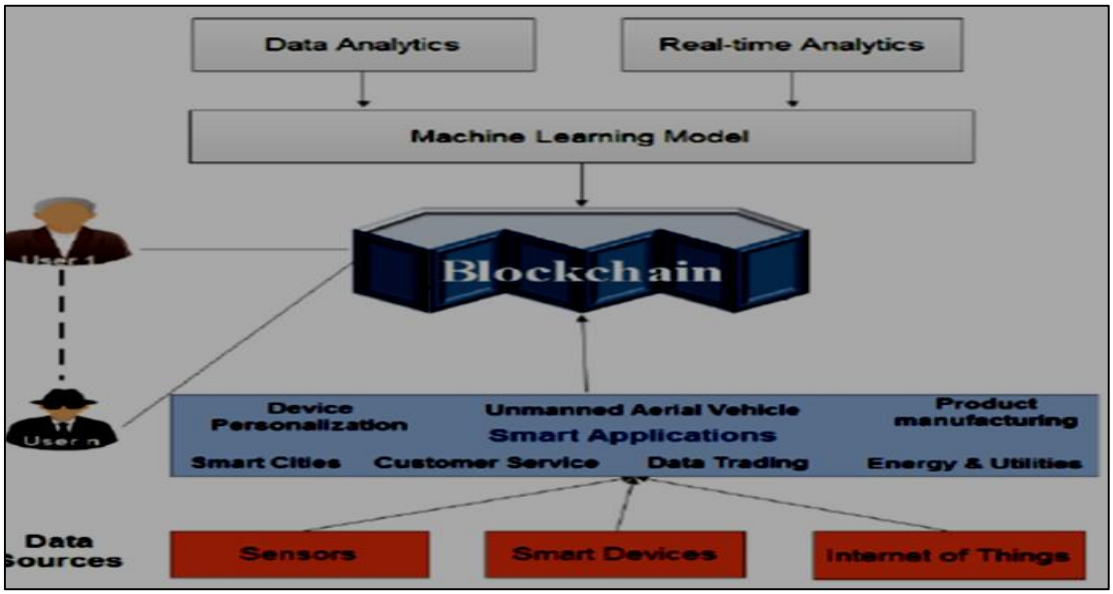

Figure 8 ML and blockchain for enhanced TCP/IP connection security

Quantum computing has the potential to break traditional cryptographic algorithms [152] used to secure TCP/IP communications, necessitating the development of quantum-resistant encryption protocols. Similarly, blockchain technology offers decentralized and tamper-resistant mechanisms for securing network transactions and verifying data integrity [153], which can complement traditional TCP/IP defense strategies by providing an additional layer of security and trust in distributed environments. As such, TCP/IP defense strategies must embrace technological innovation, adopt proactive security measures, and prioritize collaboration among stakeholders. By integrating AI and ML technologies, implementing Zero Trust architectures, developing secure-by-design protocols, fostering collaboration, and leveraging emerging technologies such as quantum computing and blockchain, organizations can enhance their resilience against TCP/IP attacks and safeguard critical network infrastructure and data assets in an evolving threat landscape.

7. Challenges and limitations

Defending against emerging TCP/IP header attacks presents various challenges and limitations in the realm of network security. One significant challenge is the increasing complexity of attack techniques, making it harder to detect and mitigate threats effectively [154]. Moreover, the automation of attacks through cyber-attacks-as-a-service models poses a formidable challenge, as attackers can rapidly deploy sophisticated tactics without manual intervention [155]. Intelligent attacks that can bypass traditional detection systems further complicate defense strategies, requiring innovative approaches to stay ahead of malicious actors [156], [157]. Machine learning algorithms, while powerful tools for threat detection, may introduce biases and assumptions that impact the accuracy of attack identification. Additionally, the sheer volume of network connections and the complexity of high-dimensional data make it challenging to classify and analyze potential threats accurately. The rugged protection of multiple network components and the human factor in security also contribute to the limitations faced in defending against emerging TCP/IP header attacks. Consideration of factors such as resource constraints [158] is crucial in the design of secure protocols . Scalability issues

must also be taken into account to ensure that the protocol can handle increasing demands without compromising security. Furthermore, the ongoing arms race between attackers and defenders necessitates continuous adaptation and innovation in cybersecurity measures [159].

8. Case studies

In the realm of cybersecurity, understanding the real-world implications of TCP/IP header attacks is crucial for organizations and security professionals to grasp the severity of cyber threats [160]. By examining case studies and examples of notable incidents, the impact of these attacks on networks and entities becomes apparent. Table 2 presents a curated selection of case studies and real-world examples of TCP/IP header attacks, highlighting the diverse range of cyber threats that exploit vulnerabilities in the TCP/IP protocol suite.

Table 2 Real-world examples of TCP/IP header attacks

Case Studies or Real-World Examples	Description	Year	Impact	Attack Technique
SolarWinds Supply Chain Attack [164]	Sophisticated cyberattack targeting SolarWinds software, compromising numerous organizations	2020	Compromised data integrity, exposed sensitive information, undermined trust in software supply chain	Supply chain compromise
Mirai Botnet DDoS Attacks [165]	IoT botnet targeting Dyn DNS service, launching massive DDoS attacks disrupting internet services	2016	Disrupted internet services, caused downtime for major websites, highlighted IoT [166] security vulnerabilities	IoT botnet DDoS attacks
Equifax Data Breach [167]	Massive data breach at Equifax exposing sensitive personal information of millions of individuals	2017	Compromised personal data, led to identity theft, regulatory fines, damaged reputation of Equifax	Data breach
WannaCry Ransomware Attack [168]	Global ransomware attack exploiting Windows SMB vulnerability, encrypting data and demanding ransom	2017	Encrypted data, disrupted operations, financial losses, highlighted the impact of ransomware attacks	Ransomware attack
NotPetya Cyberattack [169]	NotPetya malware disguised as ransomware, targeting Ukrainian infrastructure and spreading globally	2017	Caused widespread damage, disrupted critical infrastructure, financial losses, attributed to nation-state actors	Malware disguised as ransomware

These instances demonstrate the tangible consequences of cyberattacks on organizations, emphasizing the importance of robust defense mechanisms and proactive security measures in safeguarding against evolving threats.

9. Future research directions

As we look to the future, there are several promising avenues for further research and development in TCP/IP header security. One area of focus could be on the development of advanced anomaly detection techniques (shown in Figure 9) that leverage machine learning algorithms to detect subtle deviations in TCP/IP header patterns indicative of malicious activity [170], [171]. Additionally, research into enhancing the security features of TCP/IP headers themselves, such as incorporating cryptographic mechanisms for authentication and integrity verification [172], holds potential for strengthening overall network defenses. Figure 10 shows a typical integrity verification in TCP/IP networks. Moreover, exploring the application of blockchain technology in securing TCP/IP headers and preventing unauthorized modifications could pave the way for innovative solutions in network security.

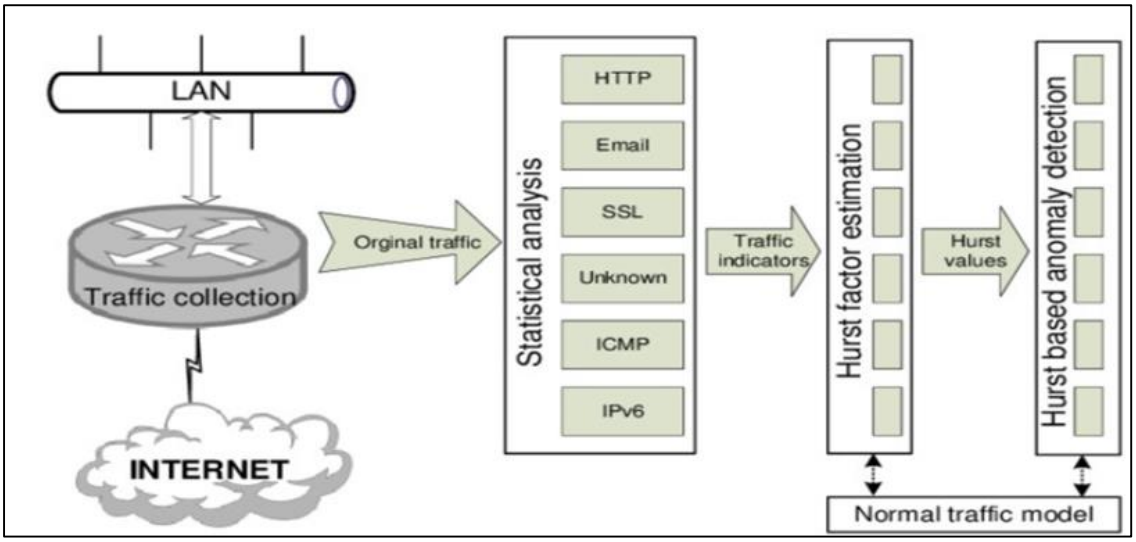

Figure 9 Network anomaly detection

Despite advancements in TCP/IP header security, there remain unresolved questions and areas requiring further investigation to bolster network defenses. One such area is the mitigation of attacks that exploit inherent vulnerabilities in the TCP/IP protocol suite, such as IP spoofing and packet injection [173], [174]. Understanding the root causes of these vulnerabilities and developing effective countermeasures is essential for minimizing the risk posed by such attacks.

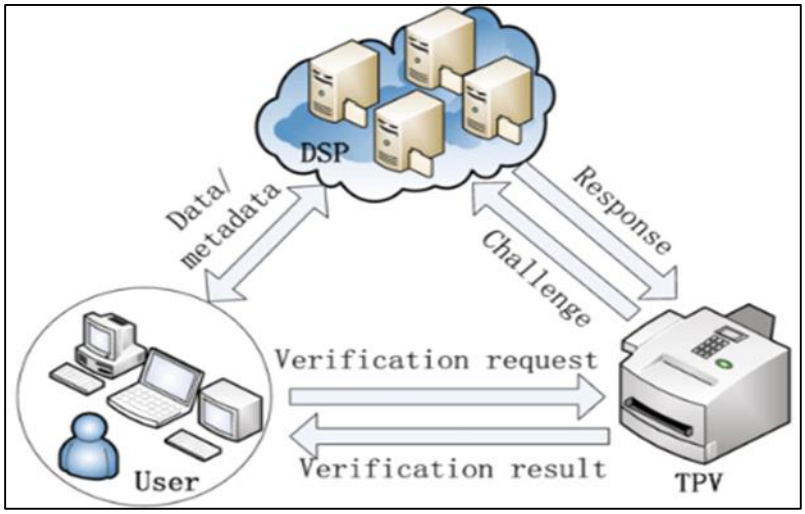

Figure 10 Traffic integrity verification

Additionally, the impact of emerging technologies, such as the Internet of Things (IoT), on TCP/IP header security warrants further exploration, particularly in identifying and addressing potential vulnerabilities introduced by interconnected devices. Furthermore, the efficacy of existing defense mechanisms in mitigating evolving TCP/IP header attacks requires empirical validation through real-world testing and analysis, highlighting the importance of continued research in this field. According to [175], future research directions in TCP/IP header attacks are crucial for staying ahead of evolving cyber threats and enhancing network security. One promising area for research is the development of advanced detection and mitigation techniques tailored to address emerging TCP/IP header attack vectors. Researchers can explore novel methods for detecting anomalies in packet headers, analyzing traffic patterns, and identifying indicators of compromise indicative of TCP/IP header attacks. By leveraging machine learning, anomaly detection algorithms, and behavioral analytics [176], researchers can develop more robust and adaptive defense mechanisms capable of mitigating a wide range of TCP/IP header attacks in real-time. Moreover, researchers can focus on understanding the underlying vulnerabilities in TCP/IP implementations and developing secure-by-design protocols to mitigate common attack vectors [177], [178]. This involves analyzing protocol specifications, identifying weaknesses in packet header fields, and proposing enhancements to strengthen TCP/IP security. By addressing vulnerabilities at

the protocol level and integrating security mechanisms into TCP/IP design principles, researchers can reduce the attack surface and minimize the impact of TCP/IP header attacks on network infrastructure and communication systems.

Furthermore, future research in TCP/IP header attacks can explore the implications of emerging technologies such as software-defined networking (SDN) and Internet of Things (IoT) on network security [179], [180]. As shown in Figure 11, SDN introduces programmability and centralized control in network management, offering opportunities for implementing dynamic security policies and mitigating TCP/IP header attacks more effectively.

Similarly, the proliferation of IoT devices introduces new challenges for TCP/IP security, as these devices often have limited processing power and lack robust security mechanisms [181]-[184]. Figure 12 gives an illustration of a typical IoT environment. Researchers can investigate the vulnerabilities inherent in IoT devices' TCP/IP implementations and develop strategies to mitigate potential risks posed by TCP/IP header attacks targeting IoT networks. Additionally, research efforts can focus on the development of collaborative defense strategies and information sharing mechanisms to combat TCP/IP header attacks effectively [185], [186]. This involves establishing partnerships between industry stakeholders, government agencies, and the cybersecurity research community to exchange threat intelligence, share best practices, and coordinate response efforts. By fostering collaboration and information sharing initiatives, researchers can leverage collective knowledge and resources to identify emerging TCP/IP header attack trends, develop timely mitigation strategies, and enhance overall network security posture.

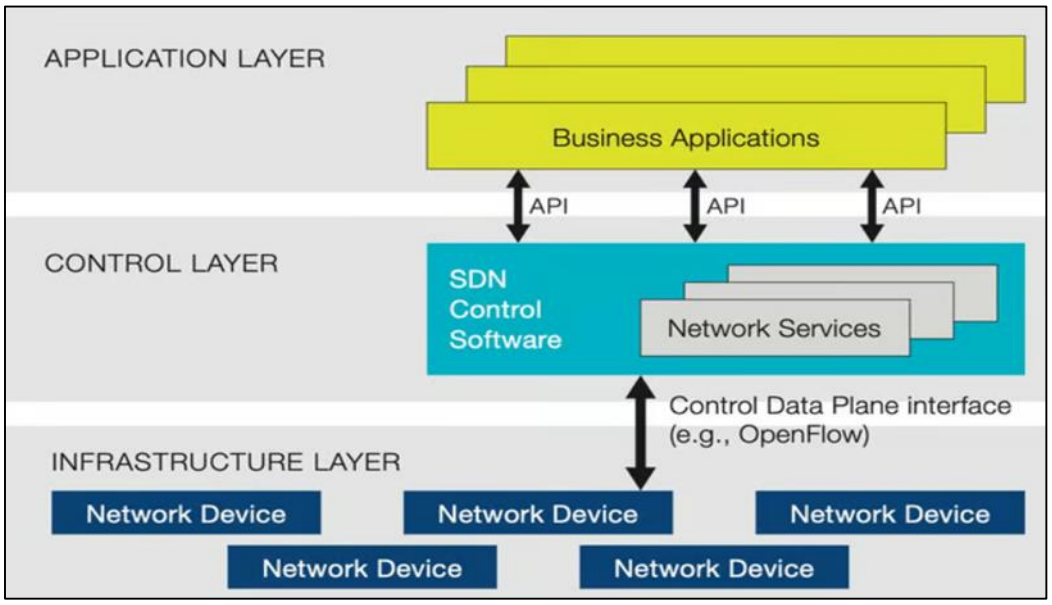

Figure 11 Software-defined networking

Moreover, future research in TCP/IP header attacks should explore the implications of quantum computing and blockchain technology on network security [187]-[189].

Quantum computing has the potential to break traditional cryptographic algorithms used to secure TCP/IP communications, necessitating the development of quantum-resistant encryption protocols. Similarly, blockchain technology offers decentralized and tamper-resistant mechanisms for securing network transactions and verifying data integrity [190], which can complement traditional TCP/IP defense strategies by providing an additional layer of security and trust in distributed environments. By investigating the intersection of TCP/IP header attacks with emerging technologies, researchers can anticipate future threats and develop proactive defense strategies to mitigate their impact on network security.

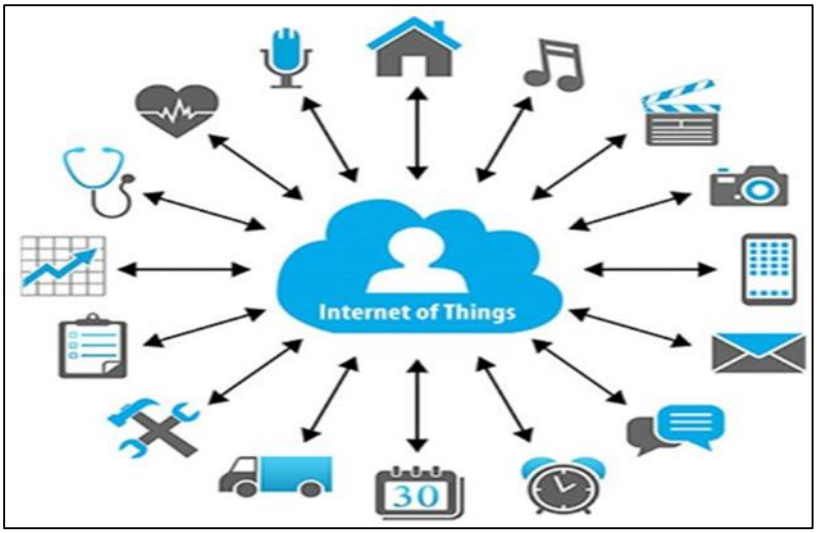

Figure 12 An IoT environment

10. Conclusion

In conclusion, this survey has highlighted the persistent threat posed by TCP/IP header attacks in the realm of network security. Through historical analysis and examination of contemporary research, it's evident that attackers exploit vulnerabilities within the TCP/IP protocol suite to launch sophisticated attacks, compromising data integrity and network stability. Emerging trends underscore the need for continuous vigilance and proactive defense strategies, with novel attack vectors and advanced evasion techniques presenting ongoing challenges. Robust security measures, including intrusion detection systems and encryption protocols, are crucial for mitigating the impact of these attacks and safeguarding network infrastructure. Moving forward, policymakers, network administrators, and security professionals must collaborate to enhance defense mechanisms against TCP/IP header attacks. Policymakers should prioritize cybersecurity initiatives and support research efforts aimed at identifying and mitigating emerging threats. Network administrators should implement robust security measures, including intrusion detection systems and encryption protocols, to detect and mitigate TCP/IP header attacks effectively. Security professionals should stay informed about evolving attack techniques and leverage anomaly detection techniques and protocol enhancements to strengthen network defenses. Additionally, continued collaboration within the cybersecurity community is vital for sharing insights and best practices in mitigating the evolving threat landscape of TCP/IP header attacks.

References

[1] 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.

[2] Qiao L, Dong E, Yin H, Li H, Yang J. Intelligent Network Device Identification based on Active TCP/IP Stack Probing. IEEE Network. 2024 Mar 7.

[3] Mantu R, Chiroiu M, Tăpuș N. Framework for evaluating TCP/IP extensions in communication protocols. International Journal of Computers Communications & Control. 2024 Mar 1;19(2).

[4] Shirichian M, Sabbaghi-Nadooshan R, Houshmand M, Houshmand M. A QTCP/IP reference model for partially trusted-node-based quantum-key-distribution-secured optical networks. Quantum Information Processing. 2024 Mar 1;23(3):87.

[5] Liu Q, Xu Z, Li Z. Implementation of hardware TCP/IP stack for DAQ systems with flexible data channel. Electronics Letters. 2017 Apr;53(8):530-2.

[6] 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.

[7] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[8] 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.

[9] Pandey A, Saini JR. Attacks & defense mechanisms for TCP/IP based protocols. International Journal of Engineering Innovations and Research. 2014 Jan 1;3(1):17.

[10] Abdullah MS, Zainal A, Maarof MA, Kassim MN. Cyber-attack features for detecting cyber threat incidents from online news. In2018 Cyber Resilience Conference (CRC) 2018 Nov 13 (pp. 1-4). IEEE.

[11] Akhtar MS, Feng T. Malware analysis and detection using machine learning algorithms. Symmetry. 2022 Nov 3;14(11):2304.

[12] Chen R, Li Y, Fang W. Android malware identification based on traffic analysis. InInternational conference on artificial intelligence and security 2019 Jul 11 (pp. 293-303). Cham: Springer International Publishing.

[13] 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.

[14] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[15] Sharma A, Islam MR, Ningombam D. Impact of TCP-SYN Flood Attack in Cloud. InContemporary Issues in Communication, Cloud and Big Data Analytics: Proceedings of CCB 2020 2021 Dec 1 (pp. 77-85). Singapore: Springer Singapore.

[16] Nalayini CM, Katiravan J. Block Link Flooding Algorithm for TCP SYN Flooding Attack. InInternational Conference on Computer Networks and Communication Technologies: ICCNCT 2018 2019 (pp. 895-905). Springer Singapore.

[17] Shah SQ, Khan FZ, Ahmad M. Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN. Computer Communications. 2022 Jan 15;182:198-211.

[18] Dang VT, Huong TT, Thanh NH, Nam PN, Thanh NN, Marshall A. Sdn-based syn proxy—a solution to enhance performance of attack mitigation under tcp syn flood. The Computer Journal. 2019 Apr 1;62(4):518-34.

[19] Mkuzangwe NN, Nelwamondo FV. A fuzzy logic based network intrusion detection system for predicting the TCP SYN flooding attack. InIntelligent Information and Database Systems: 9th Asian Conference, ACIIDS 2017, Kanazawa, Japan, April 3–5, 2017, Proceedings, Part II 9 2017 (pp. 14-22). Springer International Publishing.

[20] Mohammed MA, Hussain MA, Oraibi ZA, Abduljabbar ZA, Nyangaresi VO. Secure Content Based Image Retrieval System Using Deep Learning. J. Basrah Res.(Sci.). 2023 Dec 30;49(2):94-111.

[21] Alqahtani AH, Iftikhar M. TCP/IP attacks, defenses and security tools. International Journal of Science and Modern Engineering (IJISME). 2013 Sep;1(10):42-7.

[22] Garringer J. The Role of Protocol Analysis in Cybersecurity: Closing the Gap on Undetected Data Breaches. Utica College; 2018.

[23] Papatsaroucha D, Nikoloudakis Y, Kefaloukos I, Pallis E, Markakis EK. A survey on human and personality vulnerability assessment in cyber-security: Challenges, approaches, and open issues. arXiv preprint arXiv:2106.09986. 2021 Jun 18.

[24] Colajanni M, Marchetti M. Cyber attacks and defenses: current capabilities and future trends. InTechnology and International Relations 2021 Apr 20 (pp. 132-151). Edward Elgar Publishing.

[25] Montasari R, Hosseinian-Far A, Hill R. Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments. Cyber criminology. 2018:71-93.

[26] 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.

[27] Parian C, Guldimann T, Bhatia S. Fooling the master: Exploiting weaknesses in the modbus protocol. Procedia Computer Science. 2020 Jan 1;171:2453-8.

[28] Almaraz-Rivera JG, Perez-Diaz JA, Cantoral-Ceballos JA. Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models. Sensors. 2022 Apr 28;22(9):3367.

[29] Farha F, Chen H. Mitigating replay attacks with ZigBee solutions. Network Security. 2018 Jan 1;2018(1):13-9.

[30] Al-Rimy BA, Maarof MA, Shaid SZ. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security. 2018 May 1;74:144-66.

[31] da Silveira MG, Franco PH. IEC 61850 network cybersecurity: Mitigating GOOSE message vulnerabilities. In Proc. 6th Annual PAC World Americas Conf 2019 Aug 20 (pp. 1-9).

[32] 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.

[33] Alam S, Alam Y, Cui S, Akujuobi C. Data-driven network analysis for anomaly traffic detection. Sensors. 2023 Sep 29;23(19):8174.

[34] Çelebi M, Özbilen A, Yavanoğlu U. A comprehensive survey on deep packet inspection for advanced network traffic analysis: issues and challenges. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi. 2023 Jan 1;12(1):1-29.

[35] Munshi A. Hybrid Detection Technique for IP Packet Header Modifications Associated with Store-and-Forward Operations. Applied Sciences. 2023 Sep 12;13(18):10229.

[36] 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.

[37] AlSabeh A, Kfoury E, Crichigno J, Bou-Harb E. P4ddpi: Securing p4-programmable data plane networks via dns deep packet inspection. InNDSS Symposium 2022 2022 Apr.

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

[39] Zeng F, Yin K, Chen M. Research on TCP Initial Sequence Number prediction method based on adding-weight chaotic time series. In2008 The 9th International Conference for Young Computer Scientists 2008 Nov 18 (pp. 1511-1515). IEEE.

[40] Gu Q, Liu P, Zhu S, Chu CH. Defending against packet injection attacks unreliable ad hoc networks. InGLOBECOM'05. IEEE Global Telecommunications Conference, 2005. 2005 Nov 28 (Vol. 3, pp. 5-pp). IEEE.

[41] Valeriano B, Jensen BM, Maness RC. Cyber strategy: The evolving character of power and coercion. Oxford University Press; 2018.

[42] Mohamed YA, Hashim M, Bashir M. A Strategy to Mitigate ARP Spoofing Attacks on Hypervisors. In2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) 2024 Jan 11 (pp. 1-8). IEEE.

[43] Manzano Y. Tracing the development of denial of service attacks: a corporate analogy. XRDS: Crossroads, The ACM Magazine for Students. 2003 Sep 1;10(1):4-.

[44] 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.

[45] Singh NJ, Hoque N, Singh KR, Bhattacharyya DK. Botnet-based IoT network traffic analysis using deep learning. Security and Privacy. 2024 Mar;7(2):e355.

[46] Shukla P, Krishna CR, Patil NV. Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review. The Journal of Supercomputing. 2023 Dec 19:1-58.

[47] Adedeji KB, Abu-Mahfouz AM, Kurien AM. DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks. 2023 Jul 6;12(4):51.

[48] Li Q, Huang H, Li R, Lv J, Yuan Z, Ma L, Han Y, Jiang Y. A comprehensive survey on DDoS defense systems: New trends and challenges. Computer Networks. 2023 Jun 24:109895.

[49] Kaur Chahal J, Bhandari A, Behal S. Distributed denial of service attacks: a threat or challenge. New Review of Information Networking. 2019 Jan 2;24(1):31-103.

[50] 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.

[51] Chaddad L, Chehab A, Elhajj IH, Kayssi A. Optimal packet camouflage against traffic analysis. ACM Transactions on Privacy and Security (TOPS). 2021 Aug 19;24(3):1-23.

[52] Vidal JM, Monge MA, Monterrubio SM. Espada: Enhanced payload analyzer for malware detection robust against adversarial threats. Future Generation Computer Systems. 2020 Mar 1;104:159-73.

[53] Singh J, Singh J. Challenge of malware analysis: malware obfuscation techniques. International Journal of Information Security Science. 2018 Sep 29;7(3):100-10.

[54] Araujo F, Hamlen KW, Biedermann S, Katzenbeisser S. From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation. InProceedings of the 2014 ACM SIGSAC conference on computer and communications security 2014 Nov 3 (pp. 942-953).

[55] Ahmadi S. Next Generation AI-Based Firewalls: A Comparative Study. International Journal of Computer (IJC). 2023;49(1):245-62.

[56] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[57] 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.

[58] Abdulkadhim EG, Hayder MA. Survey of E-mail Classification: Review and Open Issues. Iraqi Journal for Computers and Informatics. 2020 Dec 3;46(2):17-23.

[59] Hui H, McLaughlin K. Investigating current plc security issues regarding siemens s7 communications and TIA portal. In5th International Symposium for ICS & SCADA Cyber Security Research 2018 2018 Aug 1. BCS Learning & Development.

[60] Gangane S, Kakade V. Base of the networking protocol–TCP/IP its design and security aspects. International Journal of Innovative Research in Computer and Communication Engineering. 2015 Apr;3(4).

[61] 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.

[62] Xi B. Adversarial machine learning for cybersecurity and computer vision: Current developments and challenges. Wiley Interdisciplinary Reviews: Computational Statistics. 2020 Sep;12(5):e1511.

[63] 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.

[64] Caviglione L. Trends and challenges in network covert channels countermeasures. Applied Sciences. 2021 Feb 11;11(4):1641.

[65] Papadogiannaki E, Ioannidis S. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. ACM Computing Surveys (CSUR). 2021 Jul 13;54(6):1-35.

[66] Lyu M, Gharakheili HH, Sivaraman V. A survey on DNS encryption: Current development, malware misuse, and inference techniques. ACM Computing Surveys. 2022 Dec 23;55(8):1-28.

[67] De Lucia MJ, Cotton C. Detection of encrypted malicious network traffic using machine learning. InMILCOM 2019-2019 IEEE Military Communications Conference (MILCOM) 2019 Nov 12 (pp. 1-6). IEEE.

[68] Yaacoubi O. The rise of encrypted malware. Network Security. 2019 May;2019(5):6-9.

[69] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[70] Salim MM, Rathore S, Park JH. Distributed denial of service attacks and its defenses in IoT: a survey. The Journal of Supercomputing. 2020 Jul;76:5320-63.

[71] Asharf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. Electronics. 2020 Jul 20;9(7):1177.

[72] Tank D, Aggarwal A, Chaubey N. Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. International Journal of Information Technology. 2019 Feb:1-6.

[73] Almutairy NM, Al-Shqeerat KH, Al Hamad HA. A taxonomy of virtualization security issues in cloud computing environments. Indian Journal of Science and Technology. 2019;12(3):1-9.

[74] Pandi GS, Shah S, Wandra KH. Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. Procedia Computer Science. 2020 Jan 1;167:163-73.

[75] Surya P, Pachauri P, Pachauri A, Chaturvedi P, Yadav SA, Singh D. Virtualization Risks and associated Issues in Cloud Environment. In2021 International Conference on Technological Advancements and Innovations (ICTAI) 2021 Nov 10 (pp. 521-525). IEEE.

[76] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[77] Mao B, Liu J, Wu Y, Kato N. Security and privacy on 6g network edge: A survey. IEEE communications surveys & tutorials. 2023 Feb 14.

[78] Wang C, Yuan Z, Zhou P, Xu Z, Li R, Wu DO. The Security and Privacy of Mobile Edge Computing: An Artificial Intelligence Perspective. IEEE Internet of Things Journal. 2023 Aug 11.

[79] Xu W, Yang Z, Ng DW, Levorato M, Eldar YC, Debbah M. Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing. IEEE journal of selected topics in signal processing. 2023 Jan 23;17(1):9-39.

[80] Kazmi SH, Qamar F, Hassan R, Nisar K, Chowdhry BS. Survey on joint paradigm of 5G and SDN emerging mobile technologies: Architecture, security, challenges and research directions. Wireless Personal Communications. 2023 Jun;130(4):2753-800.

[81] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[82] Khan M, Ghafoor L. Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions. Journal of Computational Intelligence and Robotics. 2024 Mar 7;4(1):51-63.

[83] Savas O, Ding L, Papaleo T, McCulloh I. Adversarial attacks and countermeasures against ML models in army multi-domain operations. InArtificial Intelligence and Machine Learning for Multi-Domain Operations Applications II 2020 May 19 (Vol. 11413, pp. 235-240). SPIE.

[84] Rosenberg I, Shabtai A, Elovici Y, Rokach L. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR). 2021 May 23;54(5):1-36.

[85] Hoffman W. AI and the Future of Cyber Competition. CSET Issue Brief. 2021 Jan:1-35.

[86] Bonfanti ME. Artificial intelligence and the offence-defence balance in cyber security. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge. 2022 Feb 16:64-79.

[87] 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.

[88] Thakur M. Cyber Security Threats and Countermeasures in Digital Age. Journal of Applied Science and Education (JASE). 2024 Mar 7:1-20.

[89] Safitra MF, Lubis M, Fakhrurroja H. Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability. 2023 Sep 6;15(18):13369.

[90] Abdel-Rahman M. Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology. 2023 Jul 15;7(1):138-58.

[91] Goni A, Jahangir MU, Chowdhury RR. A Study on Cyber security: Analyzing Current Threats, Navigating Complexities, and Implementing Prevention Strategies. International Journal of Research and Scientific Innovation. 2024;10(12):507-22.

[92] Xiong G, Tong J, Xu Y, Yu H, Zhao Y. A survey of network attacks based on protocol vulnerabilities. InWeb Technologies and Applications: APWeb 2014 Workshops, SNA, NIS, and IoTS, Changsha, China, September 5, 2014. Proceedings 16 2014 (pp. 246-257). Springer International Publishing.

[93] 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.

[94] Shah SS, Ahmad AR, Jamil N, Khan AU. Memory forensics-based malware detection using computer vision and machine learning. Electronics. 2022 Aug 18;11(16):2579.

[95] Zografopoulos I, Hatziargyriou ND, Konstantinou C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal. 2023 Sep 1.

[96] Hoffmann R, Napiórkowski J, Protasowicki T, Stanik J. Measurement models of information security based on the principles and practices for risk-based approach. Procedia Manufacturing. 2020 Jan 1;44:647-54.

[97] Waseem M, Adnan Khan M, Goudarzi A, Fahad S, Sajjad IA, Siano P. Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges. Energies. 2023 Jan 11;16(2):820.

[98] Vimal S, Kalaivani L, Kaliappan M. Collaborative approach on mitigating spectrum sensing data hijack attack and dynamic spectrum allocation based on CASG modeling in wireless cognitive radio networks. Cluster Computing. 2019 Sep;22:10491-501.

[99] Tripathi N, Hubballi N. Application layer denial-of-service attacks and defense mechanisms: a survey. ACM Computing Surveys (CSUR). 2021 May 3;54(4):1-33.

[100] 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).

[101] Al-Hadhrami Y, Hussain FK. DDoS attacks in IoT networks: a comprehensive systematic literature review. World Wide Web. 2021 May;24(3):971-1001.

[102] Alashhab AA, Zahid MS, Azim MA, Daha MY, Isyaku B, Ali S. A survey of low rate ddos detection techniques based on machine learning in software-defined networks. Symmetry. 2022 Jul 29;14(8):1563.

[103] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Apr 1;127:103096.

[104] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors. 2023 Apr 17;23(8):4060.

[105] Conti M, Dargahi T, Dehghantanha A. Cyber threat intelligence: challenges and opportunities. Springer International Publishing; 2018.

[106] 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.

[107] Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG. A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials. 2020 Apr 14;22(3):1942-76.

[108] Kowalski M, Mazurczyk W. Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures. Computer Networks. 2023 Apr 23:109778.

[109] Upadhyay SK, Kumar P. Security Flaw in TCP/IP and Proposed Measures. InInternational Conference on Recent Developments in Cyber Security 2023 Jun 16 (pp. 93-107). Singapore: Springer Nature Singapore.

[110] Al-Hawawreh M, Alazab M, Ferrag MA, Hossain MS. Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms. Journal of Network and Computer Applications. 2023 Dec 4:103809.

[111] Potnurwar AV, Bongirwar VK, Ajani S, Shelke N, Dhone M, Parati N. Deep Learning-Based Rule-Based Feature Selection for Intrusion Detection in Industrial Internet of Things Networks. International Journal of Intelligent Systems and Applications in Engineering. 2023 Aug 16;11(10s):23-35.

[112] 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.

[113] Hossain A, Himel SA, Hoque MM. A Novel Approach to Mitigate TCP-IP DDoS Attack Robustness. In2023 26th International Conference on Computer and Information Technology (ICCIT) 2023 Dec 13 (pp. 1-6). IEEE.

[114] Feng Y, Li J, Sisodia D, Reiher P. On Explainable and Adaptable Detection of Distributed Denial-of-Service Traffic. IEEE Transactions on Dependable and Secure Computing. 2023 Aug 3.

[115] Verma P, Bharot N, Breslin JG, Sharma M, Chaurasia N, Vidyarthi A. Uncovering collateral damages and advanced defense strategies in cloud environments against DDoS attacks: A comprehensive review. Transactions on Emerging Telecommunications Technologies. 2024 Jan 8:e4934.

[116] Jarmon JA, Yannakogeorgos P. The Cyber Threat and Globalization: The Impact on US National and International Security. Rowman & Littlefield; 2018 Jun 26.

[117] Relia S. Cyber warfare: its implications on national security. Vij Books India Pvt Ltd; 2015 Nov 1.

[118] 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.

[119] Lewis TG. Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons; 2019 Dec 17.

[120] Van Eeten M. Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. Digital Policy, Regulation and Governance. 2017 Sep 11;19(6):429-48.

[121] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.

[122] Ani UP, He H, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology. 2017 Jan 2;1(1):32-74.

[123] Nardella G, Brammer S, Surdu I. The social regulation of corporate social irresponsibility: Reviewing the contribution of corporate reputation. International Journal of Management Reviews. 2023 Jan;25(1):200-29.

[124] 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.

[125] Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. Journal of computer and system sciences. 2014 Aug 1;80(5):973-93.

[126] Popat K, Kapadia VV. Multipath TCP security issues, challenges and solutions. InInformation, Communication and Computing Technology: 6th International Conference, ICICCT 2021, New Delhi, India, May 8, 2021, Revised Selected Papers 6 2021 (pp. 18-32). Springer International Publishing.

[127] Yousuf O, Mir RN. A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures. Information & Computer Security. 2019 May 28;27(2):292-323.

[128] Ullah F, Edwards M, Ramdhany R, Chitchyan R, Babar MA, Rashid A. Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications. 2018 Jan 1;101:18-54.

[129] Shah M, Soni V, Shah H, Desai M. TCP/IP network protocols—Security threats, flaws and defense methods. In2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) 2016 Mar 16 (pp. 2693-2699). IEEE.

[130] 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.

[131] Zhang Y. A multilayer IP security protocol for TCP performance enhancement in wireless networks. IEEE Journal on selected areas in communications. 2004 May 4;22(4):767-76.

[132] Houichi M, Jaidi F, Bouhoula A. A systematic approach for IoT cyber-attacks detection in smart cities using machine learning techniques. InInternational Conference on Advanced Information Networking and Applications 2021 Apr 27 (pp. 215-228). Cham: Springer International Publishing.

[133] Humayun M, Niazi M, Jhanjhi NZ, Alshayeb M, Mahmood S. Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering. 2020 Apr;45:3171-89.

[134] Yaacoub JP, Noura HN, Salman O, Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. International Journal of Information Security. 2022 Feb;21(1):115-58.

[135] Tripathi N, Hubballi N. Detecting stealth DHCP starvation attack using machine learning approach. Journal of Computer Virology and Hacking Techniques. 2018 Aug;14:233-44.

[136] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[137] 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.

[138] Song Z, Skuric A, Ji K. A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement. IEEE Transactions on Automation Science and Engineering. 2020 Feb 5;17(2):1030-43.

[139] Cho JH, Sharma DP, Alavizadeh H, Yoon S, Ben-Asher N, Moore TJ, Kim DS, Lim H, Nelson FF. Toward proactive, adaptive defense: A survey on moving target defense. IEEE Communications Surveys & Tutorials. 2020 Jan 3;22(1):709-45.

[140] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[141] Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (zta): A comprehensive survey. IEEE Access. 2022 May 12;10:57143-79.

[142] He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing. 2022 Jun 15;2022.

[143] Ramezanpour K, Jagannath J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. Computer Networks. 2022 Nov 9;217:109358.

[144] Enright MA, Hammad E, Dutta A. A learning-based zero-trust architecture for 6g and future networks. In2022 IEEE Future Networks World Forum (FNWF) 2022 Oct 10 (pp. 64-71). IEEE.

[145] Szymanski TH. The “cyber security via determinism” paradigm for a quantum safe zero trust deterministic internet of things (IoT). IEEE Access. 2022 Apr 21;10:45893-930.

[146] 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.

[147] Volkova A, Niedermeier M, Basmadjian R, de Meer H. Security challenges in control network protocols: A survey. IEEE Communications Surveys & Tutorials. 2018 Sep 26;21(1):619-39.

[148] Hintaw AJ, Manickam S, Aboalmaaly MF, Karuppayah S. MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT). IETE Journal of Research. 2023 Aug 18;69(6):3368-97.

[149] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1;72:212-33.

[150] Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Computers & Security. 2019 Nov 1;87:101589.

[151] Lone AN, Mustajab S, Alam M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. Security and Privacy. 2023 Nov;6(6):e318.

[152] 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.

[153] Wei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1;102:902-11.

[154] Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review. 2021 Jun;54(5):3849-86.

[155] Ozkan-Ozay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, Beloev I. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. 2024 Jan 18.

[156] Adebayo OS, AbdulAziz N. An intelligence based model for the prevention of advanced cyber-attacks. InThe 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) 2014 Nov 17 (pp. 1-5). IEEE.

[157] Kallepalli K, Chaudhry UB. Intelligent Security: Applying Artificial Intelligence to Detect Advanced Cyber Attacks. InChallenges in the IoT and Smart Environments: A Practitioners' Guide to Security, Ethics and Criminal Threats 2021 Nov 27 (pp. 287-320). Cham: Springer International Publishing.

[158] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[159] Yaseen A. Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures. Quarterly Journal of Emerging Technologies and Innovations. 2024 Jan 11;9(1):38-60.

[160] Singh S, Sharma PK, Moon SY, Moon D, Park JH. A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing. 2019 Aug 1;75:4543-74.

[161] Diro A, Chilamkurti N, Nguyen VD, Heyne W. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors. 2021 Dec 13;21(24):8320.

[162] Schmidl S, Wenig P, Papenbrock T. Anomaly detection in time series: a comprehensive evaluation. Proceedings of the VLDB Endowment. 2022 May 1;15(9):1779-97.

[163] Kim S, Seo H, Lee EC. Advanced Anomaly Detection in Manufacturing Processes: Leveraging Feature Value Analysis for Normalizing Anomalous Data. Electronics. 2024 Apr 5;13(7):1384.

[164] Wolff ED, GroWlEy KM, Lerner MO, Welling MB, Gruden MG, Canter J. Navigating the solarwinds supply chain attack. Procurement Law.. 2021;56:3.

[165] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA, Invernizzi L, Kallitsis M, Kumar D. Understanding the mirai botnet. In26th USENIX security symposium (USENIX Security 17) 2017 (pp. 1093-1110).

[166] 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.

[167] Zou Y, Mhaidli AH, McCall A, Schaub F. " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. InFourteenth Symposium on Usable Privacy and security (soups 2018) 2018 (pp. 197-216).

[168] Hsiao SC, Kao DY. The static analysis of WannaCry ransomware. In2018 20th international conference on advanced communication technology (ICACT) 2018 Feb 11 (pp. 153-158). IEEE.

[169] Lika RA, Murugiah D, Brohi SN, Ramasamy D. NotPetya: cyber attack prevention through awareness via gamification. In2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) 2018 Jul 11 (pp. 1-6). IEEE.

[170] Ogu RE, Ikerionwu CI, Ayogu II. Leveraging artificial intelligence of things for anomaly detection in advanced metering infrastructures. In2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA) 2021 Feb 23 (pp. 16-20). IEEE.

[171] Luo Y, Xiao Y, Cheng L, Peng G, Yao D. Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR). 2021 May 23;54(5):1-36.

[172] 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.

[173] Singh V, Pandey SK. Revisiting cloud security threats: IP spoofing. InSoft Computing: Theories and Applications: Proceedings of SoCTA 2018 2020 (pp. 225-236). Springer Singapore.

[174] 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) 2024 Mar 4 (pp. 181-181). IEEE Computer Society.

[175] AL-Hawamleh A. Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems. 2024 Mar 10;15(1):1315-31.

[176] Cox DJ, Jennings AM. The promises and possibilities of artificial intelligence in the delivery of behavior analytic services. Behavior Analysis in Practice. 2024 Mar;17(1):123-36.

[177] Ooi SE, Beuran R, Kuroda T, Kuwahara T, Hotchi R, Fujita N, Tan Y. Intent-driven secure system design: Methodology and implementation. Computers & Security. 2023 Jan 1;124:102955.

[178] 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.

[179] Baddi Y, Sebbar A, Zkik K, Maleh Y, Bensalah F, Boulmalf M. MSDN-IoT multicast group communication in IoT based on software defined networking. Journal of Reliable Intelligent Environments. 2024 Mar;10(1):93-104.

[180] Gupta N, Maashi MS, Tanwar S, Badotra S, Aljebreen M, Bharany S. A comparative study of software defined networking controllers using mininet. Electronics. 2022 Aug 29;11(17):2715.

[181] Hussain MZ, Hanapi ZM. Efficient secure routing mechanisms for the low-powered IoT network: A literature review. Electronics. 2023 Jan 17;12(3):482.

[182] Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: Evolution, concerns and security challenges. Sensors. 2021 Mar 5;21(5):1809.

[183] Dhar S, Khare A, Dwivedi AD, Singh R. Securing IoT devices: A novel approach using blockchain and quantum cryptography. Internet of Things. 2024 Apr 1;25:101019.

[184] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[185] Guo W, Xu J, Pei Y, Yin L, Jiang C, Ge N. A distributed collaborative entrance Defense framework against DDoS attacks on satellite internet. IEEE Internet of Things Journal. 2022 May 18;9(17):15497-510.

[186] Bhatia S, Behal S, Ahmed I. Distributed denial of service attacks and defense mechanisms: current landscape and future directions. Versatile Cybersecurity. 2018:55-97.

[187] Abuarqoub A, Abuarqoub S, Alzu'bi A, Muthanna A. The impact of quantum computing on security in emerging technologies. InThe 5th International Conference on Future Networks & Distributed Systems 2021 Dec 15 (pp. 171-176).

[188] Cui W, Dou T, Yan S. Threats and opportunities: Blockchain meets quantum computation. In2020 39th Chinese control conference (CCC) 2020 Jul 27 (pp. 5822-5824). IEEE.

[189] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access. 2020 Jan 23;8:21091-116.

[190] Xu Y, Zhang C, Wang G, Qin Z, Zeng Q. A blockchain-enabled deduplicatable data auditing mechanism for network storage services. IEEE Transactions on Emerging Topics in Computing. 2020 Jun 29;9(3):1421-32.