GSC Advanced Research and Reviews
eISSN: 2582-4597 CODEN (USA): GARRC2
Cross Ref DOI: 10.30574/gscarr
Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

# Security schemes for the next-generation networks: A survey

Winnie Owoko *

*Jaramogi Odinga Oginga University of Science and Technology 40601, Bondo, Kenya.*

GSC Advanced Research and Reviews, 2024, 21(02), 427–455

Publication history: Received on 10 October 2024; revised on 18 November 2024; accepted on 21 November 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.2.0446

## Abstract

The rapid evolution of next-generation networks (NGNs), characterized by advancements such as 5G, 6G, edge computing, and the Internet of Things (IoT), has introduced unprecedented opportunities for connectivity and innovation. However, this progress has also expanded the attack surface, leading to new and complex security challenges. This paper provides a comprehensive review of state-of-the-art security schemes tailored for NGNs, emphasizing the interplay of confidentiality, integrity, availability, and privacy. Key areas explored include authentication mechanisms, end-to-end encryption, intrusion detection systems, and distributed ledger technologies. Furthermore, the role of artificial intelligence and machine learning in predicting and mitigating threats is analyzed. The paper also investigates emerging paradigms such as zero-trust architectures, quantum-resistant cryptographic algorithms, and secure network slicing. Through a critical assessment of existing frameworks and their limitations, this work proposes a unified approach that integrates adaptive security policies, decentralized trust models, and real-time threat intelligence. By addressing both technical and operational perspectives, this study aims to guide the development of resilient and secure NGNs, ensuring a sustainable digital future.

**Keywords:** NGNs; Security; Privacy; IoT; Architecture; Next generation networks

## 1. Introduction

Next-Generation Networks (NGNs), driven by technological advancements such as 5G, 6G, edge computing, and the Internet of Things (IoT), are reshaping the global communications landscape [1], [2]. As shown in Figure 1, these networks promise unparalleled connectivity, ultra-low latency, massive device density, and enhanced data rates, laying the foundation for transformative applications across industries [3], [4]. From autonomous vehicles and smart cities to remote healthcare and industrial automation, NGNs are poised to support a wide range of critical use cases. However, as these networks evolve, so do the security challenges they face.

The complexity and heterogeneity of NGNs introduce a vastly expanded attack surface. Unlike traditional networks, NGNs rely on highly distributed architectures, dynamic spectrum sharing, and virtualization technologies, such as Network Function Virtualization (NFV) and Software-Defined Networking (SDN). While these innovations enable flexibility and scalability, they also introduce new vulnerabilities that adversaries can exploit [5]. For instance, the integration of billions of IoT devices, many with limited computational and security capabilities [6], presents a significant challenge in ensuring secure communication and data integrity.

---

* Corresponding author: Winnie Owoko

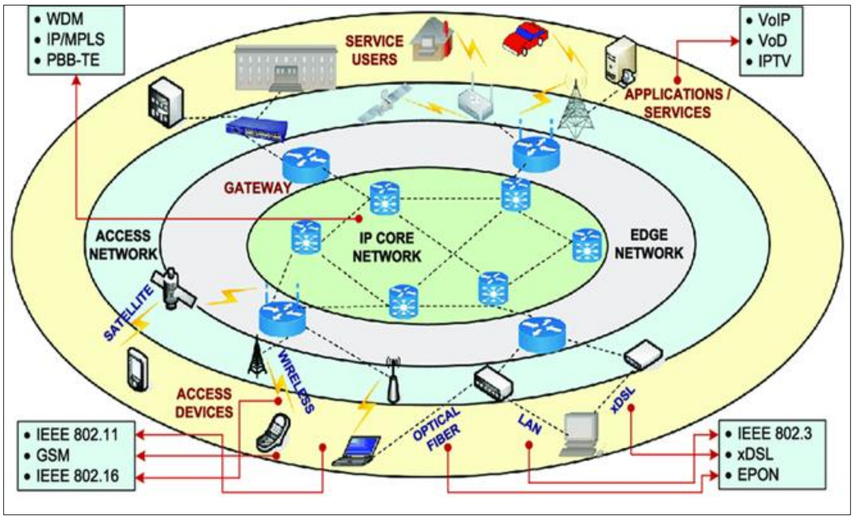

**Figure 1** Next generation network

Furthermore, the convergence of physical and digital domains in NGNs amplifies the risks associated with cyber-physical systems [7], [8]. Attackers can exploit vulnerabilities to disrupt critical infrastructure, compromise sensitive data, or even endanger human lives. These risks necessitate a paradigm shift in how security is approached. Traditional, perimeter-based security measures are insufficient in an environment where devices, users, and applications interact dynamically across diverse trust domains [9]-[11]. This paper focuses on addressing the pressing need for robust and adaptive security schemes for NGNs. Current security solutions must evolve to address the unique characteristics of NGNs, including:

- *Distributed architecture*: NGNs rely on edge computing and fog networks to process data closer to the source, reducing latency but increasing the complexity of securing multiple decentralized nodes.
- *Dynamic and multi-tenant environments*: Virtualization and network slicing enable resource sharing across multiple users and applications. Ensuring isolation and preventing data leakage in such environments is a critical challenge.
- *Emerging threats*: Sophisticated attacks such as Advanced Persistent Threats (APTs), Distributed Denial-of-Service (DDoS) attacks, and quantum computing-driven cryptographic breaches require proactive and innovative countermeasures.
- *Regulatory and privacy concerns*: As NGNs become the backbone of sensitive and critical services, compliance with global data protection regulations and safeguarding user privacy are paramount.

To address these challenges, this paper provides a comprehensive analysis of existing security frameworks and emerging technologies tailored to NGNs. It explores the role of artificial intelligence (AI) and machine learning (ML) in threat detection and response, the potential of blockchain and distributed ledger technologies for decentralized trust, and the development of quantum-resistant cryptographic algorithms to future-proof NGNs.

By evaluating the strengths and limitations of current security schemes, this study aims to propose a holistic and adaptive approach to securing NGNs. The findings and recommendations presented in this paper will serve as a valuable resource for researchers, practitioners, and policymakers, guiding the development of resilient security architectures that can meet the demands of next-generation networks.

## 2. Architecture of next-generation networks

The architecture of NGNs represents a significant departure from traditional network designs, emphasizing flexibility, scalability, and user-centric service delivery [12]. NGNs integrate advanced technologies such as virtualization, distributed computing, and intelligent resource management to meet the demands of modern applications. Their architecture is characterized by a convergence of diverse technologies, enabling seamless integration across fixed, wireless, and mobile networks. NGNs employ a layered architecture comprising access, core, and service layers, each optimized to deliver high-speed connectivity, ultra-low latency [13], and massive device support. The access layer facilitates connectivity for end-users and IoT devices through advanced wireless technologies like 5G/6G, fiber optics, and Wi-Fi 6/7 [14]-[17]. At the core layer, NGNs utilize Software-Defined Networking (SDN) and Network Function

Virtualization (NFV) to centralize control and virtualize network functions [18], ensuring efficient resource allocation and rapid service provisioning [19]. The service layer hosts applications and services, leveraging edge computing and cloud platforms to deliver personalized, low-latency experiences.

A defining feature of NGN architecture is its reliance on network programmability, virtualization, and distributed computing [20]-[22]. SDN enables centralized management of the network control plane, while NFV decouples network functions from hardware, allowing rapid deployment of services across diverse environments [23], [24]. Additionally, network slicing enables the creation of multiple virtualized networks on a shared physical infrastructure, each tailored to specific use cases, such as autonomous vehicles or smart healthcare. Figure 2 shows the various functional units of the NGNs.

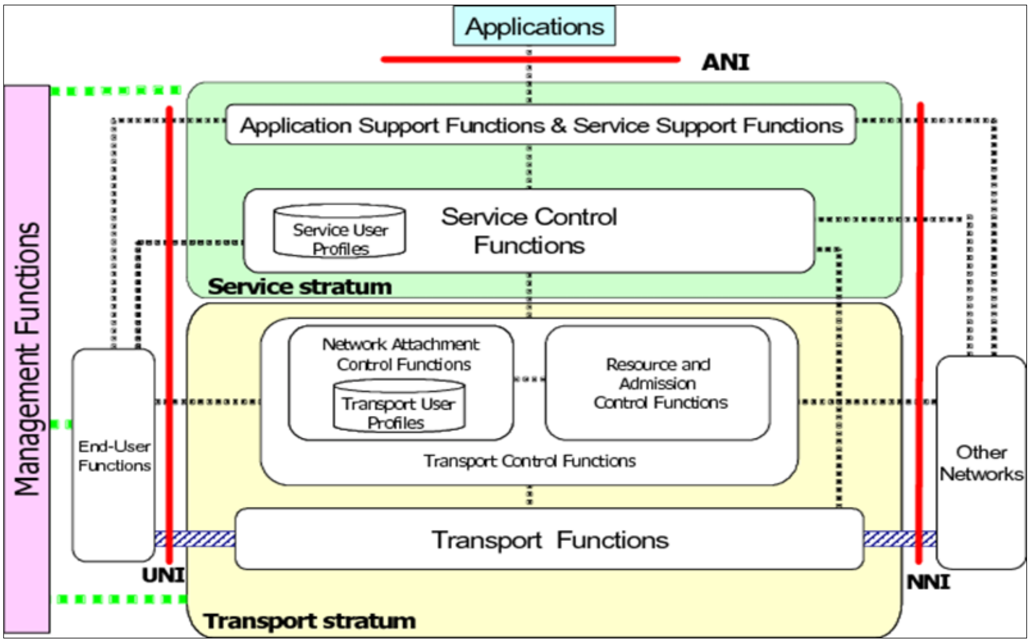

**Figure 2** Overview of next generation network

Distributed edge computing nodes extend computational power [25] closer to end-users, reducing latency and bandwidth usage while enhancing data processing capabilities. Together, these components create a highly adaptable and efficient architecture, capable of supporting future innovations and the exponential growth of connected devices [26], [27]. This architecture not only underpins the evolution of communication systems but also sets the stage for smart cities, industrial automation, and other advanced applications. Table 1 provides an overview of the key components and architectural principles that define NGNs.

**Table 1** NGNs key concepts

| Concept | Discussion |
|---|---|
| Multi-tier architecture | NGNs employ a layered and hierarchical architecture to ensure efficient resource utilization and service delivery [28]-[30]. The key tiers include:<br>Core Network Layer:<br>Acts as the backbone of the network, providing high-speed, high-capacity data transport.<br>Utilizes technologies like Network Function Virtualization (NFV) and Software-Defined Networking (SDN) for flexibility and programmability.<br>Supports advanced routing, traffic management, and interconnectivity with legacy and external networks.<br>Edge Network Layer:<br>Hosts edge computing nodes to process and store data closer to end-users, reducing latency. |

| | |
|---|---|
| | Enables localized services such as content caching, real-time analytics, and low-latency applications (e.g., augmented reality and autonomous vehicles).<br>Incorporates Multi-Access Edge Computing (MEC) to support diverse access technologies.<br>Access Network Layer:<br>Provides the interface between end-users/devices and the network.<br>Utilizes a mix of wireless (e.g., 5G/6G, Wi-Fi) and wired (e.g., optical fiber) technologies to ensure seamless connectivity.<br>Supports dynamic spectrum allocation and adaptive transmission protocols for high performance [31]. |
| Virtualized and programmable infrastructure | Network Function Virtualization (NFV):<br>Replaces dedicated hardware appliances with software-based network functions (e.g., firewalls, load balancers) hosted on generic hardware [32], [33].<br>Enables rapid deployment and scaling of network services.<br>Software-Defined Networking (SDN):<br>Decouples the control plane (decision-making) from the data plane (traffic forwarding) for centralized network management [34], [35].<br>Facilitates dynamic configuration, traffic optimization [36], and integration with third-party applications. |
| Network slicing | Allows the creation of multiple virtual networks (slices) over a shared physical infrastructure [37], [38].<br>Each slice is tailored to specific use cases with distinct requirements (e.g., ultra-low latency for autonomous vehicles, high bandwidth for video streaming).<br>Enables multi-tenancy and supports various service-level agreements (SLAs). |
| Convergence of heterogeneous technologies | NGNs integrate a wide range of access and core technologies, ensuring seamless interoperability across networks [39], [40]. Key technologies include:<br>Wireless Technologies: 5G/6G, Wi-Fi 6/7, and satellite communications.<br>IoT Integration: Supports billions of devices through low-power, wide-area networks (e.g., NB-IoT, LoRaWAN).<br>Fixed Networks: High-speed optical fiber for backhaul and fronthaul connectivity. |
| Intelligence and automation | Artificial Intelligence (AI) and Machine Learning (ML)<br>Enable intelligent resource allocation, traffic prediction, anomaly detection [42], and self-healing capabilities.<br>Autonomous Networks<br>Employ closed-loop automation for real-time monitoring and decision-making (e.g., self-optimizing networks). |
| Security and privacy mechanisms | Zero-Trust Architecture<br>Ensures that every device, user, and application is continuously authenticated and authorized before granting access [43]-[46].<br>End-to-End Encryption<br>Protects data integrity and confidentiality across the entire communication pathway [47].<br>Quantum-safe cryptography<br>Prepares for the advent of quantum computing by adopting cryptographic algorithms resistant to quantum attacks [48]. |
| Service-Oriented Architecture (SOA) | Focuses on delivering user-centric services rather than infrastructure-centric management [49].<br>Employs APIs and microservices to enable modular, scalable, and reusable service components. |

| | |
|---|---|
| | Supports diverse applications, including enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC) [50]. |
| Sustainability and energy efficiency | Integrates green technologies such as renewable energy-powered base stations and energy-efficient protocols [51], [52].<br>Optimizes resource utilization through intelligent traffic management and adaptive load balancing. |

The architecture of NGNs is built on the principles of flexibility, scalability, and intelligence to meet the diverse and dynamic requirements of modern applications [53]. By leveraging advancements in virtualization, distributed computing, AI, and secure communication, NGNs provide a robust foundation for the digital transformation of industries and society [54]-[56]. This architectural framework ensures seamless connectivity, high performance, and resilience, enabling a wide range of use cases for the future digital ecosystem.

## 3. Security issues in next generation networks

The NGNs bring transformative capabilities, including ultra-low latency, high bandwidth, and massive connectivity. However, the same features that make NGNs revolutionary also introduce significant security challenges. As these networks become integral to critical infrastructures and everyday life, addressing security concerns is paramount to ensure their reliability, privacy, and resilience [57]. Table 2 explores the key security issues in NGNs, focusing on their sources, and implications.

**Table 2** Key security issues in NGNs

| **Security issue** | **Details** |
|---|---|
| Increased attack surface | Massive device connectivity<br>NGNs, particularly through IoT, support billions of interconnected devices, many with minimal or no built-in security features [58]-[60].<br>Compromised IoT devices can serve as entry points for attacks like Distributed Denial-of-Service (DDoS) or data breaches [61], [62].<br>Heterogeneous network environment<br>The integration of various access technologies (5G/6G, Wi-Fi, satellite, etc.) creates a complex ecosystem with diverse vulnerabilities [63].<br>Securing all interfaces and ensuring seamless handovers between technologies remain significant challenges. |
| Vulnerabilities in virtualized and programmable infrastructure | Network Function Virtualization (NFV)<br>NFV decouples network functions from dedicated hardware, making them vulnerable to software-based attacks, such as malware and rootkits []64], [65].<br>Multi-tenancy in virtualized environments raises risks of side-channel attacks and resource exploitation.<br>Software-Defined Networking (SDN)<br>The centralization of the control plane in SDN creates a single point of failure [66]. An attacker compromising the SDN controller can gain control over the entire network.<br>Network Slicing<br>While network slicing allows multiple virtual networks to coexist, a breach in one slice could potentially affect others, particularly if isolation mechanisms are inadequate [67]. |
| Sophistication of cyber threats | Advanced Persistent Threats (APTs)<br>NGNs' critical role in industries and national infrastructure makes them prime targets for state-sponsored and highly sophisticated attacks [68], [69]. |

| | |
|---|---|
| | APTs are stealthy, persistent, and capable of exfiltrating sensitive information over long periods.<br>DDoS attacks<br>The higher bandwidth and interconnected nature of NGNs amplify the potential impact of DDoS attacks [70], which can disrupt critical services such as healthcare and emergency communication.<br>Zero-day exploits<br>The rapid deployment of new technologies in NGNs may introduce unknown vulnerabilities, creating opportunities for zero-day exploits [71]. |
| Privacy Concerns | Data collection and surveillance<br>NGNs process vast amounts of sensitive user data, including location, health, and financial information [72].<br>Unauthorized access to this data can lead to breaches of privacy and regulatory violations [73].<br>Data sharing across domains<br>NGNs enable cross-domain services, where data flows between multiple providers. Ensuring data protection across these domains is complex and requires robust policies [74].<br>AI-driven inference attacks<br>Malicious actors can use AI and machine learning to analyze network traffic and infer sensitive information about users or organizations [75]. |
| Emerging threats from quantum computing | Cryptographic vulnerabilities<br>Quantum computing poses a threat to traditional encryption algorithms, such as RSA and ECC, used in NGNs [76], [77].<br>Without quantum-resistant cryptography, NGNs risk exposure to future decryption of encrypted data. |
| Edge computing and distributed architecture | Edge node vulnerabilities<br>Edge computing nodes process and store data closer to users but are often less secure than centralized data centers [78].<br>Attacks on edge nodes can disrupt services or compromise sensitive data [79].<br>Inter-edge communication risks<br>As edge nodes communicate with each other and the core network, securing these interactions against tampering and eavesdropping is critical [80]. |
| Insider threats | Compromised trusted entities<br>Insider threats, whether intentional or accidental, remain a significant concern in NGNs [81], especially in multi-tenant environments where administrators manage shared infrastructure.<br>Access control failures<br>Inadequate or poorly implemented access control policies can lead to unauthorized data access and privilege escalation [82]. |
| Trust management | Lack of a unified trust framework<br>The diverse components of NGNs require interoperable trust mechanisms [83] to ensure secure interactions between devices, users, and networks.<br>Current trust frameworks are often fragmented, leading to potential vulnerabilities.<br>Fake base stations and spoofing<br>Attackers can set up fake base stations to intercept communications [84], disrupt services, or distribute malware. |
| Threats to critical infrastructure | Cyber-Physical Systems (CPS) |

| | |
|---|---|
| | NGNs underpin critical infrastructures like smart grids, transportation, and healthcare systems [85]. Attacks on these systems can have catastrophic consequences.<br>Ensuring the security of both physical and digital components is a complex challenge.<br>Service disruption<br>The reliance on NGNs for essential services makes them attractive targets for attackers [86] seeking to cause widespread disruption. |

NGNs' advanced capabilities come with complex security challenges, requiring a holistic and adaptive approach. By addressing vulnerabilities in architecture, protecting user privacy, and preparing for future threats like quantum computing, NGNs can be secured against evolving risks.

## 4. Current security solutions for next generation networks

The NGNs encompass advanced technologies such as 5G, 6G, edge computing, and the Internet of Things (IoT). As shown in Figure 3, 5G provides the foundation with ultra-high-speed data rates, low latency, and massive device connectivity, making it ideal for real-time applications like autonomous vehicles and smart healthcare [87]-[89]. Building on this, 6G envisions even faster data transmission, AI-driven network optimization, and advanced use cases such as holographic communication and brain-computer interfaces [90]. Edge computing complements these networks by processing data closer to the source, reducing latency, conserving bandwidth, and supporting time-sensitive applications. Meanwhile, the IoT connects billions of devices, from sensors and wearables to industrial machines, facilitating smart environments and pervasive connectivity [91], [92]. Together, these technologies form a cohesive ecosystem in NGNs, delivering unprecedented capabilities to meet the demands of future digital transformation.

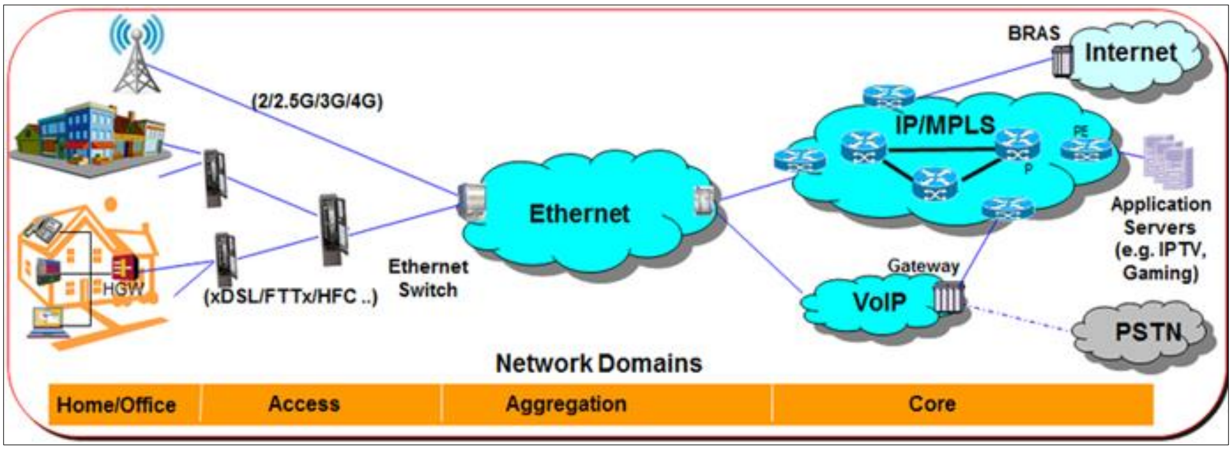

**Figure 3** Technologies in NGNs

Securing these networks requires innovative solutions tailored to address their unique characteristics and vulnerabilities. Table 3 provides an extensive discussion of the current security solutions being implemented or developed to safeguard NGNs, emphasizing their capabilities, applications, and limitations.

**Table 3** Current security solutions

| Solution | Example | Explanation |
|---|---|---|
| Authentication mechanisms | Authentication is fundamental to securing NGNs by ensuring that only authorized entities can access network resources [93]. | |
| | *Multi-Factor Authentication (MFA)* | Combines multiple forms of verification (e.g., passwords, biometrics, and device authentication) to enhance security [94], [95]. |

| | | |
|---|---|---|
| | | Addresses vulnerabilities of single-factor authentication by requiring multiple proofs of identity.<br>Used in access control for NGN devices, especially in IoT and edge environments. |
| | *Mutual authentication* | Ensures that both parties in communication verify each other's identities [96], [97].<br>Particularly useful in securing connections between edge nodes and core networks. |
| | *Public Key Infrastructure (PKI)* | Employs digital certificates to authenticate devices and users [98], [99].<br>Widely used in NGNs for secure communication, especially in IoT ecosystems. |
| Encryption technologies | Encryption ensures data confidentiality and integrity during transmission and storage in NGNs [100]. | |
| | *End-to-End Encryption (E2EE)* | Protects data from being accessed by unauthorized parties throughout its journey [101].<br>Ensures secure communication for services like voice over IP (VoIP), messaging, and video streaming. |
| | *Quantum-Resistant Cryptography* | Emerging solutions such as lattice-based, hash-based, and multivariate cryptography address threats posed by quantum computing [102], [103].<br>Designed to replace traditional encryption algorithms (e.g., RSA, ECC) vulnerable to quantum attacks. |
| | *Lightweight Cryptography* | Tailored for resource-constrained devices [104] in IoT environments.<br>Algorithms like SPECK, SIMON, and ChaCha20 provide strong encryption with low computational overhead [105], [106]. |
| Secure network slicing | Network slicing allows the creation of multiple virtual networks, each with tailored security measures [107]. | |
| | *Slice isolation* | Enforces strict separation between network slices to prevent lateral movement of attacks [108].<br>Achieved through virtualization technologies such as hypervisors and container-based solutions. |
| | *Slice-specific security policies* | Each slice is provisioned with unique security configurations [109] based on its use case (e.g., high priority for healthcare, low latency for autonomous vehicles). |
| Intrusion Detection and Prevention Systems (IDPS) | IDPS monitor NGN traffic for malicious activities [110] and take action to mitigate threats. | |
| | *AI-powered IDPS* | Leverage machine learning algorithms to identify patterns of known and unknown attacks [111].<br>Effective in detecting anomalies and advanced persistent threats (APTs) in real time. |
| | *Distributed IDPS* | Deployed at edge nodes and core networks to provide multi-layered monitoring and defense [112].<br>Ensures low-latency threat detection close to data sources. |
| Artificial Intelligence (AI) and Machine Learning (ML) | AI and ML are central to NGN security due to their ability to analyze massive data volumes and adapt to evolving threats [113]. | |

| | | |
|---|---|---|
| | *Threat prediction* | ML models trained on historical data predict potential attack vectors and vulnerabilities [114].<br>Proactively identifies weak points in network configurations and traffic flows. |
| | *Dynamic resource allocation* | AI-driven mechanisms allocate network resources [115] based on security needs, such as enhancing bandwidth for critical services under attack. |
| Blockchain and Distributed Ledger Technology (DLT) | Blockchain ensures secure and tamper-proof transaction records, enhancing trust in NGNs [116]. | |
| | *Decentralized identity management* | Blockchain enables secure authentication and identity verification without centralized authorities [117].<br>Suitable for multi-party environments like IoT ecosystems. |
| | *Secure data sharing* | Facilitates transparent and verifiable data exchanges among stakeholders while maintaining data integrity [118]. |
| Secure edge computing | | Edge computing processes data closer to the source, reducing latency but introducing new security risks [119]. |
| | *Trusted Execution Environments (TEEs)* | Hardware-based isolation for secure data processing at edge nodes.<br>Protects sensitive computations [120] and keys from unauthorized access. |
| | *Edge-specific firewalls* | Distributed security models where edge nodes collaborate to detect and mitigate threats [121]. |
| | *Decentralized security mechanisms* | Distributed security models where edge nodes collaborate to detect and mitigate threats [122]. |
| Zero-trust security model | Zero-trust architecture assumes no implicit trust within the network and verifies every access request [123]. | |
| | *Micro-segmentation* | Divides the network into smaller zones, each with its own access policies [124].<br>Limits the movement of attackers within the network. |
| | *Continuous monitoring and validation* | Real-time validation of user and device [125] behaviors ensures ongoing compliance with security policies. |
| Advanced DDoS mitigation techniques | NGNs are vulnerable to Distributed Denial-of-Service (DDoS) attacks due to their high bandwidth and interconnected nature [126]. | |
| | *AI-based traffic analysis* | AI tools differentiate between legitimate traffic and DDoS attacks based on behavioral patterns [127].<br>Enables dynamic rerouting and traffic shaping to mitigate attacks. |
| | *Cloud-based DDoS protection* | Offloads traffic to cloud-based solutions [128] for scrubbing before forwarding legitimate traffic to the NGN. |
| Privacy-preserving technologies | With increasing data privacy concerns, solutions focus on protecting user data without compromising functionality [129], [130]. | |
| | *Differential privacy* | Adds noise to data analytics outputs to prevent reverse engineering of sensitive information [131].<br>Used in NGNs for statistical analysis without compromising user privacy. |

| | | |
|---|---|---|
| | *Homomorphic encryption* | Allows computations on encrypted data without decrypting it [132].<br>Ensures data confidentiality during processing in NGNs. |
| | *Data minimization techniques* | Restrict data collection to the bare minimum required for functionality, reducing exposure risks [133], [134]. |
| Resilient infrastructure | NGNs employ redundancy and self-healing mechanisms to ensure availability even under attack [135], [136]. | |
| | *Redundant architectures* | Multiple backup systems and alternate communication paths enhance network resilience [137]. |
| | *Self-healing networks* | AI-driven networks detect faults and automatically reroute traffic or deploy patches [138]. |

As shown in Figure 4, current security solutions for NGNs leverage cutting-edge technologies such as AI, blockchain, and zero-trust models to address unique vulnerabilities. AI enhances NGNs by enabling real-time threat detection, predictive maintenance, and intelligent resource management [139], [140]. Machine learning algorithms analyze vast amounts of network data to identify anomalies and mitigate threats like Distributed Denial-of-Service (DDoS) attacks, while deep learning models [141] optimize traffic routing and load balancing. AI also facilitates the automation of network operations, allowing NGNs to adapt dynamically to changing conditions and demands. For instance, AI-driven intrusion detection systems not only recognize known attack patterns [142] but also anticipate emerging threats, making NGNs resilient against sophisticated cyberattacks.

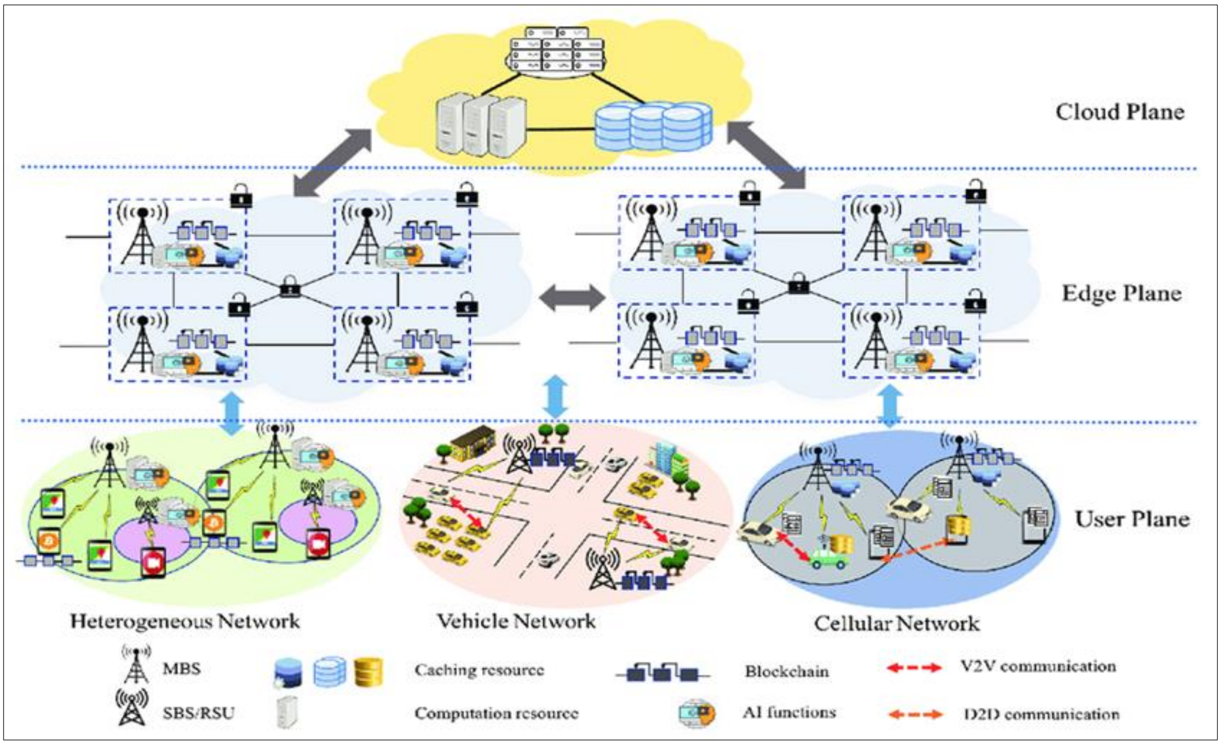

**Figure 4** Solutions to NGNs security issues

Blockchain introduces a decentralized and tamper-proof framework for securing NGNs. Its distributed ledger technology ensures data integrity and enhances trust among stakeholders, making it particularly valuable in multi-tenant environments like IoT ecosystems [143]-[146]. Blockchain can securely manage identities, enforce access controls, and facilitate transparent data sharing across devices and networks. For example, smart contracts can automate and enforce security policies in network slicing, ensuring compliance without human intervention. Complementing these technologies, the zero-trust security model addresses the fundamental vulnerabilities of traditional perimeter-based defenses [147], [148]. By assuming no implicit trust within the network, zero-trust enforces strict identity verification and continuous monitoring of all entities, regardless of their location. Micro-segmentation and dynamic access controls prevent lateral movement of attackers [149], safeguarding NGNs against insider threats and breaches. Together, AI, blockchain, and zero-trust models establish a robust and adaptive security foundation for NGNs, ensuring reliability and trustworthiness in increasingly complex and interconnected environments. While these solutions provide robust defenses against a wide range of threats, continuous innovation and adaptation are required to meet the evolving challenges of NGNs.

## 5. Research gaps and future research direction is next generation networks security

While significant progress has been made in securing NGNs, several research gaps persist due to the complexity and evolving nature of these networks. Addressing these gaps is critical for enhancing security, ensuring resilience, and enabling the full potential of NGNs. Table 4 and Table 5 present some key research gaps and proposed future research directions in NGN security, respectively.

**Table 4** Research gaps

| Gap | Description |
|---|---|
| Lack of comprehensive security frameworks | Existing security solutions often focus on specific aspects of NGNs (e.g., IoT, SDN) but fail to address security holistically across the entire ecosystem [150].<br>The absence of a unified, end-to-end security framework [151] that integrates access, edge, core, and application layers is a significant gap. |
| Insufficient real-time threat detection | While AI and ML-based systems have shown promise in detecting threats [152], their effectiveness in real-time, dynamic NGN environments is limited by:<br>Scalability challenges with large datasets.<br>The inability to quickly adapt to new, sophisticated attack vectors.<br>Current intrusion detection systems struggle to provide actionable insights during zero-day attacks [153]-[156]. |
| Inadequate quantum-resistant cryptographic solutions | Although research in quantum-resistant cryptography is progressing [157], practical implementations of these algorithms in NGNs remain scarce.<br>Existing cryptographic methods may not meet the performance requirements of NGNs, particularly in latency-sensitive applications [158] like autonomous vehicles. |
| Privacy challenges in cross-domain data sharing | NGNs require seamless data sharing across domains (e.g., healthcare, transportation), but ensuring privacy during such exchanges is complex [159].<br>Current privacy-preserving techniques, such as differential privacy and homomorphic encryption, are computationally intensive and may not scale efficiently [160], [161]. |
| Vulnerabilities in edge computing | Edge computing nodes are more susceptible to physical and cyber threats due to their distributed and resource-constrained nature [162]-[166].<br>Research on lightweight yet robust security solutions for edge devices is still in its infancy. |
| Network slicing security | Network slicing introduces vulnerabilities related to slice isolation, tenant data leakage, and misconfigured policies [167], [168].<br>Comprehensive solutions for securing multi-tenant environments and enforcing slice-specific policies are lacking. |
| Lack of trust models for heterogeneous environments | NGNs integrate diverse technologies and devices, making it challenging to establish and maintain trust across the ecosystem [169], [170].<br>Existing trust models do not fully address issues like dynamic device behavior and multi-vendor environments. |
| DDoS attack mitigation challenges | The scale and sophistication of Distributed Denial-of-Service (DDoS) attacks targeting NGNs surpass the capabilities of many existing defence mechanisms [171], [172]. |

| | |
|---|---|
| | There is a need for scalable and proactive solutions that can effectively mitigate such attacks without disrupting legitimate traffic. |
| Inadequate security metrics and benchmarks | The absence of standardized security metrics and benchmarks makes it difficult to evaluate and compare the effectiveness of different security solutions in NGNs [173], [174].<br>This gap hinders the development of universally accepted best practices. |

The future of Next-Generation Networks depends on robust, scalable, and adaptive security mechanisms. For instance, Artificial Intelligence (AI) and Machine Learning (ML) are transformative technologies in the evolution of Next-Generation Networks (NGNs), playing a crucial role in optimizing performance, enhancing security, and enabling automation. AI and ML empower NGNs to process massive volumes of data generated by devices, users, and applications, enabling real-time decision-making and dynamic network management [175], [176]. For example, ML algorithms can predict traffic patterns and dynamically allocate resources to ensure consistent Quality of Service (QoS) for latency-sensitive applications like autonomous vehicles and telemedicine. Additionally, AI-driven automation in Software-Defined Networking (SDN) and Network Function Virtualization (NFV) enables NGNs to adapt to changing demands without human intervention, reducing operational costs and improving efficiency [177], [178].

In the realm of security, AI and ML enhance NGNs by proactively detecting and mitigating threats. As shown in Figure 5, advanced ML models can identify anomalies in network traffic, recognize patterns of known attacks, and even detect zero-day vulnerabilities through behavioral analysis [179]-[182]. These technologies also play a pivotal role in threat prediction and prevention, using historical data to forecast potential attack vectors and vulnerabilities.

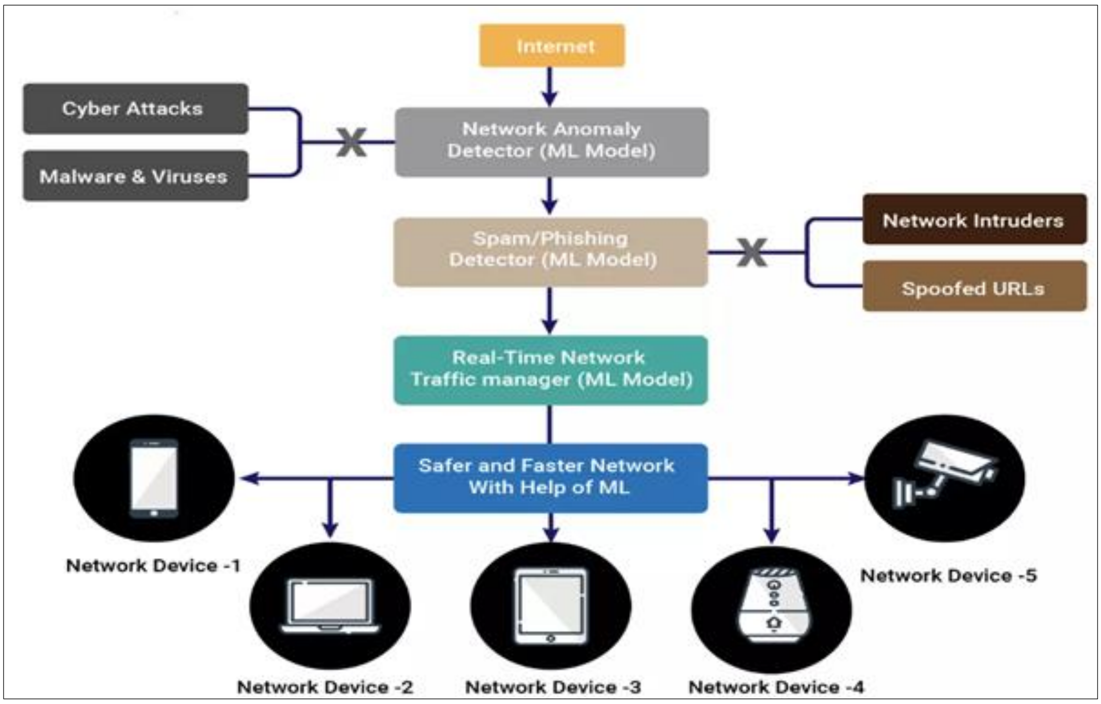

**Figure 5** AI and ML for enhanced NGNs security

Moreover, AI-powered systems support edge computing by enabling distributed intelligence, where edge nodes process data locally and make autonomous decisions, reducing latency and enhancing responsiveness [183], [184]. The integration of AI and ML into NGNs creates intelligent, resilient, and adaptive networks capable of meeting the growing demands of future applications while maintaining robust security and reliability [185]. Securing edge computing in NGNs is critical due to its decentralized nature and proximity to end-users, which increase its vulnerability to cyber threats [186]. Edge devices shown in Figure 6 often operate in resource-constrained environments and are geographically dispersed, making them prime targets for attacks like Distributed Denial-of-Service (DDoS), data breaches, and physical tampering [187]-[190]. To address these challenges, robust security measures such as Trusted Execution Environments (TEEs) are employed to provide hardware-based protection for sensitive data and computations.

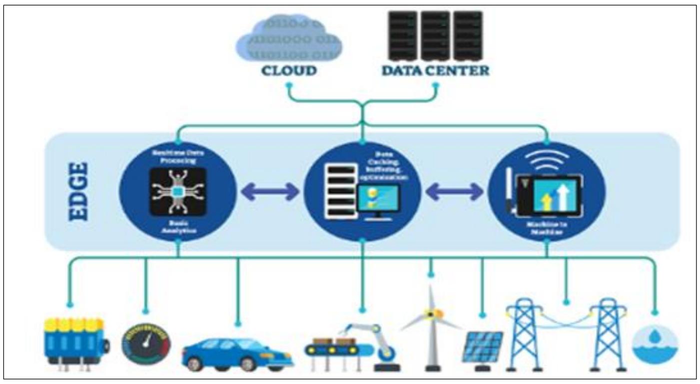

**Figure 6** Edge computing in NGNs

Lightweight encryption protocols and authentication mechanisms tailored for edge devices ensure secure communication between the edge and core network [191], [192]. Additionally, decentralized security models, such as blockchain, enhance trust by enabling tamper-proof data integrity and transparent access control [193], [194]. AI and machine learning further fortify edge computing by enabling real-time threat detection and autonomous mitigation at the edge nodes [195]. These combined strategies ensure that edge computing remains a secure and reliable enabler of NGN services, from IoT applications to real-time analytics. Figure 7 shows network slicing in next generation networks.

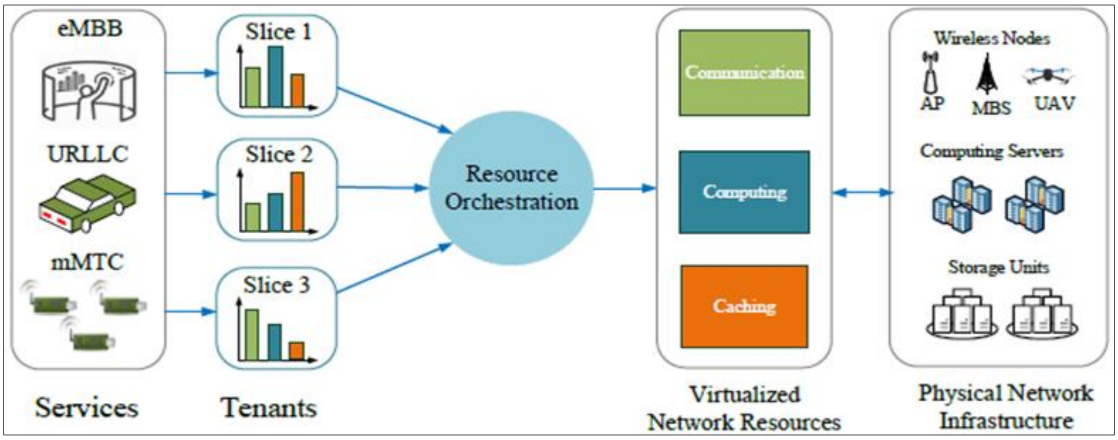

**Figure 7** Network slicing in NGNs

Enhancing network slicing security in NGNs is crucial for safeguarding the tailored virtual networks that cater to diverse use cases, such as healthcare, autonomous vehicles, and smart cities [195], [196]. Network slices, being logically isolated, face challenges like tenant data leakage [197], misconfiguration, and cross-slice attacks. To mitigate these risks, advanced slice isolation mechanisms are implemented to prevent lateral movement of threats between slices [198]. Dynamic policy enforcement ensures that security configurations for each slice are consistently maintained and adapted to its specific requirements. Additionally, blockchain technology can enhance transparency and trust by managing slice-specific identities and access controls in a decentralized manner [199]-[201]. AI and machine learning also play a vital role, enabling real-time monitoring of slices to detect anomalies [202] and automatically mitigate threats. By integrating these technologies, NGNs can maintain robust security across all network slices, ensuring the reliability and privacy of critical applications.

Trust management is a cornerstone of security in NGNs, given their complex and heterogeneous environments that integrate diverse devices, users, and technologies [203]-[205]. Figure 8 presents a typical zero trust model. With the proliferation of IoT devices, cloud services, and edge computing nodes, traditional trust models relying on static credentials or centralized authorities are no longer adequate [206].

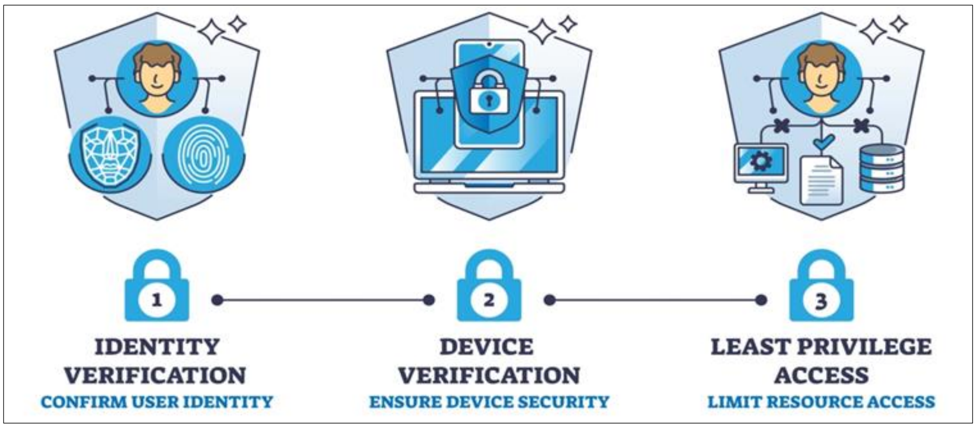

**Figure 8** Zero trust model

NGNs require dynamic and distributed trust management systems capable of evaluating trustworthiness in real-time. This involves assessing the behavior of devices, users, and network components based on multiple parameters, such as past interactions, compliance with policies, and environmental context. By leveraging AI and machine learning [207], NGNs can establish behavior-based trust scoring systems that continuously adapt to the dynamic conditions of the network, enabling rapid identification of malicious entities.

As shown in Figure 9, blockchain technology is emerging as a powerful tool for decentralized trust management in NGNs [208]. Its distributed ledger ensures tamper-proof recording of transactions, making it ideal for managing trust across diverse and untrusted entities [209]-[211]. For instance, blockchain can be used to securely validate device identities in IoT networks, ensuring only authorized devices participate in communications [212]. Additionally, smart contracts can automate trust-related functions, such as access control and policy enforcement, without relying on centralized systems.

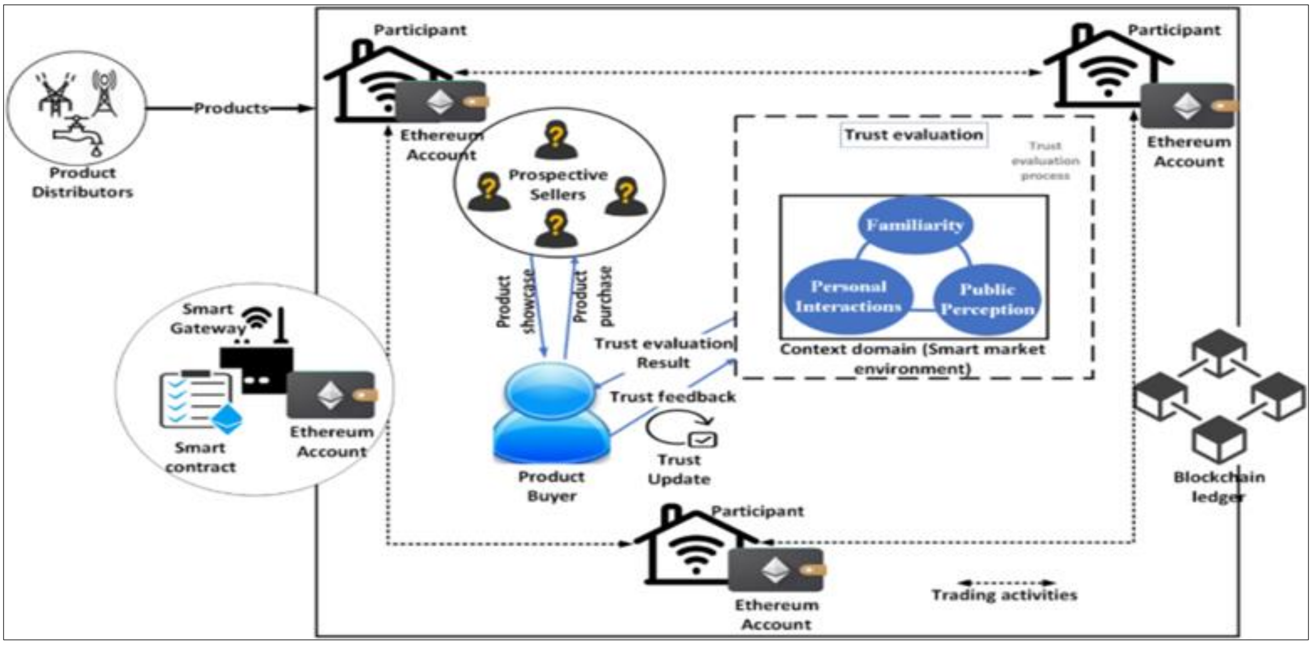

**Figure 9** Blockhain-based trust management

Combining blockchain with zero-trust security principles further strengthens NGNs by ensuring that no entity, regardless of its location or role, is inherently trusted [213], [214]. Together, these technologies enable NGNs to achieve robust and scalable trust management, fostering secure and reliable interactions in increasingly interconnected ecosystems. As illustrated in Figure 10, Distributed Denial-of-Service (DDoS) attacks are serious security challenges in NGNs. Mitigating DDoS attacks in NGNs is critical due to the increasing scale and sophistication of such threats [215],

[216]. NGNs leverage technologies like AI and machine learning [217] to detect and respond to anomalous traffic patterns in real time, enabling proactive mitigation before attacks overwhelm the network.

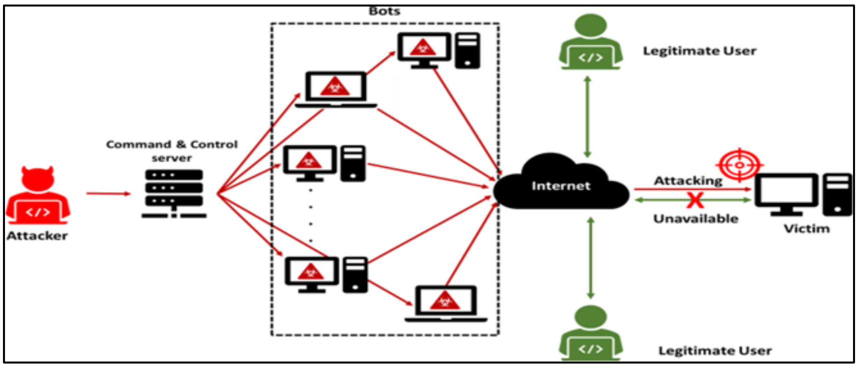

**Figure 10** Distributed Denial-of-Service in NGNs

These systems analyze traffic behavior to distinguish between legitimate and malicious flows, even in large-scale attacks [218], [219]. Network Function Virtualization (NFV) and Software-Defined Networking (SDN) enhance DDoS defense by dynamically reallocating resources, rerouting traffic, and deploying virtualized security functions where needed [220], [221].

**Table 5** Future research scopes

| **Scope** | **Explanation** |
|---|---|
| Development of holistic security architectures | Design end-to-end security frameworks [222] that integrate access, edge, core, and application layers.<br>Incorporate adaptive mechanisms to respond to emerging threats dynamically [223]. |
| Advancing AI and ML for proactive security | Develop AI and ML models capable of:<br>Detecting and mitigating zero-day threats [224] in real time.<br>Handling large-scale, heterogeneous NGN traffic without significant computational overhead.<br>Focus on explainable AI (XAI) to provide transparency [225] and trust in automated decision-making processes. |
| Quantum-resistant and post-quantum cryptography | Conduct large-scale testing and deployment of quantum-resistant cryptographic algorithms in NGN environments [226].<br>Explore hybrid cryptographic solutions [227] that combine classical and quantum-resistant algorithms during the transition to quantum-secure networks. |
| Privacy-preserving data sharing | Develop efficient privacy-preserving techniques tailored for NGN applications, such as federated learning for decentralized data analysis [228], [229].<br>Explore novel methods, such as secure multi-party computation (SMPC) [230], for cross-domain collaborations. |
| Securing edge computing | Investigate lightweight security protocols optimized for edge nodes with limited resources [231], [232].<br>Focus on self-healing mechanisms for edge nodes [233] to recover quickly from cyberattacks or failures. |
| Enhancing network slicing security | Design advanced isolation techniques to prevent lateral movement between slices [234], [235].<br>Develop automated policy enforcement mechanisms to ensure slice-specific security configurations are accurately implemented. |

| | |
|---|---|
| Trust management in heterogeneous environments | Research blockchain-based decentralized trust models [236] for managing diverse entities in NGNs.<br>Incorporate behavior-based trust scoring systems to adapt to dynamic changes in device and user behavior. |
| Advanced DDoS mitigation techniques | Explore AI-driven adaptive mitigation strategies [237] capable of distinguishing between legitimate and malicious traffic in real time.<br>Investigate distributed and collaborative DDoS defense mechanisms leveraging edge nodes [238]. |
| Sustainability in security | Develop energy-efficient security mechanisms to align with the sustainability goals of NGNs [239]-[242].<br>Explore the trade-offs between security, performance, and energy consumption in resource-constrained environments. |
| Standardization and benchmarks | Collaborate with international organizations to establish standardized security metrics and testing protocols for NGNs.<br>Promote the development of open-source tools and frameworks for benchmarking security solutions [243]-[245]. |

At the edge, edge computing nodes play a vital role by filtering malicious traffic closer to its source, reducing the load on core infrastructure. Additionally, blockchain-based decentralized defense mechanisms are emerging as a means to enhance collaboration among distributed nodes, enabling more effective identification and blocking of malicious traffic [246]. Basically, mechanisms offer robust solutions for securing next-generation networks by enabling trustless, transparent, and tamper-resistant environments. These mechanisms distribute network security responsibilities across multiple nodes, reducing single points of failure and enhancing resilience against cyberattacks [247]. Smart contracts can automate threat detection and mitigation, ensuring faster response times without requiring centralized control. Additionally, blockchain ensures the integrity of data and logs, enabling effective auditing and forensic analysis for improved cybersecurity [248]. These combined strategies ensure NGNs remain resilient against DDoS attacks, safeguarding critical applications and services.

## 6. Conclusion

Next-generation networks are poised to transform communication systems by offering unprecedented capabilities, including ultra-low latency, massive connectivity, and enhanced bandwidth. However, these advancements come with complex security challenges that threaten the confidentiality, integrity, and availability of NGN infrastructures. Addressing these challenges is critical as NGNs become the backbone of critical services across healthcare, transportation, smart cities, and industrial automation. This paper has examined the security landscape of NGNs, highlighting key issues such as increased attack surfaces, vulnerabilities in virtualized environments, privacy concerns, and emerging threats like quantum computing. Existing security solutions, including AI-driven intrusion detection systems, blockchain for decentralized trust, and advanced cryptographic techniques, were explored for their potential to mitigate these risks. Despite these advancements, significant research gaps remain, such as the need for holistic security architectures, scalable threat detection mechanisms, and quantum-resistant cryptographic implementations. Future research must focus on developing comprehensive, adaptive, and sustainable security frameworks that can scale with the dynamic and heterogeneous nature of NGNs. Emphasis should be placed on integrating privacy-preserving technologies, trust management models, and proactive defense mechanisms to ensure resilience against evolving threats. Additionally, global collaboration among academia, industry, and regulatory bodies is essential to establish standardized practices and benchmarks, fostering a secure and interoperable NGN ecosystem.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

The author declares that she holds no conflict of interest.

## References

[1] El Rajab M, Yang L, Shami A. Zero-touch networks: Towards next-generation network automation. Computer Networks. 2024 Apr 1;243:110294.

[2] Adenekan OA, Ezeigweneme C, Chukwurah EG. Driving innovation in energy and telecommunications: next-generation energy storage and 5G technology for enhanced connectivity and energy solutions. International Journal of Management & Entrepreneurship Research. 2024 May 12;6(5):1581-97.

[3] Hassan MU, Al-Awady AA, Ali A, Iqbal MM, Akram M, Jamil H. Smart Resource Allocation in Mobile Cloud Next-Generation Network (NGN) Orchestration with Context-Aware Data and Machine Learning for the Cost Optimization of Microservice Applications. Sensors. 2024 Jan 29;24(3):865.

[4] Pizzato F, Bringhenti D, Sisto R, Valenza F. Security Automation in next-generation Networks and Cloud environments. InNOMS 2024-2024 IEEE Network Operations and Management Symposium 2024 May 6 (pp. 1-4). IEEE.

[5] Rathee G, Iqbal R, Kerrache CA, Song H. TrustNextGen: Security Aspects of Trustworthy Next Generation Industrial Internet of Things (IIoT). IEEE Internet of Things Journal. 2024 Feb 26.

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

[7] Rachakonda LP, Siddula M, Sathya V. A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). High-Confidence Computing. 2024 Mar 12:100220.

[8] Nzeako G, Okeke CD, Akinsanya MO, Popoola OA, Chukwurah EG. Security paradigms for IoT in telecom networks: Conceptual challenges and solution pathways. Engineering Science & Technology Journal. 2024 May 5;5(5):1606-26.

[9] Paya A, Gómez A. Securesdp: a novel software-defined perimeter implementation for enhanced network security and scalability. International Journal of Information Security. 2024 May 20:1-6.

[10] Azad MA, Abdullah S, Arshad J, Lallie H, Ahmed YH. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things. 2024 Oct 1;27:101227.

[11] Nahar N, Andersson K, Schelén O, Saguna S. A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. IEEE Access. 2024 Jul 9.

[12] Gupta S, Verma R, Dhanda N. Introduction to Next-Generation Internet and Distributed Systems. Decentralized Systems and Distributed Computing. 2024 Jul 31:1-34.

[13] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[14] Edirisinghe S, Galagedarage O, Dias I, Ranaweera C. Recent development of emerging indoor wireless networks towards 6G. Network. 2023 May 12;3(2):269-97.

[15] Yaacoub E, Alouini MS. A key 6G challenge and opportunity—Connecting the base of the pyramid: A survey on rural connectivity. Proceedings of the IEEE. 2020 Mar 19;108(4):533-82.

[16] Alimi IA, Patel RK, Muga NJ, Pinto AN, Teixeira AL, Monteiro PP. Towards enhanced mobile broadband communications: A tutorial on enabling technologies, design considerations, and prospects of 5G and beyond fixed wireless access networks. Applied Sciences. 2021 Nov 5;11(21):10427.

[17] Jobish J, Noor-A-Rahim M, Vijayan A, Poor HV, Pesch D. Industry 4.0 and Beyond: The Role of 5G, WiFi 7, and Time-Sensitive Networking (TSN) in Enabling Smart Manufacturing. Future Internet. 2024;16(9):345.

[18] Papavassiliou S. Software defined networking (SDN) and network function virtualization (NFV). Future Internet. 2020 Jan 2;12(1):7.

[19] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[20] Chouman A, Manias DM, Shami A. A Modular, End-to-End Next-Generation Network Testbed: Towards a Fully Automated Network Management Platform. arXiv preprint arXiv:2403.15376. 2024 Mar 22.

[21] Xiao Q, Zhao J, Feng S, Li G, Hu A. Securing NextG networks with physical-layer key generation: A survey. Security and Safety. 2024;3:2023021.

[22] Nadal L, Martínez R, Ali M, Vílchez FJ, Fàbrega JM, Svaluto Moreolo M, Casellas R. Advanced optical transceiver and switching solutions for next-generation optical networks. Journal of Optical Communications and Networking. 2024 Aug 1;16(8):D64-75.

[23] Mariyappan IV, Kavitha V, Aravindaraj R, Chockalingam SC, Guerrero JM. Prospects of Network Function Virtualization (NFV) and Software-Defined Networking (SDN) Techniques for Smart Grid Cyber Defense. In5G and Fiber Optics Security Technologies for Smart Grid Cyber Defense 2024 (pp. 306-332). IGI Global.

[24] Cunha J, Ferreira P, Castro EM, Oliveira PC, Nicolau MJ, Núñez I, Sousa XR, Serôdio C. Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. Future Internet. 2024 Jun 27;16(7):226.

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

[26] Mzukwa A. Exploring Next-Generation Architectures for Advanced Computing Systems: Challenges and Opportunities. Journal of Advanced Computing Systems. 2024 Jun 6;4(6):9-18.

[27] Serôdio C, Cunha J, Candela G, Rodriguez S, Sousa XR, Branco F. The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges. Future Internet. 2023 Oct 25;15(11):348.

[28] Ali SA, Elsaid SA, Ateya AA, ElAffendi M, El-Latif AA. Enabling Technologies for Next-Generation Smart Cities: A Comprehensive Review and Research Directions. Future Internet. 2023 Dec 9;15(12):398.

[29] Chai Y, Zeng XJ, Liu Z. The future of wireless mesh network in next-generation communication: a perspective overview. Evolving Systems. 2024 Apr 23:1-4.

[30] Mohammed SA, Ralescu AL. Future Internet Architectures on an Emerging Scale—A Systematic Review. Future Internet. 2023 Apr 29;15(5):166.

[31] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[32] Alam I, Sharif K, Li F, Latif Z, Karim MM, Biswas S, Nour B, Wang Y. A survey of network virtualization techniques for Internet of Things using SDN and NFV. ACM Computing Surveys (CSUR). 2020 Apr 16;53(2):1-40.

[33] Hoffmann M, Jarschel M, Pries R, Schneider P, Jukan A, Bziuk W, Gebert S, Zinner T, Tran-Gia P. SDN and NFV as enabler for the distributed network cloud. Mobile Networks and Applications. 2018 Jun;23:521-8.

[34] Abdi AH, Audah L, Salh A, Alhartomi MA, Rasheed H, Ahmed S, Tahir A. Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. IEEE Access. 2024 Apr 25.

[35] Jisi C, Roh BH, Ali J. Reliable paths prediction with intelligent data plane monitoring enabled reinforcement learning in SD-IoT. Journal of King Saud University-Computer and Information Sciences. 2024 Mar 1;36(3):102006.

[36] 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.

[37] Rafique W, Barai J, Fapojuwo AO, Krishnamurthy D. A survey on beyond 5g network slicing for smart cities applications. IEEE Communications Surveys & Tutorials. 2024 Jun 6.

[38] Alnaim AK. Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security. International Journal of Information Security. 2024 Aug 20:1-21.

[39] Hang CN, Yu PD, Morabito R, Tan CW. Large Language Models Meet Next-Generation Networking Technologies: A Review. Future Internet. 2024 Oct 7;16(10):365.

[40] Daousis S, Peladarinos N, Cheimaras V, Papageorgas P, Piromalis DD, Munteanu RA. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. Future Internet. 2024 Jan 21;16(1):33.

[41] Goumopoulos C. Smart City Middleware: A Survey and a Conceptual Framework. IEEE Access. 2024 Jan 3.

[42] Mohammed RJ, Ghrabat MJ, Abduljabbar ZA, Nyangaresi VO, Abduljaleel IQ, Ali AH, Honi DG, Neamah HA. A Robust Hybrid Machine and Deep Learning-based Model for Classification and Identification of Chest X-ray Images. Engineering, Technology & Applied Science Research. 2024 Oct 9;14(5):16212-20.

[43] Ahmadi S. Zero trust architecture in cloud networks: application, challenges and future opportunities. Ahmadi, S.(2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports. 2024 Feb 13;26(2):215-28.

[44] Abedi K, Nguyen GT, Strufe T. Improving Resilience of Future Mobile Network Generations Implementing Zero Trust Paradigm. InNOMS 2024-2024 IEEE Network Operations and Management Symposium 2024 May 6 (pp. 1-5). IEEE.

[45] Zhu H, Xue X, Xu M, Kim BG, Lyu X, Rani S. Zero-Trust Blockchain-Enabled Secure Next-Generation Healthcare Communication Network. IEEE Transactions on Network and Service Management. 2024 Oct 3.

[46] Kroculick JB. Zero trust decision analysis for next generation networks. InDisruptive Technologies in Information Sciences VIII 2024 Jun 6 (Vol. 13058, pp. 278-286). SPIE.

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

[48] Chirra DR. Quantum-Safe Cryptography: New Frontiers in Securing Post-Quantum Communication Networks. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 2024 Oct 13;15(1):670-88.

[49] Mishra AK. Quantification of Maintainability in Service-Oriented Architecture. In2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2024 Mar 14 (pp. 1-6). IEEE.

[50] Adhikari B, Jaseemuddin M, Anpalagan A. Resource Allocation for Co-existence of eMBB and URLLC Services in 6G Wireless Networks: A Survey. IEEE Access. 2023 Dec 14.

[51] Kumar R, Gupta SK, Wang HC, Kumari CS, Korlam SS. From Efficiency to sustainability: Exploring the potential of 6G for a greener future. Sustainability. 2023 Nov 28;15(23):16387.

[52] 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.

[53] Singh M, Bhardwaj P, Bhardwaj R, Narayan S. Advancing Scalability and Efficiency in Distributed Network Computing Through Innovative Resource Allocation and Load Balancing Strategies. InInternational Conference on Intelligent and Fuzzy Systems 2024 Jul 16 (pp. 722-740). Cham: Springer Nature Switzerland.

[54] Ngo DT, Aouedi O, Piamrat K, Hassan T, Raipin-Parvédy P. Empowering digital twin for future networks with graph neural networks: Overview, enabling technologies, challenges, and opportunities. Future internet. 2023 Nov 24;15(12):377.

[55] Toy M, editor. Future Networks, Services and Management: Underlay and Overlay, Edge, Applications, Slicing, Cloud, Space, AI/ML, and Quantum Computing. Springer Nature; 2021 Nov 24.

[56] Ahmad R, Hämäläinen M, Wazirali R, Abu-Ain T. Digital-care in next generation networks: Requirements and future directions. Computer Networks. 2023 Apr 1;224:109599.

[57] 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.

[58] Ahmed SF, Alam MS, Afrin S, Rafa SJ, Taher SB, Kabir M, Muyeen SM, Gandomi AH. Towards a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities. IEEE Access. 2024 Jan 10.

[59] El-Afifi MI, Sedhom BE, Padmanaban S, Eladl AA. A review of IoT-enabled smart energy hub systems: Rising, applications, challenges, and future prospects. Renewable Energy Focus. 2024 Sep 12:100634.

[60] Taherdoost H. Security and internet of things: benefits, challenges, and future perspectives. Electronics. 2023 Apr 18;12(8):1901.

[61] Adekunle TS, Alabi OO, Lawrence MO, Adeleke TA, Afolabi OS, Ebong GN, Egbedokun GO, Bamisaye TA. An intrusion system for internet of things security breaches using machine learning techniques. InArtificial Intelligence and Applications 2024 Mar 6 (Vol. 2, No. 3, pp. 188-194).

[62] 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.

[63] Dik G, Bogdanov A, Shchegoleva N, Dik A, Kiyamov J. Challenges of IoT identification and multi-level protection in integrated data transmission networks based on 5G/6G technologies. Computers. 2022 Dec 7;11(12):178.

[64] Pattaranantakul M, He R, Song Q, Zhang Z, Meddahi A. NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures. IEEE Communications Surveys & Tutorials. 2018 Jul 25;20(4):3330-68.

[65] Muñoz A. Cracking the Core: Hardware Vulnerabilities in Android Devices Unveiled. Electronics. 2024 Oct 31;13(21):4269.

[66] Yalda K, Hamad DJ, Tapus N. Comparative Analysis of Centralized and Distributed SDN Environments for IoT Networks. Journal of Control Engineering and Applied Informatics. 2024 Sep 24;26(3):84-91.

[67] Singh VP, Singh MP, Hegde S, Gupta M. Security in 5G Network Slices: Concerns and Opportunities. IEEE Access. 2024 Apr 9.

[68] 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.

[69] Daniel SA, Victor SS. Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review. Computer Science & IT Research Journal. 2024 Mar 10;5(3):576-93.

[70] Xu R, Nagothu D, Chen Y, Aved A, Ardiles-Cruz E, Blasch E. A Secure Interconnected Autonomous System Architecture for Multi-Domain IoT Ecosystems. IEEE Communications Magazine. 2024 Jul 2;62(7):52-7.

[71] Zengeni IP, fadli Zolkipli M. Zero-Day Exploits and Vulnerability Management. Borneo International Journal eISSN 2636-9826. 2024 Sep 1;7(3):26-33.

[72] Aboukadri S, Ouaddah A, Mezrioui A. Machine learning in identity and access management systems: Survey and deep dive. Computers & Security. 2024 Jan 23:103729.

[73] 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.

[74] Chiasserini CF, Bizzarri S, Costa C, Davoli G, Llorca J, Lucrezia VL, Malandrino F, Miano S, Molinaro A, Palazzo S, Risso F. Morphable Networks for Cross-Layer and Cross-Domain Programmability: A Novel Network Paradigm. IEEE Vehicular Technology Magazine. 2024 Aug 9.

[75] Blauth TF, Gstrein OJ, Zwitter A. Artificial intelligence crime: An overview of malicious use and abuse of AI. Ieee Access. 2022 Jul 18;10:77110-22.

[76] Azhari R, Salsabila AN. Analyzing the Impact of Quantum Computing on Current Encryption Techniques. IAIC Transactions on Sustainable Digital Innovation (ITSDI). 2024 Feb 22;5(2):148-57.

[77] Fatima E, Akhtar AN, Arslan M. Evaluating Quantum Cybersecurity: A Comparative Study of Advanced Encryption Methods. Journal of Computing & Biomedical Informatics. 2024 Sep 1;7(02).

[78] Rupanetti D, Kaabouch N. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. Applied Sciences. 2024 Aug 13;14(16):7104.

[79] 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.

[80] Li P, Xia J, Wang Q, Zhang Y, Wu M. Secure architecture for Industrial Edge of Things (IEoT): A hierarchical perspective. Computer Networks. 2024 Jul 14:110641.

[81] Jaiswal A, Dwivedi P, Dewang RK. Machine learning approaches to detect, prevent and mitigate malicious insider threats: State-of-the-art review. Multimedia Tools and Applications. 2024 Oct 4:1-41.

[82] Jimmy FN. Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Apr 12;2(1):129-71.

[83] Fernandez-Gago C, Ferraris D, Roman R, Lopez J. Trust interoperability in the Internet of Things. Internet of Things. 2024 Jul 1;26:101226.

[84] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[85] Shafik W. Shaping the Next Generation Smart City Ecosystem: An Investigation on the Requirements, Applications, Architecture, Security and Privacy, and Open Research Questions. InSmart Cities: Innovations, Challenges and Future Perspectives 2024 Jun 5 (pp. 3-52). Cham: Springer Nature Switzerland.

[86] Abdelkader S, Amissah J, Kinga S, Mugerwa G, Emmanuel E, Mansour DE, Bajaj M, Blazek V, Prokop L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering. 2024 Jul 30:102647.

[87] Nuriev M, Kalyashina A, Smirnov Y, Gumerova G, Gadzhieva G. The 5G revolution transforming connectivity and powering innovations. InE3S Web of Conferences 2024 (Vol. 515, p. 04008). EDP Sciences.

[88] Fowdur TP, Babooram L, Indoonundon M, Murdan AP, Bojkovic ZS, Milovanovic DA. Enabling technologies and applications of 5G/6G-Powered Intelligent Connectivity. InDriving 5G Mobile Communications with Artificial Intelligence towards 6G 2023 Apr 6 (pp. 355-402). CRC Press.

[89] 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.

[90] Zawish M, Dharejo FA, Khowaja SA, Raza S, Davy S, Dev K, Bellavista P. AI and 6G into the metaverse: Fundamentals, challenges and future research trends. IEEE Open Journal of the Communications Society. 2024 Jan 29;5:730-78.

[91] Chataut R, Phoummalayvane A, Akl R. Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. Sensors. 2023 Aug 16;23(16):7194.

[92] Bhatt K, Agrawal C, Bisen AM. A Review on Emerging Applications of IoT and Sensor Technology for Industry 4.0. Wireless Personal Communications. 2024 Apr 22:1-9.

[93] Paskauskas RA. Countering Hybrid Threats: Towards an Ontology for Securing 5G Networks. InInternational Conference on Computer and Communication Engineering 2024 May 24 (pp. 104-121). Cham: Springer Nature Switzerland.

[94] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[95] Mahmood RK, Mahameed AI, Lateef NQ, Jasim HM, Radhi AD, Ahmed SR, Tupe-Waghmare P. Optimizing Network Security with Machine Learning and Multi-Factor Authentication for Enhanced Intrusion Detection. Journal of Robotics and Control (JRC). 2024 Aug 8;5(5):1502-24.

[96] Hasan MK, Weichen Z, Safie N, Ahmed FR, Ghazal TM. A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. IEEE Access. 2024 Apr 25.

[97] Soni M, Singh DK. Blockchain-based group authentication scheme for 6G communication network. Physical Communication. 2023 Apr 1;57:102005.

[98] El-Hajj M, Beune P. Lightweight public key infrastructure for the Internet of Things: A systematic literature review. Journal of Industrial Information Integration. 2024 Aug 10:100670.

[99] 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.

[100] Rahiman MA. Next-gen security for medical data: optical encryption empowered by generative adversarial networks. Multimedia Tools and Applications. 2024 Aug 5:1-24.

[101] Hazra R, Chatterjee P, Singh Y, Podder G, Das T. Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 546-570). IGI Global.

[102] Asif R. Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. IoT. 2021 Mar;2(1):71-91.

[103] Mamatha GS, Dimri N, Sinha R. Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. arXiv preprint arXiv:2403.11741. 2024 Mar 18.

[104] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).DOI: 10.18421/TEM133-61

[105] Gupta A, Bozorgzadeh E. Optimizing Lightweight Cryptographic Algorithms for Enhanced Performance and Security in IoT Medical Devices. Authorea Preprints. 2024 Oct 7.

[106] Gadalla ER, Sallabi OM, Kasih TM, Emhemed AA. Evaluation of the Recommended Algorithms in the Internet of Things. InArtificial Intelligence of Things for Smart Green Energy Management 2022 Jun 24 (pp. 141-161). Cham: Springer International Publishing.

[107] De Alwis C, Porambage P, Dev K, Gadekallu TR, Liyanage M. A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. IEEE Communications Surveys & Tutorials. 2023 Sep 6.

[108] Esmaeily A, Kralevska K. Orchestrating Isolated Network Slices in 5G Networks. Electronics. 2024 Apr 18;13(8):1548.

[109] Wichary T, Mongay Batalla J, Mavromoustakis CX, Żurek J, Mastorakis G. Network slicing security controls and assurance for verticals. Electronics. 2022 Jan 11;11(2):222.

[110] 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.

[111] Yellepeddi SM, Ravi CS, Vangoor VK, Chitta S. AI-Powered Intrusion Detection Systems: Real-World Performance Analysis. Journal of AI-Assisted Scientific Discovery. 2024 Jan 11;4(1):279-89.

[112] An L, Qiu J, Zhang H, Liu C. Design of distributed network intrusion prevention system based on Spark and P2DR models. Cluster Computing. 2024 May 11:1-20.

[113] Sindiramutty SR, Prabagaran KR, Jhanjhi NZ, Murugesan RK, Brohi SN, Masud M. Generative AI in Network Security and Intrusion Detection. InReshaping CyberSecurity With Generative AI Techniques 2025 (pp. 77-124). IGI Global.

[114] Bilgin Z, Ersoy MA, Soykan EU, Tomur E, Çomak P, Karaçay L. Vulnerability prediction from source code using machine learning. IEEE Access. 2020 Aug 14;8:150672-84.

[115] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[116] Yang J, Wen J, Jiang B, Wang H. Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network. 2020 Jul 22;34(4):62-7.

[117] Rodionov A. The Potential of Blockchain Technology for Creating Decentralized Identity Systems: Technical Capabilities and Legal Regulation. International Journal of Law and Policy. 2024 Apr 30;2(4):19-30.

[118] Udeh EO, Amajuoyi P, Adeusi KB, Scott AO. Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology. Finance & Accounting Research Journal. 2024 Jun 6;6(6):851-67.

[119] Rancea A, Anghel I, Cioara T. Edge Computing in Healthcare: Innovations, Opportunities, and Challenges. Future Internet. 2024 Sep 10;16(9):329.

[120] 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.

[121] 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.

[122] Meng W, Katsikas SK, Chen J, Chen C. Security, Privacy, and Trust Management on Decentralized Systems and Networks. International Journal of Network Management. 2024:e2311.

[123] Annabi M, Zeroual A, Messai N. Towards zero trust security in connected vehicles: A comprehensive survey. Computers & Security. 2024 Jul 26:104018.

[124] A Al-Ofeishat H, Alshorman R. Build a Secure Network using Segmentation and Micro-segmentation Techniques. International Journal of Computing and Digital Systems. 2023 Sep 20;16(1):1499-508.

[125] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[126] Hasan MK, Habib AA, Islam S, Safie N, Abdullah SN, Pandey B. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Reports. 2023 Oct 1;9:1318-26.

[127] Kalutharage CS, Liu X, Chrysoulas C, Pitropakis N, Papadopoulos P. Explainable AI-based DDOS attack identification method for IoT networks. Computers. 2023 Feb 3;12(2):32.

[128] Ouhssini M, Afdel K, Akouhar M, Agherrabi E, Abarda A. Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches. Egyptian Informatics Journal. 2024 Sep 1;27:100517.

[129] Sargiotis D. Data Security and Privacy: Protecting Sensitive Information. InData Governance: A Guide 2024 Sep 12 (pp. 217-245). Cham: Springer Nature Switzerland.

[130] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[131] Zhao W, Sang Y, Xiong N, Tian H. Privacy-Preserving Deep Reinforcement Learning based on Differential Privacy. In2024 International Joint Conference on Neural Networks (IJCNN) 2024 Jun 30 (pp. 1-8). IEEE.

[132] Su G, Wang J, Xu X, Wang Y, Wang C. The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology. 2024 Mar 13;2(1):52-8.

[133] Staab R, Jovanović N, Balunović M, Vechev M. From principle to practice: Vertical data minimization for machine learning. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 4733-4752). IEEE.

[134] Yusupova G, Ismailov A. Advancing Robust and Ethical Data Minimization Techniques: Theoretical Foundations and Practical Implementations. Journal of Intelligent Connectivity and Emerging Technologies. 2023 Apr 7;8(2):35-47.

[135] Johnphill O, Sadiq AS, Al-Obeidat F, Al-Khateeb H, Taheir MA, Kaiwartya O, Ali M. Self-Healing in Cyber–Physical systems using machine learning: A critical analysis of theories and tools. Future Internet. 2023 Jul 17;15(7):244.

[136] 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.

[137] Rafy MF, Srivastava AK, Neto F, Biasi J. Communication Technologies for DER-centric Power Distribution Systems: A Comparative Analysis and Cyber-Resilience Guidelines. IEEE Access. 2024 Jun 3.

[138] Fang H, Yu P, Tan C, Zhang J, Lin D, Zhang L, Zhang Y, Li W, Meng L. Self-Healing in Knowledge-Driven Autonomous Networks: Context, Challenges, and Future Directions. IEEE Network. 2024 Jun 19.

[139] Ameedeen MA, Hamid RA, Aldhyani TH, Al-Nassr LA, Olatunji SO, Subramanian P. A Framework for Automated Big Data Analytics in Cybersecurity Threat Detection. Mesopotamian Journal of Big Data. 2024 Sep 25;2024:175-84.

[140] Tooki OO, Popoola OM. A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems. Renewable Energy Focus. 2024 Sep 2:100628.

[141] Ahmad AY, Alzubi J, James S, Nyangaresi VO, Kutralakani C, Krishnan A. Enhancing Human Action Recognition with Adaptive Hybrid Deep Attentive Networks and Archerfish Optimization. Computers, Materials & Continua. 2024 Sep 1;80(3).

[142] Andronikidis G, Eleftheriadis C, Batzos Z, Kyranou K, Maropoulos N, Sargsyan G, Grammatikis PR, Sarigiannidis P. AI-Driven Anomaly and Intrusion Detection in Energy Systems: Current Trends and Future Direction. In2024 IEEE International Conference on Cyber Security and Resilience (CSR) 2024 Sep 2 (pp. 777-782). IEEE.

[143] Chen Y, Jian P, Zhang Y, Li J, Wu Z, Liu Z. A systematic solution of distributed and trusted chain-network integration. Journal of Industrial Information Integration. 2024 Sep 1;41:100664.

[144] Alzhrani F, Saeedi K, Zhao L. Architectural Patterns for Blockchain Systems and Application Design. Applied Sciences. 2023 Oct 21;13(20):11533.

[145] Shinde NK, Seth A, Kadam P. Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications. Machine Learning and Optimization for Engineering Design. 2023 Dec 27:85-119.

[146] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering & Systems. 2024 Nov 1;17(6).

[147] Patel R, Müller K, Kvirkvelia G, Smith J, Wilson E. Zero Trust Security Architecture Raises the Future Paradigm in Information Systems. Informatica and Digital Insight Journal. 2024 Jan 31;1(1):24-34.

[148] Ahn G, Jang J, Choi S, Shin D. Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. IEEE Access. 2024 Jun 21.

[149] Daniel C. Building a More Secure Network: A Comprehensive Guide to Network Segmentation Strategies and Best Practices. Revista de Inteligencia Artificial en Medicina. 2024 Sep 9;15(1):959-68.

[150] Ray PP, Kumar N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. Computer Communications. 2021 Mar 1;169:129-53.

[151] 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.

[152] Anandharaj N. AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. Journal of recent trends in computer science and engineering (JRTCSE). 2024 Jul 25;12(2):21-30.

[153] Neupane S, Ables J, Anderson W, Mittal S, Rahimi S, Banicescu I, Seale M. Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. IEEE Access. 2022 Oct 25;10:112392-415.

[154] Isong B, Kgote O, Abu-Mahfouz A. Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. Electronics. 2024 Jun 17;13(12):2370.

[155] Verma J, Bhandari A, Singh G. iNIDS: SWOT Analysis and TOWS Inferences of State-of-the-Art NIDS solutions for the development of Intelligent Network Intrusion Detection System. Computer Communications. 2022 Nov 1;195:227-47.

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

[157] Widodo AM, Pappachan P, Sekti BA, Anwar N, Widayanti R, Rahaman M, Bansal R. Quantum-Resistant Cryptography. InInnovations in Modern Cryptography 2024 (pp. 100-130). IGI Global.

[158] Theodoropoulos T, Violos J, Makris A, Tserpes K. A New Approach for Evaluating the Performance of Distributed Latency-Sensitive Services. In2024 IEEE International Conference on Communications Workshops (ICC Workshops) 2024 Jun 9 (pp. 365-370). IEEE.

[159] Alsamhi SH, Hawbani A, Kumar S, Timilsina M, Al-Qatf M, Haque R, Nashwan F, Zhao L, Curry E. Empowering Dataspace 4.0: Unveiling Promise of Decentralized Data-Sharing. IEEE Access. 2024 Aug 13.

[160] Pulido-Gaytan B, Tchernykh A, Cortés-Mendoza JM, Babenko M, Radchenko G, Avetisyan A, Drozdov AY. Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. Peer-to-Peer Networking and Applications. 2021 May;14(3):1666-91.

[161] 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.

[162] Arroba P, Buyya R, Cárdenas R, Risco-Martín JL, Moya JM. Sustainable edge computing: Challenges and future directions. Software: Practice and Experience. 2024.

[163] AlAqqad W, Nijim M, Onyeakazi U, Albataineh H. Cyber Edge: Mitigating Cyber-Attacks in Edge Computing Using Intrusion Detection System. InInternational Conference on Advances in Computing Research 2024 Mar 29 (pp. 292-305). Cham: Springer Nature Switzerland.

[164] Baidya T, Moh S. Comprehensive survey on resource allocation for edge-computing-enabled metaverse. Computer Science Review. 2024 Nov 1;54:100680.

[165] Sharma M, Tomar A, Hazra A. Edge computing for industry 5.0: fundamental, applications and research challenges. IEEE Internet of Things Journal. 2024 Mar 7.

[166] 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).

[167] Abood MJ, Abdul-Majeed GH. Classification of network slicing threats based on slicing enablers: A survey. International Journal of Intelligent Networks. 2023 Jan 1;4:103-12.

[168] Gao S, Lin R, Fu Y, Li H, Cao J. Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey. Electronics. 2024 May 10;13(10):1860.

[169] Hakkarainen T, Colicev A, Pedersen T. A perspective on three trade-offs of blockchain technology for the global strategy of the MNC. Global Strategy Journal. 2024 Jun 9.

[170] Wang X, Wang B, Wu Y, Ning Z, Guo S, Yu FR. A Survey on Trustworthy Edge Intelligence: From Security and Reliability to Transparency and Sustainability. IEEE Communications Surveys & Tutorials. 2024 Aug 20.

[171] 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.

[172] Manan J, Ahmed A, Ullah I, Merghem-Boulahia L, Gaïti D. Distributed intrusion detection scheme for next generation networks. Journal of Network and Computer Applications. 2019 Dec 1;147:102422.

[173] Magán-Carrión R, Urda D, Díaz-Cano I, Dorronsoro B. Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches. Applied Sciences. 2020 Mar 4;10(5):1775.

[174] Shahin M, Maghanaki M, Hosseinzadeh A, Chen FF. Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. Advanced Engineering Informatics. 2024 Oct 1;62:102685.

[175] Gupta U, Pantola D, Bhardwaj A, Singh SP. Next-generation networks enabled technologies: Challenges and applications. Next generation communication networks for industrial internet of things systems. 2022 Dec 16:191-216.

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

[177] Polónio J, Moura J, Marinheiro RN. On the Road to Proactive Vulnerability Analysis and Mitigation Leveraged by Software Defined Networks: A Systematic Review. IEEE Access. 2024 Jul 16.

[178] Abid MA, Afaqui N, Khan MA, Akhtar MW, Malik AW, Munir A, Ahmad J, Shabir B. Evolution towards smart and software-defined internet of things. AI. 2022 Feb 21;3(1):100-23.

[179] Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA. Zero-day attack detection: a systematic literature review. Artificial Intelligence Review. 2023 Oct;56(10):10733-811.

[180] Ali S, Rehman SU, Imran A, Adeem G, Iqbal Z, Kim KI. Comparative evaluation of ai-based techniques for zero-day attacks detection. Electronics. 2022 Nov 28;11(23):3934.

[181] Zoppi T, Ceccarelli A, Bondavalli A. Unsupervised algorithms to detect zero-day attacks: Strategy and application. Ieee Access. 2021 Jun 21;9:90603-15.

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

[183] Mishra AK, Ravinder Reddy R, Tyagi AK, Arowolo MO. Artificial Intelligence-Enabled Edge Computing: Necessity of Next Generation Future Computing System. InIoT Edge Intelligence 2024 Jun 4 (pp. 67-109). Cham: Springer Nature Switzerland.

[184] Raghav YY, Kait R. Edge computing empowering distributed computing at the edge. InEmerging Trends in Cloud Computing Analytics, Scalability, and Service Models 2024 (pp. 67-83). IGI Global.

[185] Al Ridhawi I, Otoum S. Supporting next-generation network management with intelligent moving devices. IEEE Network. 2022 Jul 13;36(3):8-15.

[186] Tahirkheli AI, Shiraz M, Hayat B, Idrees M, Sajid A, Ullah R, Ayub N, Kim KI. A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. Electronics. 2021 Jul 28;10(15):1811.

[187] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE.

[188] Ma Y, Liu L, Liu Z, Li F, Xie Q, Chen K, Lv C, He Y, Li F. A Survey of DDoS Attack and Defense Technologies in Multi-Access Edge Computing. IEEE Internet of Things Journal. 2024 Nov 4.

[189] Sathupadi K. Ai-based intrusion detection and ddos mitigation in fog computing: Addressing security threats in decentralized systems. Sage Science Review of Applied Machine Learning. 2023 Nov 15;6(11):44-58.

[190] Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25;22(3):927.

[191] Zerraza I. Lightweight Authentication for IOT Edge Devices. Informatica. 2024 Nov 8;48(18).

[192] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[193] Daah C, Qureshi A, Awan I, Konur S. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. Electronics. 2024 Feb 23;13(5):865.

[194] Hossain MI, Steigner T, Hussain MI, Akther A. Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. arXiv preprint arXiv:2405.04837. 2024 May 8.

[195] Banik S, Kothamali PR, Dandyala SS. Strengthening Cybersecurity in Edge Computing with Machine Learning. Revista de Inteligencia Artificial en Medicina. 2024 Mar 31;15(1):332-64.

[196] Martins JS, Carvalho TC, Moreira R, Both CB, Donatti A, Corrêa JH, Suruagy JA, Corrêa SL, Abelem AJ, Ribeiro MR, José-marcos SN. Enhancing network slicing architectures with machine learning, security, sustainability and experimental networks integration. IEEE Access. 2023 Jul 5;11:69144-63.

[197] 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.

[198] Bera B, Das AK, Sikdar B. Digital Twins-Empowered Secure Network Slice Access and Isolation for Consumer Healthcare Applications. IEEE Transactions on Services Computing. 2024 Jul 3.

[199] Javed F, Antevski K, Mangues-Bafalluy J, Giupponi L, Bernardos CJ. Distributed ledger technologies for network slicing: A survey. IEEE Access. 2022 Feb 11;10:19412-42.

[200] Onopa S, Kotulski Z. State-of-the-art and New challenges in 5G networks with Blockchain Technology. Electronics. 2024 Mar 3;13(5):974.

[201] Osorio DP, Ahmad I, Sánchez JD, Gurtov A, Scholliers J, Kutila M, Porambage P. Towards 6G-enabled internet of vehicles: Security and privacy. IEEE Open Journal of the Communications Society. 2022 Jan 14;3:82-105.

[202] Ali AH, Jasim HM, Abduljabbar ZA, Nyangaresi VO, Umran SM, Ma J, Honi DG. Provably Efficient and Fast Technique for Determining the Size of a Brain Tumor in T1 MRI Images. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 608-613). IEEE.

[203] Ziegler V, Schneider P, Viswanathan H, Montag M, Kanugovi S, Rezaki A. Security and Trust in the 6G Era. Ieee Access. 2021 Oct 14;9:142314-27.

[204] Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. Journal of Electrical Systems and Information Technology. 2024 Aug 5;11(1):30.

[205] Tripi G, Iacobelli A, Rinieri L, Prandini M. Security and Trust in the 6G Era: Risks and Mitigations. Electronics. 2024 Jun 1;13(11):2162.

[206] Alshammari ST, Al-Razgan M, Alfakih T, AlGhamdi KA. Building a Comprehensive Trust Evaluation Model to Secure Cloud Services from Reputation Attacks (February 2024). IEEE Access. 2024 Oct 1.

[207] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[208] Mlika F, Karoui W, Romdhane LB. Blockchain solutions for trustworthy decentralization in social networks. Computer Networks. 2024 Mar 16:110336.

[209] AlMarshoud M, Sabir Kiraz M, H. Al-Bayatti A. Security, privacy, and decentralized trust management in VANETs: a review of current research and future directions. ACM Computing Surveys. 2024 Jun 22;56(10):1-39.

[210] Xevgenis M, Kogias DG, Karkazis P, Leligou HC, Patrikakis C. Application of blockchain technology in dynamic resource management of next generation networks. Information. 2020 Dec 6;11(12):570.

[211] Hemamalini V, Mishra AK, Tyagi AK, Kakulapati V. Artificial intelligence–blockchain-enabled–internet of things-based cloud applications for next-generation society. Automated Secure Computing for Next-Generation Systems. 2024 May 3:65-82.

[212] 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.

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

[214] Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, Hamid Y. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors. 2024 Feb 19;24(4):1328.

[215] Valdovinos IA, Pérez-Díaz JA, Choo KK, Botero JF. Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. Journal of Network and Computer Applications. 2021 Aug 1;187:103093.

[216] Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review. 2020 Aug 1;37:100279.

[217] Mohialdin SH, Abdulrahman LQ, Al-Yoonus MH, Abduljabbar ZA, Honi DG, Nyangaresi VO, Abduljaleel IQ, Neamah HA. Utilizing Machine Learning for the Early Detection of Coronary Heart Disease. Engineering, Technology & Applied Science Research. 2024 Oct 9;14(5):17363-75.

[218] Vo HV, Du HP, Nguyen HN. Ai-powered intrusion detection in large-scale traffic networks based on flow sensing strategy and parallel deep analysis. Journal of Network and Computer Applications. 2023 Nov 1;220:103735.

[219] Arivudainambi D, KA VK, Visu P. Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance. Computer Communications. 2019 Nov 1;147:50-7.

[220] Domínguez-Dorado M, Calle-Cancho J, Galeano-Brajones J, Rodríguez-Pérez FJ, Cortés-Polo D. Detection and Mitigation of Security Threats Using Virtualized Network Functions in Software-Defined Networks. Applied Sciences. 2023 Dec 31;14(1):374.

[221] Rashidi B, Fung C, Bertino E. A collaborative DDoS defence framework using network function virtualization. IEEE Transactions on Information Forensics and Security. 2017 May 26;12(10):2483-97.

[222] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[223] Patwary M, Ramchandran P, Tibrewala S, Lala TK, Kautz F, Coronado E, Riggio R, Ganugapati S, Ranganathan S, Liu L, Giambene G. Edge Services. In2023 IEEE Future Networks World Forum (FNWF) 2023 Nov 13 (pp. 1-68). IEEE.

[224] Gowthami G, Priscila SS. Zero-Day Threat Detection A Machine Learning Paradigm for Intrusion Prevention. In2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT) 2024 Aug 8 (Vol. 1, pp. 852-857). IEEE.

[225] Ali A. Explainable AI: Examining Challenges and Opportunities in Developing Explainable AI Systems for Transparent Decision-Making. Journal of Artificial Intelligence Research. 2024 Feb 27;4(1):1-3.

[226] Thanalakshmi P, Rishikhesh A, Marion Marceline J, Joshi GP, Cho W. A quantum-resistant blockchain system: a comparative analysis. Mathematics. 2023 Sep 17;11(18):3947.

[227] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[228] Beltrán ET, Pérez MQ, Sánchez PM, Bernal SL, Bovet G, Pérez MG, Pérez GM, Celdrán AH. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. IEEE Communications Surveys & Tutorials. 2023 Sep 15.

[229] Beltrán ET, Gómez ÁL, Feng C, Sánchez PM, Bernal SL, Bovet G, Pérez MG, Pérez GM, Celdrán AH. Fedstellar: A platform for decentralized federated learning. Expert Systems with Applications. 2024 May 15;242:122861.

[230] Rahaman M, Arya V, Orozco SM, Pappachan P. Secure Multi-Party Computation (SMPC) Protocols and Privacy. InInnovations in Modern Cryptography 2024 (pp. 190-214). IGI Global.

[231] Du J, Zhang G. A Lightweight Node Verification and Protection Strategy for Edge Computing. In2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) 2024 Mar 29 (pp. 620-625). IEEE.

[232] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[233] Mata L, Sousa M, Vieira P, Queluz MP, Rodrigues A. On the Use of Spatial Graphs for Performance Degradation Root-Cause Analysis Towards Self-Healing Mobile Networks. IEEE Access. 2024 Feb 1.

[234] Kotulski Z, Nowak TW, Sepczuk M, Tunia M, Artych R, Bocianiak K, Osko T, Wary JP. Towards constructive approach to end-to-end slice isolation in 5G networks. EURASIP Journal on Information Security. 2018 Dec;2018:1-23.

[235] Mahboubi A, Luong K, Aboutorab H, Bui HT, Jarrad G, Bahutair M, Camtepe S, Pogrebna G, Ahmed E, Barry B, Gately H. Evolving techniques in cyber threat hunting: A systematic review. Journal of Network and Computer Applications. 2024 Aug 23:104004.

[236] Truong N, Lee GM, Sun K, Guitton F, Guo Y. A blockchain-based trust system for decentralised applications: When trustless needs trust. Future Generation Computer Systems. 2021 Nov 1;124:68-79.

[237] 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.

[238] Chahal JK, Bhandari A, Behal S. DDoS attacks & defense mechanisms in SDN-enabled cloud: Taxonomy, review and research challenges. Computer Science Review. 2024 Aug 1;53:100644.

[239] He P, Zhou Y, Qin X. A Survey on Energy-Aware Security Mechanisms for the Internet of Things. Future Internet. 2024 Apr 8;16(4):128.

[240] Aqeel I. Enhancing Security and Energy Efficiency in Wireless Sensor Networks for IoT Applications. Journal of Electrical Systems. 2024;20(3s):807-16.

[241] Hu L, Han C, Wang X, Zhu H, Ouyang J. Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks. Sensors. 2024 Mar 21;24(6):1993.

[242] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[243] Bassey C, Chinda ET, Idowu S. Building a Scalable Security Operations Center: A Focus on Open-source Tools. Journal of Engineering Research and Reports. 2024 Jun 21;26(7):196-209.

[244] Gentile AF, Macrì D, Carnì DL, Greco E, Lamonaca F. A Performance Analysis of Security Protocols for Distributed Measurement Systems Based on Internet of Things with Constrained Hardware and Open Source Infrastructures. Sensors. 2024 Apr 26;24(9):2781.

[245] Manzoor J, Waleed A, Jamali AF, Masood A. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. Plos one. 2024 Mar 28;19(3):e0301183.

[246] Jiang S, Yang L, Gao X, Zhou Y, Feng T, Song Y, Liu K, Cheng G. BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks. Security and communication networks. 2022;2022(1):1608689.

[247] Shah Z, Ullah I, Li H, Levula A, Khurshid K. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors. 2022 Jan 31;22(3):1094.

[248] Li W, Wang Y, Li J, Au MH. Toward a blockchain-based framework for challenge-based collaborative intrusion detection. International Journal of Information Security. 2021 Apr;20:127-39.