World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Performance, privacy and security issues at the TCP internet layer

Ogweno Jeremiah okeyo *

Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya.

World Journal of Advanced Research and Reviews, 2024, 21(03), 1386–1410

Publication history: Received on 01 February 2024; revised on 13 March 2024; accepted on 15 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0811

Abstract

The rapid growth of internet-based services and applications has revolutionized the way we communicate, interact, and conduct business. However, this widespread connectivity also brings forth numerous challenges related to performance and privacy security at the internet layer. This paper aims to provide a comprehensive analysis of the various issues that arise in this context, highlighting their impact on user experience, data protection, and network efficiency, to address performance concerns; the research paper investigates the factors affecting internet Layer. Through extensive research studies, the paper examines the impact of network congestion, routing inefficiencies, and protocol limitations on the overall performance of internet-based services. This research delves into the vulnerabilities and risks associated with the internet layer. It investigates the potential threats posed by malicious actors, including hackers, data breaches, and unauthorized access to sensitive information. The findings of this research contribute to a comprehensive understanding of the interplay between performances and privacy security issues at the internet layer. By identifying the key challenges and potential solutions, this study provides valuable insights for network administrators, service providers, policymakers, and end-users to optimize performance while ensuring robust privacy and security measures. Ultimately, this research aims to foster a safer and more efficient internet ecosystem for all stakeholders.

Keywords: TCP/I; Networks; Attacks; Protocols; Security; Privacy

1. Introduction

The Internet Layer of the TCP/IP model aligns with the Layer 3 (Network) layer of the OSI model. This is where IP addresses and routing live. When data is transmitted from a node on one LAN to a node on a different LAN, the Internet Layer is used. IPv4, IPv6, ICMP, and routing protocols (among others) are Internet Layer TCP/IP protocols [1] [2]. The Internet layer, so called because of the addressing scheme that makes communications possible across a network of networks, or internetwork, is responsible for packaging, addressing, and routing the data. When this layer was originally conceived, the Internet as we know it today did not exist. The concept behind this layer was to define a framework for two computers to connect to one another to share data. This laid the foundation for widespread internetworking, which led to what we now know as the Internet. Before data can be sent out over the Network Interface, it must have a standard format, size, and addressing scheme. The Network Interface layer is responsible only for taking the data it is given and translating that to signals on a physical medium. The Internet layer defines packet structure (what each bit of a data segment means), addressing, and routing [3]. As shown in Figure 1, the Internet layer is the third layer in TCP/IP model, and it is equivalent to the network layer in the OSI model. The main function for the Internet layer is to handle communication from one PC to another. This layer is responsible to request and send a packet from the transport layer by knowing to which PC it will be delivered [4] [5].

At the TCP/IP internet layer, performance, privacy, and security issues [6] intersect in complex ways, influencing the overall functionality and reliability of internet communications. Performance concerns often revolve around the efficient routing of data packets across vast networks, where factors such as network congestion, packet loss, and

* Corresponding author: Ogweno Jeremiah okeyo

latency can degrade user experience [7]. TCP/IP's routing protocols, such as Border Gateway Protocol (BGP), are susceptible to attacks like route hijacking and spoofing, which not only impact performance by causing data to be routed inefficiently but also raise security concerns by potentially exposing sensitive information to unauthorized parties [8]-[12]. Furthermore, as the internet continues to grow in scale and complexity, scalability becomes a performance challenge at the TCP/IP internet layer, requiring constant optimization efforts to maintain network efficiency and responsiveness.

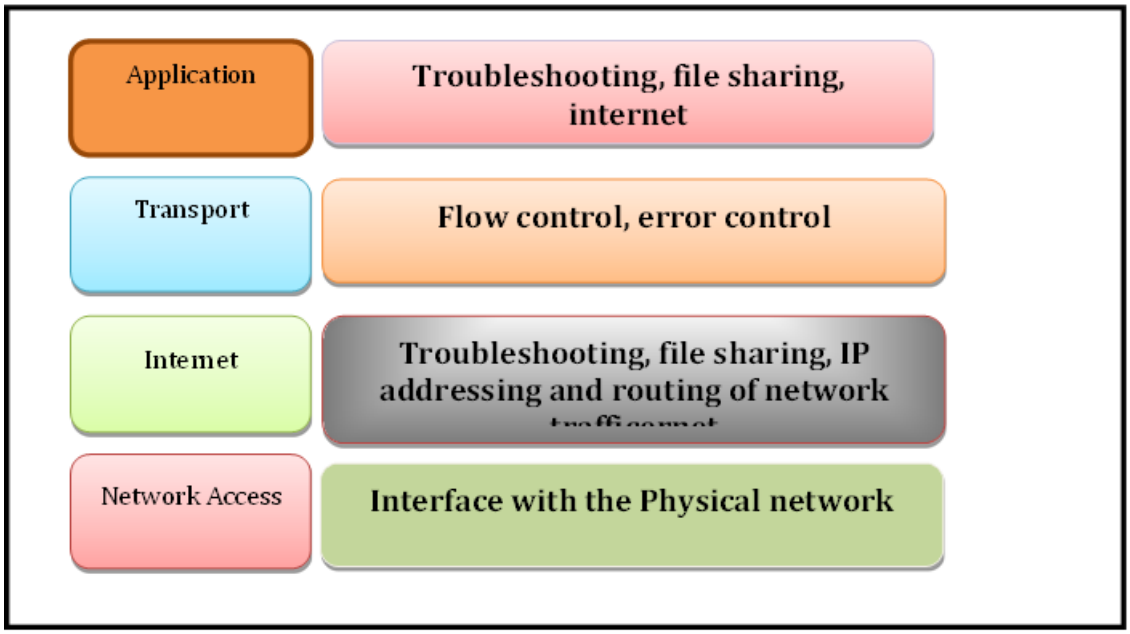

Figure 1 TCP/IP Protocol

Privacy issues at the TCP/IP internet layer stem from the inherent lack of encryption and authentication mechanisms, leaving data vulnerable to interception and manipulation by malicious actors [13]. Without encryption, data transmitted across the internet can be intercepted at various points along its journey, compromising user privacy and confidentiality. Additionally, the absence of strong authentication mechanisms leaves TCP/IP networks susceptible to unauthorized access, allowing attackers to masquerade as legitimate users or devices and gain unauthorized access to sensitive information [14]-[18] Privacy-enhancing technologies such as Virtual Private Networks (VPNs) and Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption protocols help mitigate these risks, but their adoption and implementation remain uneven across the internet landscape, leaving many users exposed to privacy breaches.

According to [19], security issues at the TCP/IP internet layer encompass a wide range of threats, including Distributed Denial of Service (DDoS) attacks, packet sniffing, and IP spoofing. DDoS attacks exploit vulnerabilities in TCP/IP protocols to flood targeted servers or networks with an overwhelming volume of traffic, disrupting services and causing downtime. Packet sniffing techniques allow attackers to intercept and analyze data packets traversing the network, potentially exposing sensitive information such as passwords, financial transactions, or personal communications [20]-[24]. IP spoofing involves forging the source IP address of data packets to disguise the attacker's identity or launch attacks on unsuspecting targets, undermining the integrity and trustworthiness of TCP/IP communications. Mitigating these security risks requires a multi-faceted approach, including the implementation of robust network security measures, regular vulnerability assessments, and user education initiatives to raise awareness about safe internet practices and privacy-enhancing technologies.

1.1. Motivation

The rapid growth and widespread use of the internet have brought about numerous benefits and opportunities in various aspects of our lives. However, with this increased connectivity comes a range of challenges and concerns related to performance, privacy, and security. These issues have become increasingly important as more individuals, businesses, and organizations rely on the internet for their daily activities. The internet layer, which is responsible for routing and forwarding data packets across different networks, plays a crucial role in the overall functioning of the internet It serves as the foundation for various internet protocols and technologies that enable efficient communication and data exchange between different devices and systems. Given the critical role of the internet layer, it is essential to

thoroughly understand the performance, privacy, and security issues associated with this layer. This understanding is crucial for researchers, network administrators, policymakers, and other stakeholders to develop effective solutions and strategies to address these challenges.

1.2. Overview of TCP/IP Model

The TCP/IP Protocol Suite is a group of different communication protocols working through the Internet and other private communication networks, and it carries most of the essential services running over the network. It provides end-to-end connectivity by establishing, maintaining, and releasing connections between the sender and receiver. It provides for flow control, error control, IP addressing and the routing of network traffic and an interface between the node and the physical network [25]. Figure 2 shows the communication model in TCP/IP networks.

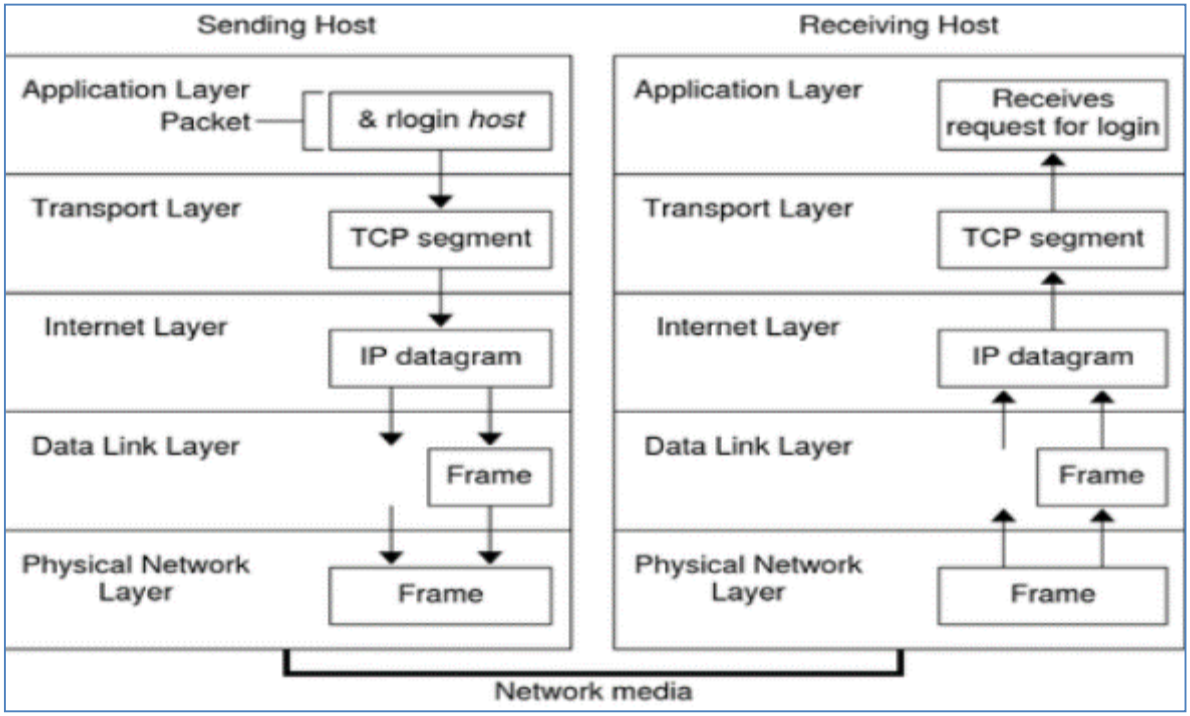

Figure 2 TCP/IP communication model

At the Internet layer, IP is responsible for routing datagrams (packets) from host to host. IP does not guarantee the delivery of datagrams, but it tries to deliver them as best. If a datagram cannot be delivered, IP will return an error message to the source host. The TCP/IP protocol suite is the most commonly used protocol suite on the Internet today, and it is also the protocol suite used by most LANs and WANs [26], [27].

2. Literature Review

The Internet has become an integral part of our daily lives, enabling seamless communication, information sharing, and access to various services [28]. However, as the Internet grows in scale and complexity, it also gives rise to several challenges related to performance, privacy, and security. This literature review aims to explore the existing research on these issues at the Internet layer;

Xaminer [29] the first Internet cross-layer resilience analysis tool, to evaluate the interplay between physical and network-layer failures, Using a cross-layer Internet map [30] and a failure event model, Xaminer generates a risk profile encompassing a cross-layer impact report, critical infrastructure identification at each layer, and the discovery of trends and patterns under different failure event settings. Xaminer's key strengths lie in its adaptability to diverse disaster scenarios, the ability to assess risks at various granularities, and the capability to generate joint risk profiles for multiple events. We demonstrate Xaminer's capabilities in cross-layer analysis across a spectrum of disaster event models and regions, showcasing its potential role in facilitating well-informed decision-making for resilience planning and deployments.

The review also delves on several factors which plays a crucial role in facilitating data transmission and routing.

2.1. Performance Issues

Scalability: One of the primary concerns at the Internet layer is scalability [30]-[33]. As the number of connected devices and users continues to increase, the current Internet infrastructure faces challenges in efficiently handling the growing traffic demands. Researchers have proposed various solutions such as network address translation (NAT), quality of service (QoS) mechanisms, and IPv6 adoption to address scalability issues.

Traffic Engineering: Efficient management of network traffic is crucial for maintaining optimal performance. Researchers have explored different techniques like traffic engineering protocols [34] traffic classification algorithms, and load balancing mechanisms to enhance network performance and minimize congestion [35].

Latency and Delay: The delay experienced during data transmission can significantly impact user experience. Studies have focused on reducing latency through techniques like caching, content delivery networks (CDNs), and protocol optimizations such as Multipath TCP (MPTCP) to improve response times and enhance overall performance [36]-[38].

2.2. Privacy Issues

IP Address Tracking: The use of IP addresses as unique identifiers raises concerns about user privacy [39]. IP address tracking refers to the technique of monitoring and logging the Internet Protocol (IP) addresses that access a network or website. This process is essential for various purposes, including network management, security, and analytics. By tracking IP addresses, administrators can identify where traffic is coming from, detect and respond to unauthorized access or malicious activities such as hacking attempts and denial of service (DoS) attacks, and enforce access controls and policies [40]-[44]. Additionally, IP address tracking allows for the collection of data for analytics, providing insights into user behavior, demographics, and preferences, which can be invaluable for optimizing website performance and targeting content or advertisements. However, this practice also raises privacy concerns, as it involves the collection and sometimes the storage of data that can potentially be used to identify individual users, highlighting the importance of balancing operational and security needs with user privacy rights. Researchers have investigated techniques like IP address obfuscation, anonymous routing protocols (e.g., Tor), and the use of virtual private networks (VPNs) to protect user privacy and prevent unauthorized tracking or surveillance [45], [46].

Traffic Analysis: Adversaries can perform traffic analysis to infer sensitive information about users' online activities [47]. According to [48], TCP traffic analysis involves the examination and interpretation of the flow of packets over TCP (Transmission Control Protocol) connections to understand network behavior, identify potential security threats, and optimize performance. By analyzing the characteristics of TCP traffic, such as volume, packet sizes, timing, and the sequence of TCP flags (e.g., SYN, ACK), network administrators and security analysts can detect anomalies that may indicate malicious activities like port scans, denial-of-service attacks, or data exfiltration attempts [49], [50]. Furthermore, TCP traffic analysis helps in assessing network efficiency [51], identifying bottlenecks, and understanding user behavior, thereby enabling better network management and planning. However, sophisticated encryption techniques and the use of secure protocols like TLS/SSL can challenge traffic analysis efforts by obscuring packet contents, thus requiring advanced tools and techniques for effective analysis while respecting privacy and security protocols. Researchers have proposed various countermeasures such as traffic padding, traffic shaping, and encryption techniques to prevent traffic analysis attacks and preserve user privacy.

Location Privacy: Location-based services raise concerns about the disclosure of users' physical whereabouts. TCP location-based services leverage the Transmission Control Protocol (TCP) along with geographical data and IP address mapping to deliver content and services tailored to the user's physical location [52], [53]. These services encompass a wide range of applications, from location-specific advertising and personalized content delivery to local weather forecasts and navigation aids. By analyzing the IP address of a user's device, which can give a rough estimate of its geographical location, service providers can customize the information and services offered to enhance user experience and relevance. However, the accuracy of TCP/IP-based location determination can vary significantly, influenced by factors such as the method used for assigning IP addresses and the use of VPNs or proxy servers, which can obscure the device's actual location [54]-[57]. Despite these challenges, TCP location-based services represent a crucial intersection of network technology and geographic information systems, offering significant benefits for both users and providers by delivering more personalized and location-aware online experiences. Studies have examined approaches like k-anonymity spatial cloaking, and privacy-preserving location-based services to safeguard users' location privacy while still enabling the benefits of location-based applications [58], [59].

2.3. Security Issues

Denial of Service (DoS) Attacks: The Internet layer is vulnerable to DoS attacks that aim to disrupt network services by overwhelming the target with excessive traffic [60]. According to [61], DoS attacks at the TCP/IP internet layer are malicious attempts to disrupt the normal functioning of targeted servers, services, or networks by overwhelming them with a flood of internet traffic as shown in Figure 3.

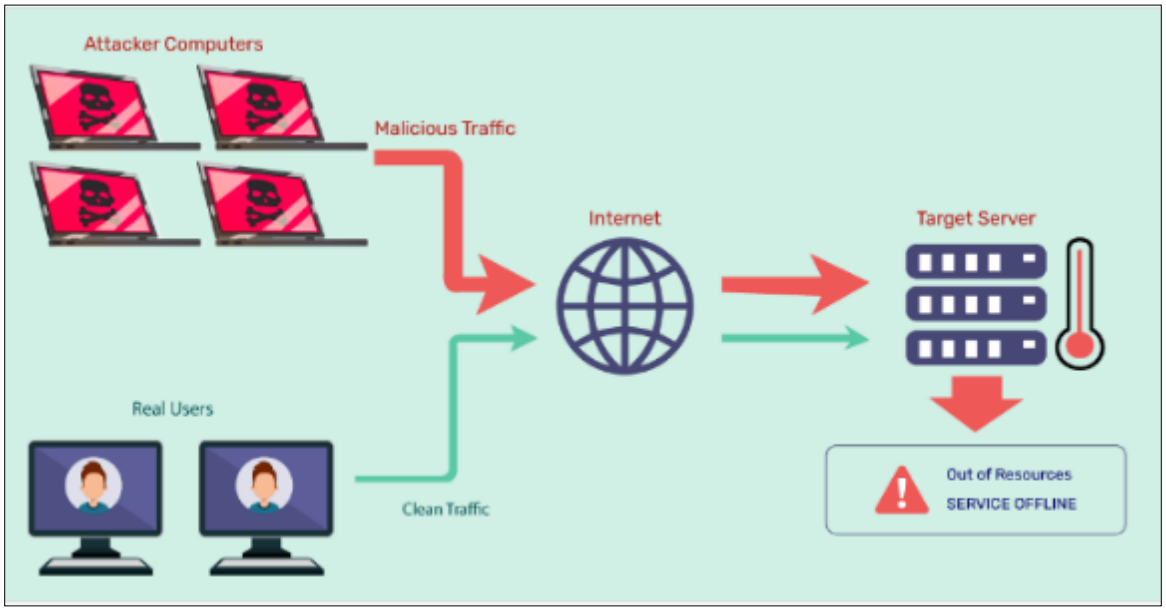

Figure 3 DoS attack

These attacks exploit the fundamental mechanisms of the TCP/IP protocol suite, such as the three-way handshake process in TCP, by sending numerous connection requests faster than the target can process them, leading to saturation of bandwidth or depletion of system resources. This prevents legitimate users from accessing the services or resources they need. Attackers may use various techniques, including SYN flood attacks, where a surge of SYN requests is sent without completing the handshake with ACK responses, or ICMP flooding, which overwhelms the target with ping requests [62], [63]. By exploiting vulnerabilities inherent in the way TCP/IP protocols operate, DoS attacks can cause significant disruptions, making the mitigation and prevention of such attacks a critical concern for network administrators and security professionals. Researchers have explored various defense mechanisms, including rate limiting, traffic filtering, and anomaly detection, to mitigate the impact of DoS attacks and ensure network availability.

IP Spoofing: IP spoofing allows attackers to impersonate legitimate sources, leading to potential security breaches. IP spoofing at the TCP/IP internet layer involves the manipulation of packet headers to alter the source IP address, making the traffic appear as though it is coming from a different, trusted source rather than the attacker's actual location [64], [65]. Figure 4 depicts how IP spoofing attacks are perpetrated. This technique is often used in various cyber attacks, including Denial of Service (DoS) attacks, to conceal the attacker's identity and location, bypass IP address-based authentication and access controls, and exploit trust relationships between networked systems. By masquerading as a legitimate entity, attackers can significantly increase the chances of their malicious packets being accepted and processed by the target system, facilitating unauthorized access, data breaches, or service disruptions [66]-[69]. The fundamental statelessness and lack of authentication at the internet layer of the TCP/IP model inherently allow such vulnerabilities, making IP spoofing a persistent threat that necessitates robust countermeasures, such as packet filtering, ingress and egress filtering, and the implementation of security protocols that provide mutual authentication and encryption. Researchers have proposed techniques like ingress filtering, source address validation, and cryptographic mechanisms to detect and prevent IP spoofing attacks [70], [71].

Routing Attacks: The Internet layer's routing protocols are susceptible to attacks that can disrupt communication or divert traffic [72], [73]. These attacks exploit vulnerabilities in the internet's routing protocols, such as Border Gateway Protocol (BGP) and Routing Information Protocol (RIP), to manipulate or disrupt the path that data packets take across the network. Attackers can perform routing attacks through techniques such as route hijacking, where malicious actors divert traffic intended for a specific destination to an unauthorized route, potentially intercepting, modifying, or blocking the data.

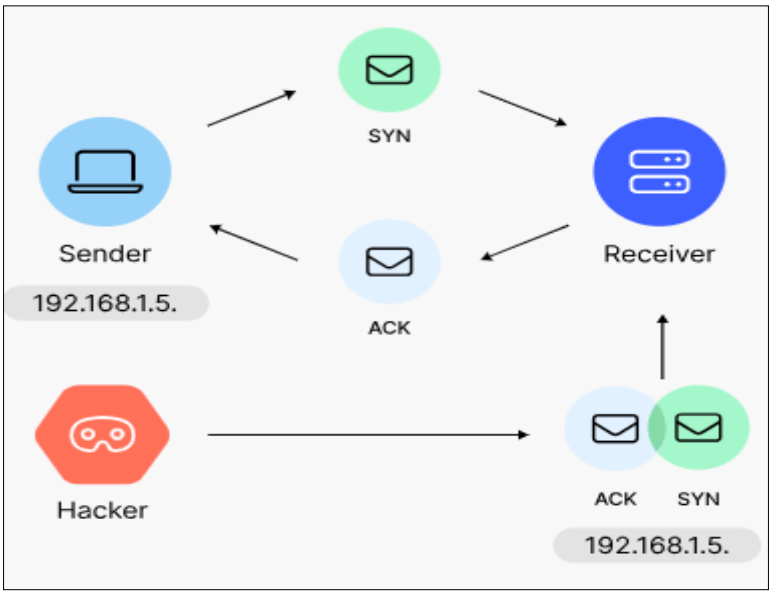

Figure 4 IP spoofing

Another example is the route poisoning attack, where false routing information is introduced into the network, causing packets to take suboptimal paths or enter routing loops, leading to delays or denial of service. These attacks compromise the integrity and availability of network communications, undermining trust in the internet's routing infrastructure [74],[75]. Addressing these threats requires the implementation of secure routing protocols, continuous monitoring of routing updates, and the adoption of best practices in network management to detect and mitigate anomalous routing behaviors [76]. Research has focused on secure routing protocols, route verification mechanisms, and anomaly detection techniques to enhance the security of routing infrastructure and prevent unauthorized route manipulation.

This literature review highlights the performance, privacy, and security challenges faced at the Internet layer. Researchers have proposed various solutions to address these issues, ranging from protocol optimizations and privacy-enhancing techniques to advanced security mechanisms. However, as the Internet continues to evolve, it is crucial to further explore and develop innovative approaches to ensure a robust and secure Internet infrastructure that can meet the growing demands of users while safeguarding their privacy.

Table 1 Summary of Literature Review

Reference	Description		
[28]	Privacy can be defined as controllingwhat happens with personal information and hiding this personal information as well. There are some technologies called Privacy Enhancing Technologies (PET) that are important in achieving goals of privacy and security.	Virtual Private Networks (VPN)	VPN can provide a high level of integrity and confidentiality. VPN have zero or very little overhead onperformance. VPN enable hiding network traffic which also can be monitored or prevented.
		Transport Layer Security (TLS)	TLS is a protocol that is used in networks to enhance and support security by initiating end- to-end security into networks. TLS can enhance security in communication in client-server models. It is mostly and widely used in HTTP protocol to make it secured HTTPs. Confidentiality of IoT and integrity can be improved by using TLS. TLS is based on a global trust structure.

		DNS Security Extensions (DNSSEC)	DNSSEC is a group of protocols that use public and private keys and enhance security in DNS responses by providing layers of cryptography. DNSSEC provides data integrity and authentication of DNS response between authoritative server and DNS server. DNSSEC guarantees the integrity and authenticity of information by signing records by using the public key cryptography.
		Onion Routing	Opinion Routing is used in public networks as a communication infrastructure. Onion Routing mix and encrypts internet traffic from other different traffic sources. Onion routing is a common way to achieve anonymity for senders.
		Private Information Retrieval (PIR)	PIR enables users to download messagesfrom databases without exposing which message the user requested to download. PIR hides which user concerned about which information.
29	Security can be said to be a framework that have policies, procedure, concepts and techniques that needed to protect users and system against attackers.	Intruder Model	Dolev-Yao (DY) intruder can affect the network and can intercept sent and received messages between the IoT devices. If IoT infrastructure is DY intruder resilient, the safety will be much stronger.
		Denial-of-Service Attacks (DoS)	oS attack work on brining the networkdown and making it unavailable for users to use. Multiple system requests cause the target server or system to shut down.

3. TCP Sequence Number Prediction

TCP sequence number prediction is a type of security exploit that targets the TCP/IP protocol's mechanism for ordering data packets [77]. As shown in Figure 5, TCP connections rely on sequence numbers to ensure data is reassembled in the correct order, and that the communication between hosts remains synchronized. An attacker, by predicting the sequence numbers of a future packet in an active TCP session, can potentially inject malicious packets into the communication stream without either party's knowledge. This could allow unauthorized access to sensitive sessions, such as those for web applications or remote terminals [78], [79]. The vulnerability arises from the predictability of sequence numbers, which, in implementations where these numbers are not sufficiently randomized, can be guessed by an attacker through techniques like sniffing a few packets to infer the algorithm used for sequence number generation. Successfully predicting TCP sequence numbers can lead to session hijacking, data interception, and denial of service attacks, emphasizing the need for robust security measures, including the use of unpredictable initial sequence numbers and encryption protocols to protect data integrity and confidentiality [80], [81]. Figure 2 shows a typical TCP sequence numbers prediction attack.

The normal TCP connection establishment sequence involves a 3-way handshake. The client selects and transmits an initial sequence number ISN C, the server acknowledges it and sends its own sequence number ISN S, and the client acknowledges that. Following those three messages, data transmission may take place. The exchange may be shown schematically as follows:

C→S: SYN (ISN C)

S→C: SYN (ISN S), ACK (ISN C)

C→S: ACK (ISN S)

C→S: data

That is, for a conversation to take place, C must first hear ISN S, a more or less random number. Suppose, though, that there was a way for an intruder X to predict ISN S.

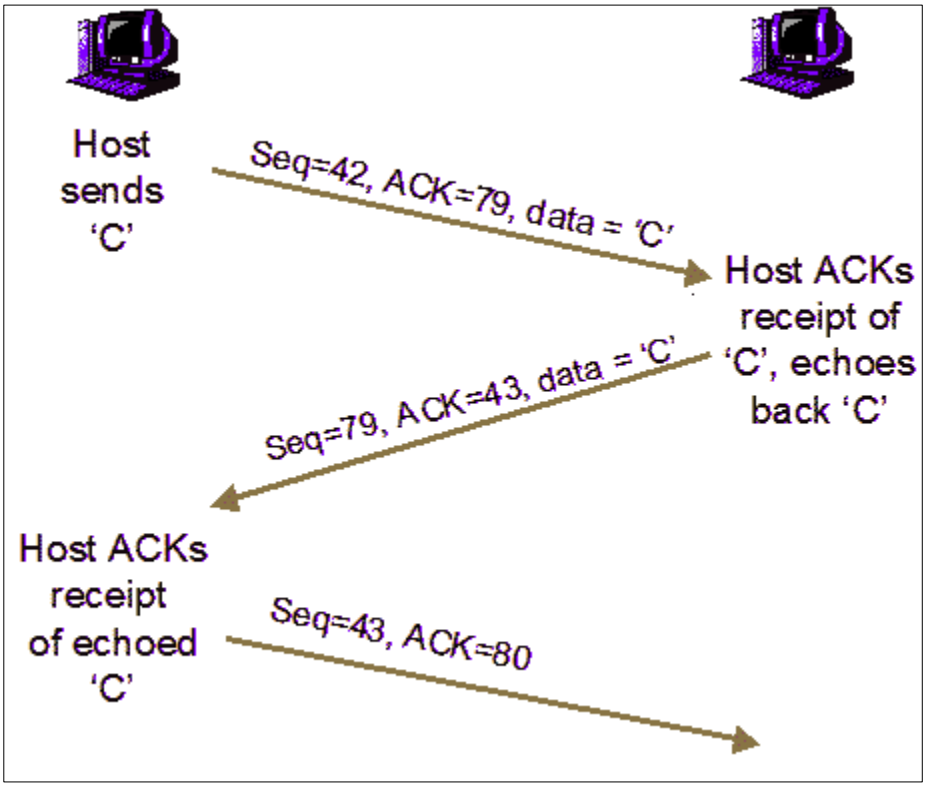

Figure 5: TCP sequence prediction attack

In that case, it could send the following sequence to impersonate trusted host T:

X→S: SYN (ISN X), SRC = T

S→T: SYN (ISN S), ACK (ISN X)

X→S: ACK (ISN S), SRC = T

X→S: ACK (ISN S), SRC = T, nasty – data

Even though the message S→T does not go to X, X was able to know its contents, and hence could send Data. If X were to perform this attack on a connection that allows command execution (i.e., the Berkeley rsh server), malicious commands could be executed. How, then, to predict the random ISN? In Berkeley systems, the initial sequence number variable is incremented by a constant amount once per second and by half that amount each time a connection is initiated. Thus, if one initiates a legitimate connection and observes the ISN S used, one can calculate, with a high degree of confidence, ISN S′ used on the next connection attempt.

Morris points out that the reply message

S→T: SYN (ISN S), ACK (ISN X)

Does not in fact vanish down a black hole; rather, the real host T will receive it and attempt to reset the connection. This is not a serious obstacle. Morris found that by impersonating a server port on T, and by flooding that port with apparent connection requests, he could generate queue overflows that would make it likely that the S→T message would be lost. Alternatively, one could wait until T was down for routine maintenance or a reboot. A variant on this TCP sequence number attack, not described by Morris, exploits the netstat service. In this attack, the intruder impersonates a host that is down. If netstat is available on the target host, it may supply the necessary sequence number information on another port; this eliminates all need to guess.

3.1. Routing

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths [82]. Routing is the process of selecting the best path using some predetermined rules. Abuse of the routing mechanisms and protocols is probably the simplest protocol-based attack available. There are a variety of ways to do this, depending on the exact routing protocols used. Some of these attacks succeed only if the remote host does source address-based authentication; others can be used for more powerful attacks [83], [84]. A number of the attacks described below can also be used to accomplish denial of service by confusing the routing tables on a host or gateway. The details are straight-forward corollaries of the penetration mechanisms, and will not be described further.

3.2. Routing Information Protocol Attacks

The Routing Information Protocol (RIP) is used to propagate routing information on local networks, especially broadcast media. Typically, the information received is unchecked [85]. This allows an intruder to send bogus routing information to a target host, and to each of the gateways along the way, to impersonate a particular host. The most likely attack of this sort would be to claim a route to a particular unused host, rather than to a network; this would cause all packets destined for that host to be sent to the intruder's machine (Diverting packets for an entire network might be too noticeable; impersonating an idle work-station is comparatively risk-free). Once this is done, protocols that rely on address-based authentication are effectively compromised. This attack can yield more subtle, and more serious, benefits to the attacker as well [86], [87]. Assume that the attacker claims a route to an active host or workstation instead. All packets for that host will be routed to the intruder's machine for inspection and possible alteration. They are then resent, using IP source address routing, to the intended destination. An outsider may thus capture passwords and other sensitive data [88]. This mode of attack is unique in that it affects outbound calls as well; thus, a user calling out from the targeted host can be tricked into divulging a password. Most of the earlier attacks discussed are used to forge a source address; this one is focused on the destination address.

3.3. Solution on Routing Information Protocol Attacks

One solution is for RIP to be more skeptical about the routes it accepts. In most environments, there is no good reason to accept new routes to your own local networks [89], [90]. A router that makes this check can easily detect intrusion attempts. Unfortunately, some implementations rely on hearing their own broadcasts to retain their knowledge of directly-attached networks. The idea, presumably, is that they can use other networks to route around local outages. While fault-tolerance is in general a good idea, the actual utility of this technique is low in many environments compared with the risks. It would be useful to be able to authenticate RIP packets; in the absence of inexpensive public-key signature schemes, this is difficult for a broadcast protocol. Even if it were done, its utility is limited; a receiver can only authenticate the immediate sender, which in turn may have been deceived by gateways further upstream [91], [92]. Even if the local routers don't implement defense mechanisms, RIP attacks carry another risk: the bogus routing entries are visible over a wide area. Any router (as opposed to host) that receives such data will rebroadcast it; a suspicious administrator almost anywhere on the local collection of networks could notice the anomaly. Good log generation would help, but it is hard to distinguish a genuine intrusion from the routing instability that can accompany a gateway crash [93], [94].

3.4. Exterior Gateway Protocol

The Exterior Gateway Protocol (EGP) is intended for communications between the core gateways and so-called exterior gateways [95], [96]. An exterior gateway, after going through a neighbor acquisition protocol, is periodically polled by the core; it responds with information about the networks it serves. These networks must all be part of its autonomous system. Similarly, the gateway periodically requests routing information from the core gateway. Data is not normally sent except in response to a poll; furthermore, since each poll carries a sequence number that must be echoed by the response, it is rather difficult for an intruder to inject a false route update [97], [98]. Exterior gateways are allowed to send exactly one spontaneous update between any two polls; this, too, must carry the sequence number of the last poll

received. It is thus comparatively difficult to interfere in an on-going EGP conversation. One possible attack would be to impersonate [99], [100] a second exterior gateway for the same autonomous system [101]. This may not succeed, as the core gateways could be equipped with a list of legitimate gateways to each autonomous system. Such checks are not currently done, however. Even if they were, they could be authenticated only by source IP address. A more powerful attack would be to claim reachability for some network where the real gateway is down. That is, if gateway X normally handles traffic for network Y, and X is down, gateway X′ could advertise a route to that network. This would allow password capture by assorted mechanisms. The main defense against this attack is topological (and quite restrictive): exterior gateways must be on the same network as the core; thus, the intruder would need to subvert not just any host, but an existing gateway or host that is directly on the main net. A sequence number attack, similar to those used against TCP, might be attempted; the difficulty here is in predicting what numbers the core gateway is using. In TCP, one can establish arbitrary connections to probe for information; in EGP, only a few hosts may speak to the core. (More accurately, the core could only speak to a few particular hosts, though as noted such checks are not currently implemented.) It may thus be hard to get the raw data needed for such an attack [102].

3.5. Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is the basic network management tool of the TCP/IP protocol suite [103]. Figure 6 shows some details of a typical ICMP connection. Surprisingly, ICMP attacks are rather difficult; still, there are often holes that may be exploited. The first, and most obvious target, is the ICMP Redirect message; it is used by gateways to advice hosts of better routes. As such it can often be abused in the same way that RIP can be [104], [105]. The complication is that a Redirect message must be tied to a particular, existing connection; it cannot be used to make an unsolicited change to the host's routing tables. Furthermore, Redirects are only applicable within a limited topology; they may be sent only from the first gateway along the path to the originating host [106]. A later gateway may not advise that host, nor may it use ICMP Redirect to control other gateways. Suppose, though, that an intruder has penetrated a secondary gateway available to a target host, but not the primary one. It may suffice to penetrate an ordinary host on the target's local network, and have it claim to be a gateway. Assume further that the intruder wishes to set up a false route to trusted host Y through that compromised secondary gateway. The following sequence may then be followed. Send a false TCP open packet to the target host, claiming to be from T. The target will respond with its own open packet, routing it through the secure primary gateway. While this is in transit, a false Redirect may be sent, claiming to be from the primary gateway, and referring to the bogus connection. This packet will appear to be a legitimate control message; hence the routing change it contains will be accepted. If the target host makes this change to its global routing tables, rather than just to the per-connection cached route, the intruder may proceed with spoofing [107] host T. Some hosts do not perform enough validity checks on ICMP Redirect messages; in such cases, the impact of this attack becomes similar to RIP-based attacks [108], [109]. ICMP may also be used for targeted denial of service attacks. Several of its messages, such as Destination Unreachable and Time to Live Exceeded, may be used to reset existing connections. If the intruder knows the local and remote port numbers of a TCP connection, an ICMP packet aimed at that connection may be forged5. Such information is sometimes not available through the netstat service [110]. A more global denial of service attack can be launched by sending a fraudulent Subnet Mask Reply message. Some hosts will accept any such message, whether they have sent a query or not; a false one could effectively block all communications with the target host.

Internet Control Message Protocol ICMP doesn't form connections [111]. Thus, netstat doesn't show anything, because there's nothing to show. It's a network layer protocol that operates in terms of discrete, isolated messages, not connections. There are no port numbers associated with ICMP as there are with TCP and UDP [112], [113]. There's no such thing as "listening for ICMP messages on port #xx" as there is with UDP. Instead, you just have a set of ICMP control messages that get passed to a host

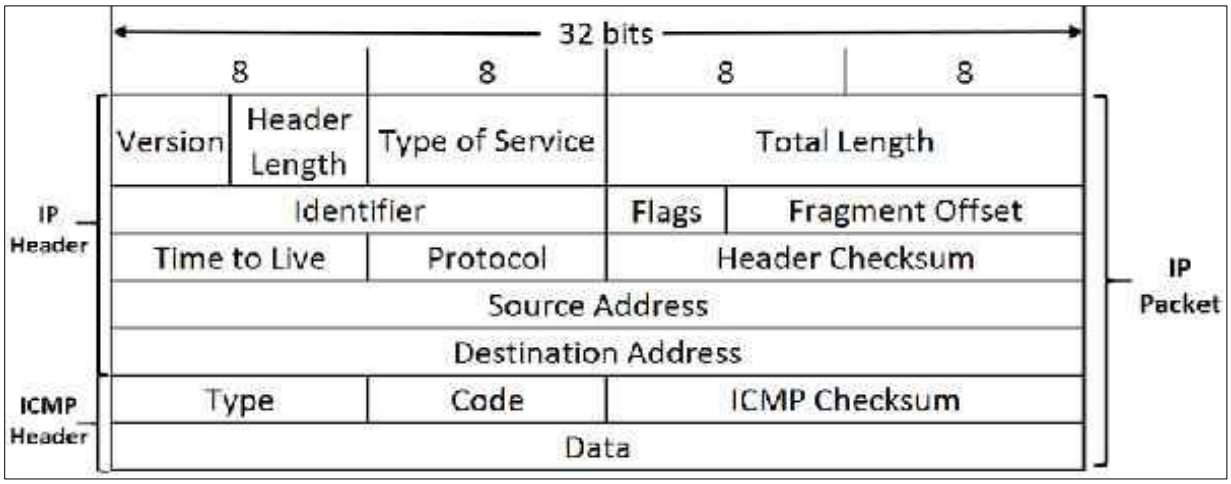

Figure 6 Information about ICMP connections

Sometimes, those messages relate to a connection, attempted connection, or other traffic using another protocol [114], such as reporting "host unreachable." Other times, they contain router advertisements and redirects. And, then there's ping and traceroute, where a pair of ICMP messages form a simple request/response.

3.6. Mitigation against Internet Control Message Protocol attacks

Most ICMP attacks are easy to defend against with just a modicum of paranoia [115], [116]. If a host is careful about checking that a message really does refer to a particular connection, most such attacks will not succeed. In the case of TCP, this includes verifying that the ICMP packet contains a plausible sequence number in the returned-packet portion. These checks are less applicable to UDP, though. A defense against Redirect attacks merits additional attention, since such attacks can be more serious. Probably, the best option is to restrict route changes to the specified connection; the global routing table should not be modified in response to ICMP Redirect messages [117]. Finally, it is worth considering whether ICMP Redirects are even useful in today's environment. They are only usable on local networks with more than one gateway to the outside world. But it is comparatively easy to maintain complete and correct local routing information. Redirect messages would be most useful from the core gateways to local exterior gateways, as that would allow such local gateways to have less than complete knowledge of the Internet; this use is disallowed, however. Subnet Mask attacks can be blocked if the Reply packet is honored only at the appropriate time. In general, a host wants to see such a message only at boot time, and only if it had issued a query; a stale reply, or an unsolicited reply, should be rejected out of hand. There is little defense against a forged reply to a genuine Subnet Mask query, as a host that has sent such a query typically has few resources with which to validate the response. If the genuine response is not blocked by the intruder, though, the target will receive multiple replies; a check to ensure that all replies agree would guard against administrative errors as well.

3.7. Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) has recently been defined to aid in network management [118], [119]. Clearly, access to such a resource must be heavily protected. The RFC states this, but also allows for a null authentication service; this is a bad idea. Even a ''read-only'' mode is dangerous; it may expose the target host to netstat-type attacks if the particular Management Information Base (MIB) used includes sequence numbers [120]. The current standardized version does not; however, the MIB is explicitly declared to be extensible.

3.8. Other attacks

Here the paper delves into some of the lesser-known but equally dangerous attacks that can compromise the security of computer systems and networks. This sub topic covers a range of attacks including Man-in-the-Middle (MitM) attacks [121], Eaves dropping, DNS spoofing [122], social engineering [123] and zero-day exploits [124]. Understanding these attacks is crucial for individuals and organizations responsible for network security. By familiarizing themselves with these attack vectors, they can better prepare and implement appropriate security measures to safeguard their networks. This includes regularly updating software, implementing strong security protocols, and educating users about potential threats and how to mitigate them [125]-[127].

3.9. Vulnerability of the Local Network

Some local-area networks, notably the Ethernet networks, are extremely vulnerable to eavesdropping and host-spoofing. If such networks are used, physical access must be strictly controlled. It is also unwise to trust any hosts on such networks if any machine on the network is accessible to untrusted personnel, unless authentication servers are used. If the local network uses the Address Resolution Protocol (ARP) more subtle forms of host-spoofing are possible [128], [129]. In particular, it becomes trivial to intercept, modify, and forward packets, rather than just taking over the host's role or simply spying on all traffic. It is possible to launch denial of service attacks by triggering broadcast storms. There are a variety of ways to do this; it is quite easy if most or all of the hosts on the network are acting as gateways. The attacker can broadcast a packet destined for a non-existent IP address. Each host, upon receiving it, will attempt to forward it to the proper destination. This alone will represent a significant amount of traffic, as each host will generate a broadcast ARP query for the destination. The attacker can follow up by broadcasting an

ARP reply claiming that the broadcast Ethernet address is the proper way to reach that destination, each susceptible host will then not only resend the bogus packet, it will also receive many more copies of it from the other susceptible hosts on the network [130], [131].

4. Internet Protocol

The Internet layer mostly depends on the communications between the nodes and deals with secure nodes from sources to destinations. As shown in Figure 7, common attacks for the Internet layer [132], [133] can be in the categories of: denial of service (DoS), disclosure, modification, destructive and escalation of privilege [134], [135].

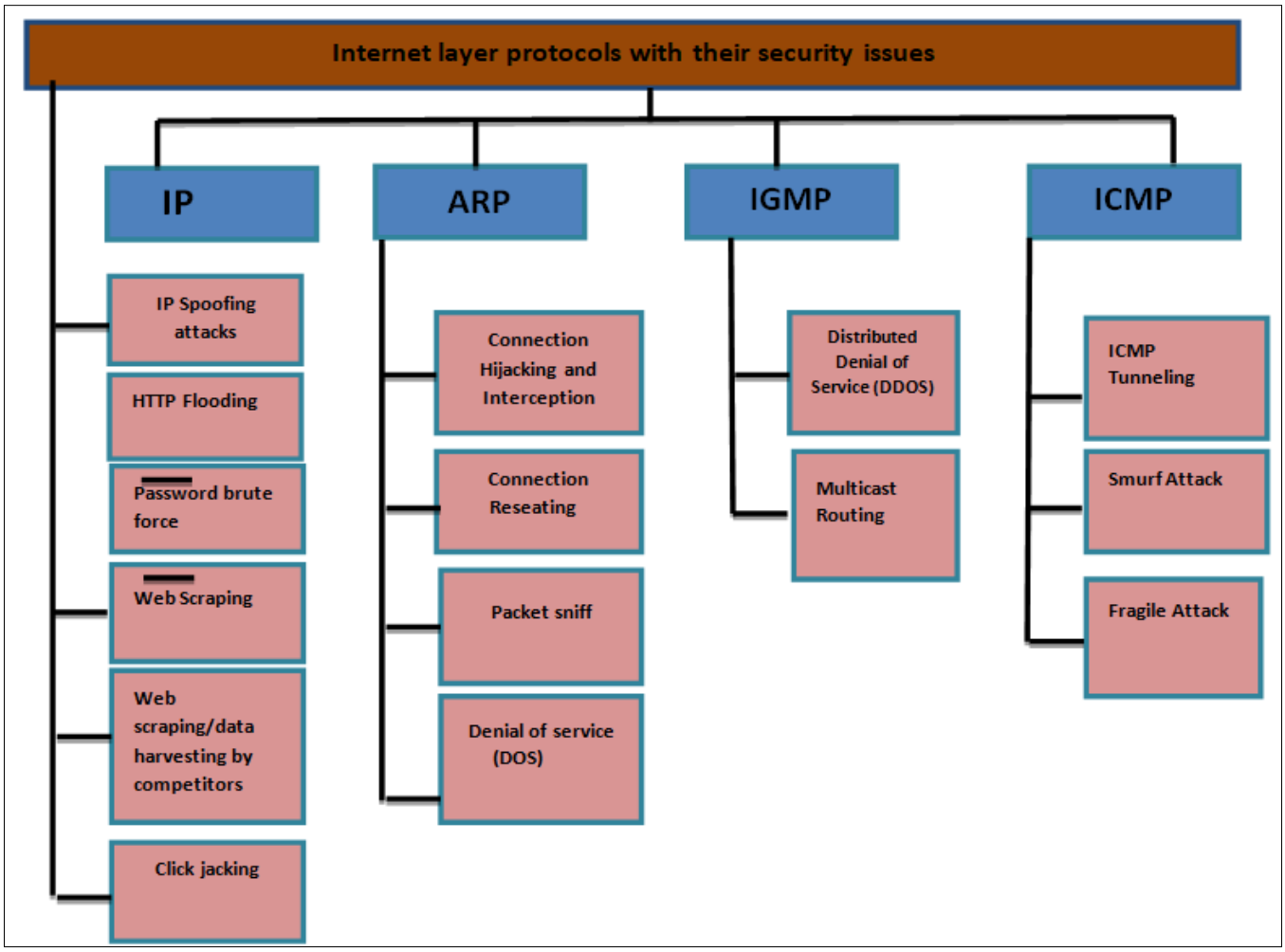

Figure 7 Internet layer protocols with their security issues

5. Comprehensive Defences

Thus far, defenses against a variety of individual attacks have been described. Several techniques are broad-spectrum defenses; they may be employed to guard against not only these attacks, but many others as well.

5.1. Authentication

Many of the intrusions described above succeed only because the target host uses the IP source address for authentication, and assumes it to be genuine. Unfortunately, there are sufficiently many ways to spoof this address that such techniques are all but worthless. Put another way, source address authentication is the equivalent of a file cabinet secured with an S100 lock; it may reduce the temptation level for more-or-less honest passers-by, but will do little or nothing to deter anyone even slightly serious about gaining entry. Some form of cryptographic authentication is needed. There are several possible approaches. Perhaps the best-known is the Needham-Schroeder algorithm [136], [137].

It relies on each host sharing a key with an authentication server; a host wishing to establish a connection obtains a session key from the Authentication server and passes a sealed version along to the destination. At the conclusion of the dialog, each side is convinced of the identity of the other. Versions of the algorithm exist for both private-key and public-key cryptosystems [138]-[140]. How do these schemes fit together with TCP/IP? One answer is obvious: with them, pre-authenticated connections can be implemented safely; without them, they are quite risky. A second answer is that the DNS provides an ideal base for authentication systems, as it already incorporates the necessary name structure, redundancy, etc [141]. To be sure, key distribution responses must be authenticated and/or encrypted; as noted, the former seems to be necessary in any event. In some environments, care must be taken to use the session key to encrypt the entire conversation; if this is not done, an attacker can take over a connection via the mechanisms described earlier [142].

5.2. Encryption

Suitable encryption can defend against most of the attacks outlined above. But encryption devices are expensive, often slow, hard to administer, and uncommon in the civilian sector. There are different ways to apply encryption; each has its strengths and weaknesses [143]-[146]. A comprehensive treatment of encryption is beyond the scope of this paper; interested readers should consult Voydock and Kent [147] or Davies and Price [148]. Link-level encryption encrypting each packet as it leaves the host computer is an excellent method of guarding against disclosure of information. It also works well against physical intrusions; an attacker who tapped in to an Ethernet cable, for example, would not be able to inject spurious packets. Similarly, an intruder who cut the line to a name server would not be able to impersonate it. The number of entities that share a given key determines the security of the network; typically, a key distribution center will allocate keys to each pair of communicating hosts.

Link-level encryption has some weaknesses, however. Broadcast packets are difficult to secure; in the absence of fast public-key cryptosystems, the ability to decode an encrypted broadcast implies the ability to send such a broadcast, impersonating any host on the network. Furthermore, link-level encryption, by definition, is not end-to-end; security of a conversation across gateways implies trust in the gateways and assurance that the full concatenated internet is similarly protected. (This latter constraint may be enforced administratively, as is done in the military sector.) If such constraints are not met, tactics such as source-routing attacks or RIP-spoofing may be employed. Paranoid gateways [149] can be deployed at the entrance to security domains; these might, for example, block incoming RIP packets or source-routed packets. Many portions of the DARPA [150] Internet employ forms of link encryption. All Defense Data Network (DDN) IMP-to-IMP trunks use DES encryption, even for non-classified traffic; classified lines use more secure cryptosystems [151], [152]. These, however, are point-to-point lines, which are comparatively easy to protect. A multi-point link encryption device for TCP/IP is the Blacker Front End (BFE) [153], [154]. The BFE looks to the host like an X.25 DDN interface, and sits between the host and the actual DDN line. When it receives a call request packet specifying a new destination, it contacts an Access Control Center (ACC) for permission, and a Key Distribution Center (KDC) for cryptographic keys. If the local host is denied permission to talk to the remote host, an appropriate diagnostic code is returned [155], [156].

A special ‘‘Emergency Mode’’ is available for communications to a restricted set of destinations at times when the link to the KDC or ACC is not working. The permission-checking can, to some extent, protect against the DNS attacks described earlier. Even if a host has been misled about the proper IP address for a particular destination, the BFE will ensure that a totally unauthorized host does not receive sensitive data. That is, assume that a host wishes to send Top Secret data to some host foo. A DNS attack might mislead the host into connecting to penetrated host 4.0.0.4, rather than 1.0.0.1. If 4.0.0.4 is not cleared for Top Secret material, or is not allowed communications with the local host, the connection attempt will fail. To be sure, a denial of service attack has taken place; this, in the military world, is far less

serious than information loss. The BFE also translates the original (‘‘Red’’) IP address to an encrypted (‘‘Black’’) address, using a translation table supplied by the ACC. This is done to foil traffic analysis techniques, the bane of all multi-point link encryption schemes [157], [158].

End-to-end encryption, above the TCP level, may be used to secure any conversation, regardless of the number of hops or the quality of the links. This is probably appropriate for centralized network management applications, or other point-to-point transfers. Key distribution and management [159] is a greater problem, since there are more pairs of correspondents involved [160]. Furthermore, since encryption and decryption are done before initiation or after termination of the TCP processing, host-level software must arrange for the translation; this implies extra overhead for each such conversation10. End-to-end encryption is vulnerable to denial of service attacks, since fraudulently-injected packets can pass the TCP checksum tests and make it to the application.

A combination of end-to-end encryption and link-level encryption can be employed to guard against this. An intriguing alternative would be to encrypt the data portion of the TCP segment, but not the header; the TCP checksum would be calculated on the clear text, and hence would detect spurious packets. Unfortunately, such a change would be incompatible with other implementations of TCP, and could not be done transparently at application level. Regardless of the method used, a major benefit of encrypted communications is the implied authentication they provide. If one assumes that the key distribution center is secure, and the key distribution protocols are adequate, the very ability to communicate carries with it a strong assurance that one can trust the source host’s IP address for identification. This implied authentication can be especially important in high-threat situations. A routing attack can be used to ‘‘take over’’ an existing connection; the intruder can effectively cut the connection at the subverted machine, send dangerous commands to the far end, and all the while translate sequence numbers on packets passed through so as to disguise the intrusion. It should be noted, of course, that any of these encryption schemes provide privacy. Often that is the primary goal of such systems [161], [162].

5.3. Trusted Systems

The Orange Book [163] (TCSEC) and Red Book [164] criteria provide a framework for evaluating the security features of computer systems, including those using TCP/IP protocols [165], [166]. Let's analyze how systems rated B1 or higher in these criteria would protect against the described attacks, considering the military security model outlined [167]:

B2 or Higher: Systems rated B2 or higher are generally immune to the attacks described [168]. These systems enforce strong mandatory access controls (MAC) and have robust security mechanisms in place. In the military security model, these systems would ensure that processes can only read or write to objects with matching or higher security labels.

B1: B1-level systems are vulnerable to some of the attacks but not all. While they may have discretionary access controls (DAC) and auditing capabilities, they might not offer the same level of protection as higher-rated systems. In the military security model, B1 systems may enforce access control based on security labels, but they may not provide the same level of assurance as B2 or higher systems.

C2: Systems rated C2 are susceptible to the attacks described. These systems may lack robust security features and rely more on user discretion and procedural controls. In the military security model, C2 systems may have weaker enforcement of access controls, making them more vulnerable to attacks.

The military security model ensures that all objects and data have security labels indicating their sensitivity levels. Processes are similarly labeled, and access to objects is restricted based on these labels. For TCP/IP connections, the security label of a process is encoded in the IP security option, ensuring that the remote TCP endpoint validates the label on received packets against the receiving process's label. While B1 or higher-rated systems offer some level of protection against the described attacks, systems rated B2 or higher are generally immune due to their stronger security mechanisms, including mandatory access controls [169]. The military security model ensures that access to objects and data is controlled based on security labels, which are enforced in TCP/IP connections to prevent unauthorized access.

5.4. Key findings

The analysis points out several crucial considerations for network security:

IP Source Address for Authentication: Relying solely on the IP source address for authentication is highly risky [170]. IP addresses can be spoofed or manipulated, making them unreliable for authentication purposes. Additional authentication mechanisms, such as cryptographic protocols or user credentials, should be used to enhance security. Cryptographic protocols are sets of rules and procedures that govern the secure communication between parties over

a network or other communication channels. These protocols utilize cryptographic techniques such as encryption, digital signatures, and key exchange to ensure confidentiality, integrity, and authenticity of the transmitted data [171], [172]. Common cryptographic protocols include SSL/TLS for securing web communications, IPsec for securing IP communications, and PGP/GPG for encrypting emails. Cryptographic protocols play a crucial role in safeguarding sensitive information from unauthorized access and manipulation, whether it's personal data, financial transactions, or confidential business communications [173]-[178]. However, the effectiveness of cryptographic protocols relies on the strength of cryptographic algorithms, proper implementation, and regular updates to address emerging threats and vulnerabilities, highlighting the ongoing need for robust security measures to protect against evolving cyber threats.

Sequence Number Attacks: Sequence numbers are vital for many protocols but must be chosen unpredictably to prevent attacks [179]. Predictable sequence numbers can be exploited by attackers to hijack connections or inject malicious data. Preventing sequence number attacks, a type of security exploit targeting the TCP/IP protocol's sequence numbers, requires implementing several protective measures. Firstly, ensuring randomization of initial sequence numbers can make prediction attacks significantly more difficult. Employing strong encryption protocols such as TLS/SSL can mitigate the risk of eavesdropping and interception, safeguarding the confidentiality of sequence numbers and data [180]. Additionally, implementing network intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help detect and block malicious activities, including attempts to manipulate TCP sequence numbers. Regular security audits and updates to network infrastructure and protocols are essential for addressing vulnerabilities and staying ahead of emerging threats [181], [182]. Furthermore, educating users and network administrators about the risks associated with sequence number attacks and promoting best practices in network security can enhance overall resilience against such exploits [183]. Efforts should be made to ensure that sequence numbers are not easily guessable, even by users on the same system.

Minimizing Gratuitous Disclosure of Information: Hosts should avoid gratuitously giving away information, especially sensitive data [184]. For example, services like finger servers should only provide information about known users, and even then, certain details may need to be withheld to mitigate security risks. According to [185], organizations should adopt strategies to limit the dissemination of unnecessary or sensitive data in various contexts, including online interactions, communications, and system configurations. This approach emphasizes the principle of least privilege, where only the minimum amount of information required for a particular task or interaction is disclosed [186], [187]. Techniques such as data minimization, anonymization, and encryption can help mitigate the risk of unauthorized access and exposure of sensitive information. Implementing privacy-enhancing technologies, robust access controls, and comprehensive data protection policies are essential for safeguarding personal and confidential information while promoting transparency and accountability in data handling practices across digital platforms and organizational settings [188], [189].

Careful Handling of Network Control Mechanisms: Network control mechanisms, such as routing protocols, should be carefully guarded against potential vulnerabilities. This is paramount for ensuring the security, reliability, and integrity of networked systems [190]. Control mechanisms, such as firewalls, intrusion detection/prevention systems, access controls, and network monitoring tools, play a critical role in managing network traffic, detecting anomalies, and enforcing security policies. However, mis-configuration or improper management of these mechanisms can inadvertently introduce vulnerabilities or disrupt network operations [191], [192]. Therefore, network administrators must exercise caution in configuring and deploying control mechanisms, ensuring they are aligned with organizational security policies and best practices [193]. Regular updates, audits, and testing are essential for identifying and addressing potential weaknesses or mis-configurations, while ongoing training and awareness efforts help ensure that personnel responsible for network management understand their roles and responsibilities in maintaining a secure and resilient network infrastructure [194]. While static routes may not be suitable for large-scale networks, the use of default routes and verifiable point-to-point routing protocols can enhance security compared to broadcast-based routing.

Overall, these points emphasize the importance of implementing robust security measures, minimizing the exposure of sensitive information, and carefully managing network control mechanisms to mitigate potential risks and vulnerabilities in network environments.

6. Conclusion

The Internet layer is a critical component of the network stack, responsible for routing data packets across networks. However, it faces challenges such as packet loss, latency, privacy breaches, and security vulnerabilities. This paper has presented a comprehensive analysis of these issues and proposes potential solutions to enhance the performance, privacy, and security of the Internet layer. By addressing the performance, privacy, and security issues at the Internet

layer, this research aims to contribute to the development of more robust and reliable network infrastructure, The proposed solutions can assist network administrators, researchers, and policymakers in enhancing the overall performance, privacy, and security of the Internet layer, thereby ensuring a more efficient and secure communication environment.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that he does not hold any conflict of interest.

References

[1] Pawar MV, Anuradha J. Network security and types of attacks in network. Procedia Computer Science. 2015 Jan 1;48:503-6.

[2] Alpern N. Eleventh hour network+: Exam n10-004 study guide. Syngress; 2009 Sep 22.

[3] Gour A, Mathews T, Behera RP. Approach towards qualification of TCP/IP network components of PFBR. Nuclear Engineering and Technology. 2022 Nov 1;54(11):3975-84.

[4] Alotaibi AM, Alrashidi BF, Naz S, Parveen Z. Security issues in protocols of TCP/IP model at layers level. International Journal of Computer Networks and Communications Security. 2017 May 1;5(5):96.

[5] 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.

[6] 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.

[7] 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.

[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] Rajeesh Kumar NV, Jaya Lakshmi N, Mallala B, Jadhav V. Secure trust aware multi-objective routing protocol based on battle competitive swarm optimization in IoT. Artificial Intelligence Review. 2023 Nov;56(Suppl 2):1685-709.

[10] Khalil A, Zeddini B. A Secure Opportunistic Network with Efficient Routing for Enhanced Efficiency and Sustainability. Future Internet. 2024 Feb 8;16(2):56.

[11] Bhatti DS, Saleem S, Imran A, Kim HJ, Kim KI, Lee KC. Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions. Scientific Reports. 2024 Feb 10;14(1):3428.

[12] 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.

[13] 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.

[14] 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.

[15] Ashrif FF, Sundararajan EA, Ahmad R, Hasan MK, Yadegaridehkordi E. Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. Journal of Network and Computer Applications. 2023 Oct 8:103759.

[16] 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.

[17] Ahmad MO, Tripathi G, Siddiqui F, Alam MA, Ahad MA, Akhtar MM, Casalino G. BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. Sensors. 2023 Mar 2;23(5):2757.

[18] 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).

[19] Patel ND, Singh A. Security Issues, Attacks and Countermeasures in Layered IoT Ecosystem. International Journal of Next-Generation Computing. 2023 Mar 1;14(2).

[20] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1;152:103322.

[21] Ganesarathinam R, Singaravelu M, Padma Pooja KN. A Detailed Review on Security Issues in Layered Architectures and Distributed Denial Service of Attacks Over IoT Environment. Cyber-Physical Systems: Foundations and Techniques. 2022 Jul 1:85-122.

[22] Hoque N, Bhattacharyya DK, Kalita JK. Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials. 2015 Jul 16;17(4):2242-70.

[23] Sundararajan A, Chavan A, Saleem D, Sarwat AI. A survey of protocol-level challenges and solutions for distributed energy resource cyber-physical security. Energies. 2018 Sep 6;11(9):2360.

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

[25] 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.

[26] Liu H. Network and Communication Protocols in Cyber-Physical Systems. InA Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations 2024 (pp. 25-88).

[27] Bahattab AA. A Survey on Packet Switching Networks. IETE Journal of Research. 2022 Mar 17:1-26.

[28] 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.

[29] Ramanathan A, Sankaran R, Abdu Jyothi S. Xaminer: An Internet Cross-Layer Resilience Analysis Tool. Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2024 Feb 21;8(1):1-37.

[30] Han C, Jornet JM, Fadel E, Akyildiz IF. A cross-layer communication module for the Internet of Things. Computer Networks. 2013 Feb 26;57(3):622-33.

[31] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. InCognitive Radio Oriented Wireless Networks and Wireless Internet: 16th EAI International Conference, CROWNCOM 2021, Virtual Event, December 11, 2021, and 14th EAI International Conference, WiCON 2021, Virtual Event, November 9, 2021, Proceedings 2022 Mar 31 (pp. 325-340). Cham: Springer International Publishing.

[32] Wu JP, Xu K. Research on next-generation Internet architecture. Journal of Computer Science and Technology. 2006 Sep;21(5):723-31.

[33] Von Behren R, Condit J, Zhou F, Necula GC, Brewer E. Capriccio: scalable threads for internet services. ACM SIGOPS Operating Systems Review. 2003 Oct 19;37(5):268-81.

[34] Mongay Batalla J, Krawiec P. Conception of ID layer performance at the network level for Internet of Things. Personal and Ubiquitous Computing. 2014 Feb;18:465-80.

[35] Xylomenos G, Polyzos GC. Internet protocol performance over networks with wireless links. IEEE network. 1999 Jul;13(4):55-63.

[36] Collina M, Bartolucci M, Vanelli-Coralli A, Corazza GE. Internet of Things application layer protocol analysis over error and delay prone links. In2014 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASMS/SPSC) 2014 Sep 8 (pp. 398-404). IEEE.

[37] Briscoe B, Brunstrom A, Petlund A, Hayes D, Ros D, Tsang J, Gjessing S, Fairhurst G, Griwodz C, Welzl M. Reducing internet latency: A survey of techniques and their merits. IEEE Communications Surveys & Tutorials. 2014 Nov 26;18(3):2149-96.

[38] 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.

[39] 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.

[40] Kyriakidou CD, Papathanasiou AM, Polyzos GC. Decentralized Identity With Applications to Security and Privacy for the Internet of Things. Computer Networks and Communications. 2023 Aug 28:244-71.

[41] Fiebig T, Gürses S, Gañán CH, Kotkamp E, Kuipers F, Lindorfer M, Prisse M, Sari T. Heads in the Clouds? Measuring Universities' Migration to Public Clouds: Implications for Privacy & Academic Freedom. InProceedings on privacy enhancing technologies symposium 2023 (Vol. 2023, No. 2, pp. 117-150).

[42] Reisinger T, Wagner I, Boiten EA. Security and privacy in unified communication. ACM Computing Surveys (CSUR). 2022 Feb 3;55(3):1-36.

[43] Özdal Oktay S, Heitmann S, Kray C. Linking location privacy, digital sovereignty and location-based services: a meta review. Journal of Location Based Services. 2023 Aug 4:1-52.

[44] 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.

[45] Bernardos CJ, Zúñiga JC, O'Hanlon P. Wi-Fi internet connectivity and privacy: Hiding your tracks on the wireless Internet. In2015 IEEE Conference on Standards for Communications and Networking (CSCN) 2015 Oct 28 (pp. 193-198). IEEE.

[46] Chung MC, Lee GM, Crespi N, Tseng CC. RFID object tracking with IP compatibility for the internet of things. In2012 IEEE International Conference on Green Computing and Communications 2012 Nov 20 (pp. 132-139). IEEE.

[47] Chen C, Asoni DE, Perrig A, Barrera D, Danezis G, Troncoso C. TARANET: Traffic-analysis resistant anonymity at the network layer. In2018 IEEE European Symposium on Security and Privacy (EuroS&P) 2018 Apr 24 (pp. 137-152). IEEE.

[48] Liaskos C, Alexandris K, Das A, Tang S, Tassiulas L. Analysis and Evaluation of Fully TCP-Compatible Backpressure-Driven Traffic Engineering. IEEE Transactions on Network Science and Engineering. 2023 Jun 5.

[49] Rawat R, Chakrawarti RK, Raj AS, Mani G, Chidambarathanu K, Bhardwaj R. Association rule learning for threat analysis using traffic analysis and packet filtering approach. International Journal of Information Technology. 2023 Aug;15(6):3245-55.

[50] Sharma A, Sharma A. QoS Parameter Analysis of TCP and UDP Traffic Over Open Flow Enabled Software Defined Network. InProceedings of International Conference on Data Science and Applications: ICDSA 2021, Volume 1 2022 (pp. 13-25). Springer Singapore.

[51] 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).

[52] Hans CY, Alhazmi K, Rao RR. Wi-Fi roaming as a location-based service. InICC 2020-2020 IEEE International Conference on Communications (ICC) 2020 Jun 7 (pp. 1-7). IEEE.

[53] Chang W, Sun D, Du Q. Intelligent Sensors for POI Recommendation Model Using Deep Learning in Location-Based Social Network Big Data. Sensors. 2023 Jan 11;23(2):850.

[54] Soni A, Dalal A, Chaurasia K, Singh MP. Emergency Response App for Enhancing Location-Based Services Using Socket. io and WebRTC. In2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM) 2023 Aug 26 (pp. 1-5). IEEE.

[55] Jiang JR, Subakti H. An Indoor Location-Based Augmented Reality Framework. Sensors. 2023 Jan 26;23(3):1370.

[56] Azzaoui N, Korichi A, Brik B, Amirat H. A survey on data dissemination in internet of vehicles networks. Journal of Location Based Services. 2023 Jul 3; 17(3):207-50.

[57] 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.

[58] Butun I, Gidlund M. Location Privacy Assured Internet of Things. ICISSP. 2019;19:1-8.

[59] Wang B, Guo Y, Li H, Li Z. k-anonymity based location privacy protection method for location-based services in Internet of Thing. Concurrency and Computation: Practice and Experience. 2023 Sep 10;35(20):e6760.

[60] Alahari HP, Yelavarthi SB. Performance analysis of denial of service dos and distributed dos attack of application and network layer of iot. In2019 Third International Conference on Inventive Systems and Control (ICISC) 2019 Jan 10 (pp. 72-81). IEEE.

[61] 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.

[62] Altulaihan E, Almaiah MA, Aljughaiman A. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. Sensors. 2024 Jan 22;24(2):713.

[63] 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.

[64] Iavich M, Gnatyuk S, Iashvili G, Odarchenko R, Simonov S. 5G Security Function and Its Testing Environment. InInternational Scientific-Practical Conference" Information Technology for Education, Science and Technics" 2022 Jun 23 (pp. 656-678). Cham: Springer Nature Switzerland.

[65] Chowdhury RR, Idris AC, Abas PE. Identifying SH-IoT devices from network traffic characteristics using random forest classifier. Wireless Networks. 2024 Jan;30(1):405-19.

[66] Rani P, Singh S, Singh K. Cloud computing security: a taxonomy, threat detection and mitigation techniques. International Journal of Computers and Applications. 2024 Feb 23:1-4.

[67] Mvah F, Kengne Tchendji V, Tayou Djamegni C, Anwar AH, Tosh DK, Kamhoua C. GaTeBaSep: game theory-based security protocol against ARP spoofing attacks in software-defined networks. International Journal of Information Security. 2024 Feb;23(1):373-87.

[68] Al-Hawawreh M, Moustafa N, Slay J. A threat intelligence framework for protecting smart satellite-based healthcare networks. Neural Computing and Applications. 2024 Jan;36(1):15-35.

[69] 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.

[70] Ali F. IP spoofing. The Internet Protocol Journal. 2007 Dec;10(4):1-9.

[71] Ehrenkranz T, Li J. On the state of IP spoofing defense. ACM Transactions on Internet Technology (TOIT). 2009 May 11;9(2):1-29.

[72] Braden R. Requirements for Internet hosts-communication layers. 1989 Oct.

[73] Hosseini M, Ahmed DT, Shirmohammadi S, Georganas ND. A survey of application-layer multicast protocols. IEEE Communications Surveys & Tutorials. 2007 Sep 24;9(3):58-74.

[74] Chao D, Xu D, Gao F, Zhang C, Zhang W, Zhu L. A Systematic Survey On Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization. IEEE Communications Surveys & Tutorials. 2024 Jan 4.

[75] 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.

[76] Murtuza S, Asawa K. Early Prevention and Mitigation of Link Flooding Attacks in Software Defined Networks. Journal of Network and Computer Applications. 2024 Apr 1;224:103832.

[77] Maxwell CN. Multipath TCP, and New Packet Scheduling Method. Scholarly Horizons: University of Minnesota, Morris Undergraduate Journal. 2023;10(1):7.

[78] Almomani A, Akour I, Manasrah AM, Almomani O, Alauthman M, Abdullah E, Al Shwait A, Al Sharaa R. Ensemble-Based Approach for Efficient Intrusion Detection in Network Traffic. Intelligent Automation & Soft Computing. 2023 Aug 1;37(2).

[79] Cao Y, Wang Z, Ding H, Zhang J, Li B. An intrusion detection system based on stacked ensemble learning for IoT network. Computers and Electrical Engineering. 2023 Sep 1;110:108836.

[80] Jadav NK, Kakkar R, Mankodiya H, Gupta R, Tanwar S, Agrawal S, Sharma R. GRADE: Deep learning and garlic routing-based secure data sharing framework for IIoT beyond 5G. Digital Communications and Networks. 2023 Apr 1;9(2):422-35.

[81] 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.

[82] Tian YC, Gao J. Network routing architecture. InNetwork analysis and architecture 2023 Oct 1 (pp. 221-273). Singapore: Springer Nature Singapore.

[83] Xing Z, Qi H, Di X, Liu J, Xu R, Chen J, Cong L. A multipath routing algorithm for satellite networks based on service demand and traffic awareness. Frontiers of Information Technology & Electronic Engineering. 2023 Jun;24(6):844-58.

[84] Vladimirov S, Vybornova A, Muthanna A, Koucheryavy A, Abd El-Latif AA. Network Coding Datagram Protocol for TCP/IP Networks. IEEE Access. 2023 Apr 11.

[85] Biswas K, Muthukkumarasamy V, Chowdhury MJ, Wu XW, Singh K. A multipath routing protocol for secure energy efficient communication in Wireless Sensor Networks. Computer Networks. 2023 May 29:109842.

[86] Deepavathi P, Mala C. Detection and prevention of various routing attacks in RPL for a smart vehicle environment using an enhanced privacy secure-RPL routing protocol. International Journal of Vehicle Information and Communication Systems. 2023;8(4):309-29.

[87] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[88] Arulselvan G, Rajaram A. Hybrid trust-based secure routing protocol for detection of routing attacks in environment monitoring over MANETs. Journal of Intelligent & Fuzzy Systems. 2023(Preprint):1-6.

[89] Yu M, Zhou M, Su W. A secure routing protocol against byzantine attacks for MANETs in adversarial environments. IEEE transactions on vehicular technology. 2008 Apr 18;58(1):449-60.

[90] Peng G, Chuanyun Z. Routing attacks and solutions in mobile ad hoc networks. In2006 International Conference on Communication Technology 2006 Nov 27 (pp. 1-4). IEEE.

[91] Kamble A, Malemath VS, Patil D. Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In2017 International Conference on Emerging Trends & Innovation in ICT (ICEI) 2017 Feb 3 (pp. 33-39). IEEE.

[92] Babu ES, Nagaraju C, Prasad MK. A secure routing protocol against heterogeneous attacks in wireless adhoc networks. InProceedings of the Sixth International Conference on Computer and Communication Technology 2015 2015 Sep 25 (pp. 339-344).

[93] Sharma P, Kherajani M, Jain D, Patel D. A study of routing protocols, security issues and attacks in network layer of internet of things framework. In2nd International conference on data, engineering and applications (IDEA) 2020 Feb 28 (pp. 1-6). IEEE.

[94] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[95] Sunita M, Mallapur SV. Optimal detection of border gateway protocol anomalies with extensive feature set. Multimedia Tools and Applications. 2023 Nov 9:1-27.

[96] Mills DL. Exterior gateway protocol formal specification. 1984 Apr.

[97] Malik A, Rashid HU, Azeem W. Analysis of border gateway protocol, its types and measures to avoid risk. Lahore Garrison University Research Journal of Computer Science and Information Technology. 2019 Sep 30;3(3):3-9.

[98] Gupta I. BIGP-a new single protocol that can work as an igp (interior gateway protocol) as well as egp (exterior gateway protocol). arXiv preprint arXiv:1207.2991. 2012 Jul 12.

[99] 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.

[100] 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.

[101] Rekhter Y, Gross P. Application of the border gateway protocol in the internet. 1995 Mar.

[102] Zang J, Song S. A Border Gateway Protocol LRA-BGP for Integrated Satellite-terrestrial Networks. InJournal of Physics: Conference Series 2023 Mar 1 (Vol. 2450, No. 1, p. 012049). IOP Publishing.

[103] Zander S, Armitage G, Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 2007 Sep 24;9(3):44-57.

[104] Feng X, Li Q, Sun K, Yang Y, Xu K. Man-in-the-middle attacks without rogue ap: When wpas meet icmp redirects. In2023 IEEE Symposium on Security and Privacy (SP) 2023 May 21 (pp. 3162-3177). IEEE.

[105] Purohit KC, Anand Kumar M, Saxena A, Mittal A. The Impact of ICMP Attacks in Software-Defined Network Environments. InInternational Conference on Computational Intelligence and Data Engineering 2022 Aug 12 (pp. 319-333). Singapore: Springer Nature Singapore.

[106] Harshita H. Detection and prevention of ICMP flood DDOS attack. International Journal of New Technology and Research. 2017;3(3):263333.

[107] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[108] Yaibuates M, Chaisricharoen R. ICMP based malicious attack identification method for DHCP. InThe 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE) 2014 Mar 5 (pp. 1-5). IEEE.

[109] Gupta N, Jain A, Saini P, Gupta V. DDoS attack algorithm using ICMP flood. In2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) 2016 Mar 16 (pp. 4082-4084). IEEE.

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

[111] Chapman DB. Network (In) Security Through IP Packet Filtering. InUSENIX Summer 1992 Sep 14 (Vol. 21).

[112] Pakanati C, Padmavathamma M, Reddy NR. Performance comparison of tcp, udp, and tfrc in wired networks. In2015 IEEE International Conference on Computational Intelligence & Communication Technology 2015 Feb 13 (pp. 257-263). IEEE.

[113] Guha S, Takeda Y, Francis P. NUTSS: A SIP-based approach to UDP and TCP network connectivity. InProceedings of the ACM SIGCOMM workshop on Future directions in network architecture 2004 Aug 30 (pp. 43-48).

[114] 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.

[115] Si W, Starobinski D, Laifenfeld M. Protocol-compliant DoS attacks on can: Demonstration and mitigation. In2016 IEEE 84th vehicular technology conference (VTC-Fall) 2016 Sep 18 (pp. 1-7). IEEE.

[116] Marchal S, Mehta A, Gurbani VK, State R, Ho TK, Sancier-Barbosa F. Mitigating mimicry attacks against the session initiation protocol. IEEE Transactions on Network and Service Management. 2015 Jul 21;12(3):467-82.

[117] Borgiani V, Moratori P, Kazienko JF, Tubino ER, Quincozes SE. Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial Internet of Things. IEEE Internet of Things Journal. 2020 Oct 5;8(6):4569-78.

[118] Shanthini J, Vijayakumar S. Modified simple network management protocol for 6Lowpan. Procedia Engineering. 2012 Jan 1;38:1024-9..

[119] Affandi A, Riyanto D, Pratomo I, Kusrahardjo G. Design and implementation fast response system monitoring server using Simple Network Management Protocol (SNMP). In2015 International Seminar on Intelligent Technology and Its Applications (ISITIA) 2015 May 20 (pp. 385-390). IEEE.

[120] McCloghrie K, Rose MT. Management Information Base for network management of TCP/IP-based internets. 1990 May.

[121] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[122] Hussain MA, Jin H, Hussien ZA, Abduljabbar ZA, Abbdal SH, Ibrahim A. DNS protection against spoofing and poisoning attacks. In2016 3rd International Conference on Information Science and Control Engineering (ICISCE) 2016 Jul 8 (pp. 1308-1312). IEEE.

[123] Ghasemi M, Saadaat M, Ghollasi O. Threats of social engineering attacks against security of Internet of Things (IoT). InFundamental Research in Electrical Engineering: The Selected Papers of The First International Conference on Fundamental Research in Electrical Engineering 2019 (pp. 957-968). Springer Singapore.

[124] Stellios I, Kotzanikolaou P, Psarakis M. Advanced persistent threats and zero-day exploits in industrial Internet of Things. Security and Privacy Trends in the Industrial Internet of Things. 2019:47-68.

[125] Berger S, Bürger O, Röglinger M. Attacks on the Industrial Internet of Things–Development of a multi-layer Taxonomy. Computers & Security. 2020 Jun 1;93:101790.

[126] De Vivo M, de Vivo GO, Isern G. Internet security attacks at the basic levels. ACM SIGOPS operating systems review. 1998 Apr 1;32(2):4-15.

[127] 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.

[128] Bruschi D, Ornaghi A, Rosti E. S-ARP: a secure address resolution protocol. In19th Annual Computer Security Applications Conference, 2003. Proceedings. 2003 Dec 8 (pp. 66-74). IEEE.

[129] Ataullah M, Chauhan N. ES-ARP: an efficient and secure address resolution protocol. In2012 IEEE Students' Conference on Electrical, Electronics and Computer Science 2012 Mar 1 (pp. 1-5). IEEE.

[130] Saulnier D, Dixit A, Nunes A, Murray V. Disaster risk factors–hazards, exposure and vulnerability. WHO guidance on research methods for health emergency and disaster risk management. 2021:151-63.

[131] Ismukhamedova A, Satimova Y, Nikiforov A, Miloslavskaya N. Practical studying of Wi-Fi network vulnerabilities. In2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC) 2016 Jul 6 (pp. 227-232). IEEE.

[132] Adeyinka O. Internet attack methods and internet security technology. In2008 Second Asia International Conference on Modelling & Simulation (AMS) 2008 May 13 (pp. 77-82). IEEE.

[133] Rai AK, Tewari RR, Upadhyay SK. Different types of attacks on integrated manet-internet communication. International Journal of Computer Science and Security. 2010 Jul;4(3):265-74.

[134] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[135] Prakash A, Kumar U. Authentication protocols and techniques: a survey. Int. J. Comput. Sci. Eng. 2018 Jun;6(6):1014-20.

[136] Dong L, Chen K. Cryptographic Protocol. Security Analysis Based on Trusted Freshness. 2012.

[137] Sharma N. A Review of Information Security using Cryptography Technique. International Journal of Advanced Research in Computer Science. 2017 May 1;8(4).

[138] Rothblum R. Homomorphic encryption: From private-key to public-key. InTheory of cryptography conference 2011 Mar 28 (pp. 219-234). Berlin, Heidelberg: Springer Berlin Heidelberg.

[139] Boneh D, Kushilevitz E, Ostrovsky R, Skeith WE. Public key encryption that allows PIR queries. InAdvances in Cryptology-CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings 27 2007 (pp. 50-67). Springer Berlin Heidelberg.

[140] 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.

[141] Zhu L, Hu Z, Heidemann J, Wessels D, Mankin A, Somaiya N. Connection-oriented DNS to improve privacy and security. In2015 IEEE symposium on security and privacy 2015 May 17 (pp. 171-186). IEEE.

[142] Schneider S. Verifying authentication protocols in CSP. IEEE Transactions on software engineering. 1998 Sep;24(9):741-58.

[143] Gupta M, Singh VP, Gupta KK, Shukla PK. An efficient image encryption technique based on two-level security for internet of things. Multimedia Tools and Applications. 2023 Feb;82(4):5091-111.

[144] Zhu Y, Wang C, Sun J, Yu F. A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. Mathematics. 2023 Feb 3;11(3):767.

[145] Rupa C, Greeshmanth, Shah MA. Novel secure data protection scheme using Martino homomorphic encryption. Journal of Cloud Computing. 2023 Mar 27;12(1):47.

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

[147] Voydock VL, Kent ST. Security mechanisms in high-level network protocols. ACM Computing Surveys (CSUR). 1983 Jun 1;15(2):135-71.

[148] Davies DW, Price WL. Security for computer networks: an introduction to data security in teleprocessing and electronic funds transfer. John Wiley & Sons, Inc.; 1984 Oct 5.

[149] 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.

[150] Clark DD. The design philosophy of the DARPA internet protocols. ACM SIGCOMM Computer Communication Review. 1995 Jan 11;25(1):102-11.

[151] 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.

[152] 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.

[153] Paliwal G, Mudgal AP, Taterh S. A study on various attacks of tcp/ip and security challenges in manet layer architecture. InProceedings of Fourth International Conference on Soft Computing for Problem Solving: SocProS 2014, Volume 2 2015 (pp. 195-207). Springer India.

[154] Hussain SZ, Parween S. Analysis of TCP issues and their possible solutions in the internet of things. Int. Arab J. Inf. Technol.. 2023 Mar 1;20(2):206-14.

[155] Kühlewind M, Bühler T, Trammell B, Neuhaus S, Müntener R, Fairhurst G. A path layer for the Internet: Enabling network operations on encrypted protocols. In2017 13th International Conference on Network and Service Management (CNSM) 2017 Nov 26 (pp. 1-9). IEEE.

[156] Medileh S, Laouid A, Euler R, Bounceur A, Hammoudeh M, AlShaikh M, Eleyan A, Khashan OA. A flexible encryption technique for the internet of things environment. Ad Hoc Networks. 2020 Sep 1;106:102240.

[157] Kounavis ME, Kang X, Grewal K, Eszenyi M, Gueron S, Durham D. Encrypting the internet. ACM SIGCOMM Computer Communication Review. 2010 Aug 30;40(4):135-46.

[158] Xin M. A mixed encryption algorithm used in internet of things security transmission system. In2015 international conference on cyber-enabled distributed computing and knowledge discovery 2015 Sep 17 (pp. 62-65). IEEE.

[159] 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.

[160] Yousefi A, Jameii SM. Improving the security of internet of things using encryption algorithms. In2017 International Conference on IoT and Application (ICIOT) 2017 May 19 (pp. 1-5). IEEE.

[161] Busta B. Encryption in theory and practice. The CPA Journal. 2002 Nov 1;72(11):42.

[162] Clark D. Encryption advances to meet Internet challenges. Computer. 2000 Aug 1;33(08):20-4.

[163] Klein MH. Trusted Computer System Evaluation Criteria. Technical report, The MITRE Corporation; 1983 Aug 15.

[164] National Computer Security Center (US). Trusted network interpretation of the trusted computer system evaluation criteria. National Computer Security Center; 1987.

[165] Bayuk J, Mostashari A. Measuring systems security. Systems Engineering. 2013 Mar;16(1):1-4.

[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] Bai J, Zhang X, Qi L, Liu W, Zhou X, Liu Y, Lv X, Sun B, Duan B, Zhang S, Che X. Survey on Application of Trusted Computing in Industrial Control Systems. Electronics. 2023 Oct 9;12(19):4182.

[168] Hill LL. The orange book. Nature Reviews. Drug Discovery. 2005 Aug 1;4(8):621.

[169] Computer Security Center (US). Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. Dod Computer Security Center; 1985.

[170] Li J, Wu J, Xu K, Chen WL. An hierarchical inter-domain authenticated source address validation solution. Chinese Journal of Computers. 2012;35(1):85-100.

[171] Moldamurat K, Seitkulov Y, Atanov S, Bakyt M, Yergaliyeva B. Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study. International Journal of Electrical & Computer Engineering (2088-8708). 2024 Feb 1;14(1).

[172] 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.

[173] Hagui I, Msolli A, ben Henda N, Helali A, Gassoumi A, Nguyen TP, Hassen F. A blockchain-based security system with light cryptography for user authentication security. Multimedia Tools and Applications. 2023 Nov 13:1-30.

[174] 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.

[175] Zukarnain ZA, Muneer A, Ab Aziz MK. Authentication securing methods for mobile identity: Issues, solutions and challenges. Symmetry. 2022 Apr 14;14(4):821.

[176] Saqib M, Moon AH. A systematic security assessment and review of Internet of things in the context of authentication. Computers & Security. 2023 Feb 1;125:103053.

[177] Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, Alrawad M. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023 Aug 27;12(17):3618.

[178] 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.

[179] Lee S, Kim G, Kim S. Sequence-order-independent network profiling for detecting application layer DDoS attacks. EURASIP Journal on Wireless Communications and Networking. 2011 Dec;2011:1-9.

[180] Dhanke J, Rastogi S, Singh K, Saxena K, Kumar K, Mishra P. An Efficient Approach for Prevention of Blackhole Attack in MANET. International Journal of Intelligent Systems and Applications in Engineering. 2024 Jan 12;12(12s):743-52.

[181] Kanaparthi VM, Vempati K. Grey hole attack in mobile ad-hoc network mitigation and protection. InAIP Conference Proceedings 2024 Jan 25 (Vol. 2802, No. 1). AIP Publishing.

[182] Kouanou AT, Fonzin TF, Zanga FM, Mouelas AN, Ndenoka GN, Ekonde MS. Machine Learning for Intrusion Detection in Ad-hoc Networks: Wormhole and Blackhole Attacks Case. Cloud Computing and Data Science. 2024:62-79.

[183] 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.

[184] Yang Q, Wang C, Yuan H, Cui J, Teng H, Chen X, Jiang C. Approaching the Information-Theoretic Limit of Privacy Disclosure with Utility Guarantees. IEEE Transactions on Information Forensics and Security. 2024 Jan 15.

[185] Weippl E, Schrittwieser S. Introduction to Security and Privacy. Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian Nida-Rümelin· Bashar Nuseibeh· Erich Prem·. 2024:397.

[186] Ramić ŠB, Prazina I, Pozderac D, Mulahasanović RT, Mrdović S. Selective disclosure of claims from multiple digital credentials. arXiv preprint arXiv:2402.15447. 2024 Feb 23.

[187] Zhang DG, An HZ, Zhang J, Zhang T, Dong WM, Jiang XR. Novel Privacy Awareness Task Offloading Approach Based On Privacy Entropy. IEEE Transactions on Network and Service Management. 2024 Jan 19.

[188] Farao A, Paparis G, Panda S, Panaousis E, Zarras A, Xenakis C. INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. International Journal of Information Security. 2024 Feb;23(1):347-71.

[189] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[190] Ahmadi S. Security Implications of Edge Computing in Cloud Networks. Journal of Computer and Communications. 2024;12(02):26-46.

[191] Abba Ari AA, Ngangmo OK, Titouna C, Thiare O, Mohamadou A, Gueroui AM. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. Applied Computing and Informatics. 2024 Jan 5;20(1/2):119-41.

[192] Abid A, Cheikhrouhou S, Kallel S, Tari Z, Jmaiel M. A smart contract-based access control framework for smart healthcare systems. The Computer Journal. 2024 Feb;67(2):407-22.

[193] Kashif M, Kalkan K. EPIoT: Enhanced privacy preservation based blockchain mechanism for internet-of-things. Computer Networks. 2024 Jan 1;238:110107.

[194] Rani S, Srivastava G. Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme. Expert Systems with Applications. 2024 Jan 1;235:121180.