Smart Technologies Academic Press

**Journal of Cyber Security and Risk Auditing**

https://www.jcsra.thestap.com/


# A Systematic Literature Review of Blockchain-Enabled Zero Trust Architectures for Secure Non-Terrestrial Networks in 6G Cloud–Edge Environments

**Abdullah Albuali [1*], Huda Aldawghan [1], and Ashwag Alotaibi [1]**

[1]*Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, 31982 Saudi Arabia*

## ARTICLE INFO

**Article History**
**Received: 01-02-2026**
**Revised: 28-02-2026**
**Accepted: 10-03-2026**
**Published: 31-03-2026**

**Vol.2026, No.1**

**DOI:**

***Corresponding author. Email:*** *aabuali@kfu.edu.sa*

**Orcid:**
https://orcid.org/0009-0003-8600-7499



## ABSTRACT

The transition to multi-layered Space-Air-Ground Integrated Networks (SAGIN) from traditional terrestrial infrastructure drastically complicates the security landscape of sixth-generation (6G) networks. In this paper, we conduct a Systematic Literature Review (SLR) evaluation on the synergistic integration of Blockchain and Zero Trust Architecture (ZTA) as two core security pillars for 6G cloud-edge Non-Terrestrial Networks (NTNs). The study investigates the use of Blockchain with Zero Trust Architecture (ZTA) to ensure context-aware access control and continuous authentication, along with decentralized trust and immutability audit property provided by Blockchain. We investigate a variety of hybrid approaches aimed at countering vulnerabilities associated with the decentralized architecture of SAGIN, such as identity spoofing, jamming, and routing attacks through a thematic and quantitative synthesis. Notably, hybrid Blockchain-ZTA-based systems attained maximum attack detection accuracies of 97%, outperforming the best standalone models in addition to requiring a latency (150−300 ms) and resource overhead. This review also explores how AI-integrated 6th-generation features can enhance anomaly detection. It concludes with a clear overview of key research trends, including the scarcity of real-world deployments, and provides a roadmap for future development focused on scalability, consensus optimization, and quantum-resilient cryptography.

**Keywords:** Blockchain; Zero Trust Architecture; 6G; Non-Terrestrial Networks; Cloud–Edge Computing; Distributed Ledger Technology; SAGIN; Security and Privacy; AI-driven Trust Management; cybersecurity; Internet of Things.

**How to cite the article**

## 1. Introduction

When designing wireless communication networks, applicants have a tendency to fall so far behind voice-based solutions that the existing systems have become highly sophisticated, information-heavy and possess global connectivity. With the advent of NTN such as satellites, unmanned aerial vehicles (UAVs), and high-altitude platform stations (HAPS), 6G is needed to expand the paradigm from terrestrial communication to wireless communication over flat air spaces. This expanded ecosystem, known as SAGIN, integrates terrestrial and non-terrestrial resources to provide ubiquitous connectivity. [1]. The rapid expansion of the NTN industry highlights how urgent it is to secure these networks. The global 6G industry is predicted to grow to over $10 billion by 2030, with non-terrestrial networks making up a sizable share of this infrastructure expenditure, according to recent market predictions. Additionally, since 2021, research papers in the intersection of 6G Security and Blockchain have increased by 300% year, according to recent bibliometric data, indicating that this area is a key priority for both the academic and business sectors. It is viewed to have SAGIN as a 6G fundamental aspect enabling new services such as autonomous mobile, autonomous digital twins, precision agriculture, and global internet of things connectivity, intelligent transportation, and real-time edge to cloud computing. The fact that 6G architectures integrate heterogeneous nodes, including satellites, edge devices, sensors, and smart gateways, hence the traditional assumptions of trust are no longer applicable in 4G and 5G [2]. Moreover, the advent of continuum computing to the cloud edge, where the processing tasks are performed freely under centralized datacenters of the clouds, distributed edge nodes, and airborne devices, makes the network more intricate and more vulnerable to attacks. Another cybersecurity problem that could be introduced by the nature of NTNs, which is dynamic, mobile, and decentralized, is weak perimeter boundaries, identity spoofing, jamming, routing attacks, and compromised satellite links [3].

In a bid to counter such shortcomings, researchers have remained interested in considering the combination of blockchain and ZTA as two supplements as security pillars in the next-generation 6G systems. By combining Blockchain's decentralized auditing with ZTA's continuous authentication, a scalable security paradigm is established for the 6G cloud-edge-NTN environment. Zero Trust, on the other hand, does not value perimeter-based security and executes continuous authentication, least privilege, and context-understanding access control [3]. Through these features, blockchain and Zero Trust can offer an effective and scalable, and decentralized security paradigm to benefit the special requirements of the 6G cloud-edge-NTN world. Given that the study in this field is fast changing, the most urgent one is a systematic review, synthesis, and analysis of the current state of affairs of blockchain- and Zero-Trust-based security solutions of 6G NTN. In this chapter, the domain itself is described, the broad methodological approaches of 6G NTN security are proposed, and the motivation, gaps in the research, and input of this systematic review are stipulated. The traditional wireless network security models attach much importance to the centralized sources of trust, periphery security systems, and fixed identities. The models were well functioning on the mobile cell networks in the ground base, whose infrastructure was immobile as the 3G, 4G, and early 5G. However, they struggle to keep pace with the greatly dynamic, multi-domain, and heterogeneous character of the SAGIN environment at the point where nodes constantly in and out or shift between space, air, and ground divisions [1].

### *1.1 Motivation*

The fast union of NTNs, edge digital computing, and AI-powered 6G information represents a basic step towards common, intelligent connectivity. But this evolution poses considerable cybersecurity risks, especially in distributed space and aerial systems. The preexisting NTN is at increased risk of more advanced threats, such as spoofing, jamming, and signal intrusions that can threaten mission-critical data. This vulnerability is key, particularly given the more than 45% increase in attacks on satellites and space systems over the past two years. As we move toward 6G, it is expected that over 10 million devices will be connected within each square kilometer, making typical centralized security approaches not only inefficient but also statistically unfeasible to scale without the use of decentralized trust models presented in this paper. Additionally, the natural movement of satellite and airborne components in SAGIN systems makes traditional centralized security models inadequate, as they fail to deliver the required reliability, scalability, and distributed trust needed to support these constantly changing environments. This review is motivated by the need to fill important gaps in existing literature and meet the high-performance demands of 6G, such as sub-1ms latency and Tbps-level throughput. Although blockchain and ZTA hold promise, existing research is fragmented across various domains such as IoT and cloud computing. There is a lack of a unified approach that is focused on SAGIN. In our quest to develop autonomous and verifiable security solutions to support AI-native communications, an analysis is required. This synthesis aims to address these shortcomings and develop a clear roadmap to implement robust and decentralized security for the next generation of global connectivity.

### *1.2 Problem Statement*

Despite the growing trend in the use of a guarantee for the security of 6G cloud-edge NTNs systems through the use of blockchain and Zero Trust models, the studies conducted so far can be considered scattered, diverse in their scope, and lacking a common assessment for their potential to address the challenge of authentication, access control, trust management, and data safety in SAGIN environments. There is no available evidence-based review that can bring all the studies conducted so far under one umbrella, identify gaps, and determine the future trends for the use of blockchain and ZTA concurrently in NTNs.

### *1.3 Research Questions (RQs)*

To fill this gap, the following research questions guide this systematic review:
• RQ1: Which are the current use cases of blockchain technologies to improve the security of 6G NTN and cloud-edge architectures?
• RQ2: How ZTA enhances authentication, access control, and trust management in distributed NTN environments?
• RQ3: What are the hybrid strategies of using blockchain and Zero Trust to secure SAGIN and 6G cloud-edge ecosystems?
• RQ4: What are the unresolved issues, challenges, and limitations that exist in the application of blockchain and Zero Trust to secure 6G NTNs?

### *1.4 Objectives*

This review aims to:
1) Examine and classify existing security methods using blockchain in NTN and 6G environments.
2) Evaluate the application of Zero Trust principles in decentralized, multi-domain cloud edge networks.
3) Discuss the existing hybrid blockchain-ZTAs offered to 6G and SAGIN.
4) Determine research gaps, limitations, and future research directions.

### *1.5 Contributions*

This systematic review makes the following contributions:

- Evaluate the application of Zero Trust principles specifically for decentralized, multi-domain cloud-edge networks.
- Examine hybrid models that combine Blockchain and ZTA for 6G and SAGIN.
- Identifies current research gaps and highlights open issues for future development of cloud-edge-NTN networks.
- Presents a research roadmap to outline steps for implementing strong, decentralized security in next-generation global connectivity.
- Evaluate performance metrics like latency, throughput, and energy efficiency to assess the technical feasibility of proposed security solutions.

This paper is divided into sections which provide a clear analysis. It begins with Section 1, which introduces the goals of the research, followed by Section 2, which provides a background on the evolution of 6G technology and decentralized trust. Sections 3 to 6 describe important technical areas: 6G visions and requirements, which include Terahertz communications; NTNs' multi-layered structure and vulnerabilities; SAGIN integration; and cloud edge computing for distributed intelligence. Section 7 provides a detailed account of the 'never trust, always verify' principle of ZTA technology. Section 8 discusses international and local laws: NCA and PDPL. The methods for conducting the study are presented in Section 9, which leads to a detailed analysis presented in Section 10: blockchain technology, hybrid approach, AI technology for enhancing security. Sections 11 to 21 present a summary of the study by discussing technical considerations, areas for further research: quantum-resistant cryptography, a general overview of the roadmap for a resilient 6G infrastructure for global deployment.

## 2. Background

The development of the new generation of wireless networks has left the early days of terrestrial cellular networks behind and now includes highly interconnected and intelligent networks with terrestrial, aerial, and space components. The path from 1G to 5G has emphasized more bandwidth, reliability, and mobility support. The move towards 6G, however, represents a paradigm shift towards global ubiquitous ultralow latency communication with the help of distributed intelligence and multi-layered network architectures [4]. In this context, NTNs as technology that includes satellite, HAPs, and UAVs have now started to emerge due to their capability to ensure coverage in extreme environments [5]. The conceptual experience of SAGIN emerges due to the requirement to interconnect these formerly non-intersecting areas into a unified, dynamic, and orchestrated 6G system [6]. There was limited satellite-terrestrial interoperability in the initial NTN rollouts with 3GPP releases 15 and 16. Later advancements included the enhancement of integration through f inter-satellite communications, laser communications, and distributed beamforming. Meanwhile, cloud computing evolved from the centralized data centers to cloud-edge-endpoint ecosystems that resulted in computation offloading, low latency services, and close to the data source [7]. These advancements were in line with the aim of 6G, which was to develop a computing-aware and programmable, AI-driven network. This was coupled with a paradigm shift in security strategies. The conventional perimeter security strategies, which were borrowed from our legacy terrestrial networks, were no longer adequate for the 6G-NTN network topology, which is highly distributed and heterogeneous. This led to the emergence of the concept of ZTA in the networking field and the integration of decentralized trust technologies such as blockchain, which was originally developed for cryptocurrency applications and later adapted for secure distributed environments [1] [8]. Thus, the historical development of the security of 6G is the convergence of NTN integration, edge intelligence, decentralized trust model, and Zero Trust paradigm. The smooth integration of terrestrial and non-terrestrial layers characterizes the architectural development of 6G. In contrast to earlier generations, 6G is a comprehensive ecosystem that uses satellites (LEO/MEO/GEO) and aerial platforms (UAVs/HAPS) to provide pervasive connection. Because of this integration, a decentralized security paradigm must replace centralized trust. A hybrid approach leverages Blockchain for auditing and ZTA for continuous, location-independent verification across the network.

### *2.1 6G Networks*

6G is the mobile communication networks that are expected around 2030. Core attributes include URLLC, ubiquitous coverage, holographic communications, and semantic transmission, as well as ISAC [5].

#### *2.1.1 Vision, Requirements, and Key Performance Targets*

To support intelligence-native, service-centric, and globally linked communication systems, 6G mobile networks are envisioned as a fundamental development beyond conventional connectivity-oriented paradigms. In contrast to 5G, which is mainly concerned with improved mobile broadband and ultrareliable low-latency communication, 6G aims to facilitate autonomous systems, seamless integration of terrestrial and non-terrestrial infrastructures, and immersive experiences. Ambitious performance goals for 6G, including sub-millisecond end-to-end latency, terabit-per-second peak data rates, extreme dependability, huge device connections, and energy-efficient and sustainable operation, are frequently highlighted in vision studies [4] [5] [9].

Ubiquitous worldwide coverage is a key part of 6G. It also involves the integration of terrestrial networks with non-terrestrial components such as satellites, high-altitude platforms, and UAVs. SAGIN and NTNs are viewed as integral parts of the architecture of 6G systems rather than being supplementary components. Moreover, there are expectations that the 6G system will have components such as computation, sensing, and AI, which have made information processing and communication indistinguishable from each other. This has created an extremely distributed, diverse, and dynamic system. This creates problems for traditional network design and security models [4] [9].

#### *2.1.2 AI-Native 6G and the Convergence of Communication-Compute-Control*

The evolution of 6G networks towards AI-native architectures, where AI is embedded into the core as a key feature rather than another optimization tool, and focuses on the evolution of network operations architecture. Machine learning models are expected to function throughout the whole network lifecycle in AI-native 6G systems, including radio resource management, mobility control, network slicing, failure prediction, and service orchestration [10] [11]. Autonomous and self-optimizing networks that can adjust to extremely dynamic situations and a variety of service requirements are made possible by this paradigm shift. 6G networks depend on the close convergence of communication, computation, and control, especially throughout the cloud–edge continuum, to enable such intelligence-driven operation. While centralized cloud resources enable extensive model training and worldwide coordination, distributed intelligence deployed at edge nodes enables latency-sensitive inference and decision-making near data sources [9] [7]. New performance metrics that supplement conventional quality-of-service indicators are also introduced by this convergence, including learning accuracy, inference latency, and AI service quality. Later sections of this review will adopt Zero Trust principles and decentralized trust mechanisms because, from a security standpoint, the widespread use of AI and automated control increases the need for continuous verification, reliable data pipelines, and auditable decision processes [10] [11].

### *2.1.3 Terahertz Communications and Ultra-High-Capacity Links*

Research is increasingly focusing on utilizing terahertz (THz) frequency ranges, which normally range from 0.1 to 10 THz, to address the huge throughput demands envisioned for 6G applications. Compared to millimeter-wave frequencies, these bands have orders of magnitude greater bandwidths, allowing for ultra-high-capacity wireless networks appropriate for data-intensive edge services, holographic communication, and high-resolution sensing [12] [13] [14] [15]. THz communication is therefore considered a crucial physical-layer enabler of 6G.

However, THz communications present significant technological difficulties, such as high path loss, atomic absorption, blockage susceptibility, and the requirement for exact beam alignment and highly directed beamforming [12] [13][14]. These restrictions form short communication ranges and high rates of connection adaptation, particularly in mobile or aerial conditions, which are relevant to NTNs. Thus, a vision for 6G incorporates tightly coupled cooperative transmissions with dense deployments and also on-demand coordination of edge computing resources powered by multi-gigahertz THz-driven systems. The integration of ultra-high capacity links, mobility, and multi-domain operation complicates security enforcement further, driving the need for resilient cross-layer coordination, secure control signaling, and solid identity management [15].

### *2.1.4 ISAC*

With the goal of integrating wireless communication and environmental sensing for a unified platform, ISAC has become one of the key components of 6G networks. With the same waveform, hardware, and spectrum resource, ISAC-based systems can support simultaneous sensing activities such as tracking, localization, and environmental perception [16] [17]. This further enhances the spectral efficiency and enables new services, comprising digital twins, context-aware network control, and autonomous mobility.

Network-wise, ISAC transforms 6G systems into sensitive networks that can interact with and respond to their actual surroundings. To achieve effective ISAC performance, however, careful waveform co-design, resource allocation strategies, and interference management between sensing and communication operations are required [16] [17] [18] [19]. Furthermore, higher-layer decision-making systems depend heavily on the sensory data produced by ISAC, including mobility, position, and situational context. Future 6G cloud-edge-NTN systems will consequently require safe, verifiable, and context-aware security procedures to ensure the integrity, authenticity, and reliability of such data.

## *2.2 Problems Facing 6G Networks*

The transition to 6G networks poses severe flaws in architecture as the network paradigm shifts to dynamic, multi-layered SAGIN [1] when changing the current, non-dynamic and non-layered approach to infrastructures. Besides UAVs and HAPS, this advancement incorporates heterogeneous nodes such as LEO, MEO and GEO satellites making it impossible to sustain a fixed security perimeter [6]. The traditional centralized trust models that have been used in 4G and 5G are no longer valid, as nodes move on a regular basis across space, air, and ground segregation's [2]. NTNs are also susceptible to advanced attacks such as jamming, spoofing, signal intrusion, and physical and link eavesdropping [20]. The unpredictable delay of propagation due to the moving nature of satellites and airborne platforms complicates the real-time authentication and safe handovers [3]. Also, there is a shift to THz communications, which is supposed to meet the colossal throughput needs of 6G, but that comes with new physical challenges of high route loss, air absorption, and susceptibility to physical obstructions [12] [13] [14] [15], all of which demand complicated, secure beam alignment methods. Incorporation of the artificial intelligence in the core of 6G (AI-native 6G) produces a new type of cybersecurity vulnerabilities. The adversaries can attack the machine learning models controlling network operations, leading to possible disruption of autonomous control of resources and anomaly detection [21] [22] through data poisoning, adversarial examples, or model extraction. These risks are also increased by the resource-constrained capabilities of NTN nodes such as UAVs and small satellites, which often do not have the energy and computing power to deploy heavyweight cryptographic solutions or continuous security surveillance [23]. Finally, governance and scalability issues affect the 6G ecosystem. Enforcing uniform security standards across international borders and various administrative domains makes incident response and regulatory compliance with frameworks like Saudi Arabia's NCA and GDPR more difficult [20] [21]. Technically speaking, current blockchain consensus methods frequently find it difficult to scale to the high node density and low latency (sub-1 ms) criteria required for 6G services, which calls for the creation of more effective and lightweight protocols [22]. Table 1 provides a comprehensive overview of the primary architectural, physical, and governance-related challenges that 6G networks must address in the context of NTNs. It also emphasizes the research importance of each issue.

**Table 1.** 6G Network Challenges

| Category | Specific Problems | Research Significance |
|---|---|---|
| Architectural | Heterogeneous nodes, dynamic SAGIN topologies, weak perimeters | Requires shift to decentralized, Zero Trust Architectures |
| Physical/Link | Jamming, spoofing, THz path loss, and signal blockages | Calls for resilient physical-layer security and secure beamforming |
| Intelligence | AI model poisoning, data extraction, and adversarial risks | Needs "Secure AI" and verifiable, tamper-resistant data pipelines |
| Resources | Energy/power constraints, high computational cost of crypto | Drives the need for lightweight security and consensus protocols |
| Governance | Multi-domain policy enforcement and regulatory compliance | Requires global standardization and auditable access control |

## 3. NTN

NTNs are comprised of satellite constellations (LEO, MEO, GEO), airborne platforms like HAPs, and UAV-based communication nodes. They increase the coverage, redundancy, and support disaster recovery.

### *3.1 NTN Architectures and 6G Integration*

NTN architectures for 6G are organized as multi-layer space–air–ground systems, where satellite constellations (LEO, MEO, and GEO), HAPs, UAVs, and terrestrial infrastructure are jointly orchestrated to provide global, resilient coverage and service continuity. In this architecture, LEO mega-constellations typically handle low-latency, high-throughput links, MEO and GEO satellites provide regional and wide-area coverage, and aerial platforms act as agile relays or moving base stations to extend connectivity in rural, maritime, and disaster scenarios. Rather than treating NTNs as overlays, recent 6G work proposes native integration of TN and NTN, using software-defined networking and virtualization so that satellite and aerial network functions can share common 6G core procedures, unified mobility management, and end-to-end network slicing across radio, transport, and core domains [6] [23].

### *3.2 Security Threats and Challenges in NTNs*

To satisfy stringent 6G requirements such as ultra-reliable low-latency communication, holographic/semantic communication, and integrated sensing and communication (ISAC), NTN architectures adopt advanced radio and networking techniques together with AI-driven orchestration. Massive MIMO, electronically steerable beams, and dense optical/RF inter-satellite links create high-capacity, flexible space backbones, while AI/ML optimizes beam scheduling, routing, and handover decisions across moving satellites and aerial nodes in space–air–ground integrated networks. At the same time, close coupling with cloud–edge–end computing distributes computation from centralized data centers to edge servers, satellite payloads, and UAV-mounted micro–data centers, enabling computation offloading and low-latency service delivery over the integrated TN–NTN continuum [24] [6].

## 4. SAGIN Architectural Overview

A unified network that contains components of space, aerial, and ground networks that allow for seamless connectivity with load balancing and multi-dimensional routing [2].

### *4.1 SAGIN Architecture and Layered Network Model*

The SAGIN paradigm of communication is a unified element that brings aerial nodes, terrestrial infrastructures, and space borne systems together in a coordinated network. Unlike traditional hierarchical cellular structures, SAGIN is a multi-layer, heterogeneous model, in which the space layer consists of LEO, MEO, and GEO satellites, the air layer consists of HAPS and UAVs, and the ground layer consists of base stations, edge servers, and IoT devices [6] [1] [5]. These layers interact dynamically in several environments to provide coverage, flexible routing, and service. Adaptive load balancing as well

ISSN: 3079-5354

as cooperative transmission can be achieved using the SAGIN architecture, which comprises layers that can dynamically offload traffic between them depending on service needs, channel conditions, and latency limits. However, the orchestration as well as control of the network can be complicated by the presence of heterogeneous nodes that possess diverse capabilities, as well as varying domains of ownership and mobility. Thus, SAGIN architectures require the presence of intelligent control frameworks that can operate across the space, air, and ground domains while at the same time maintaining service continuity as well as dependability.

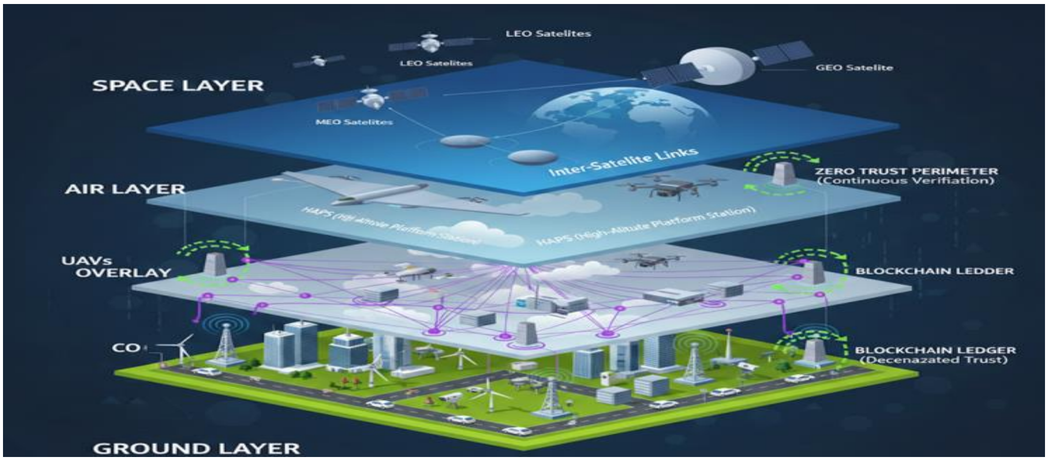



**Figure 1.** Multi-layered SAGIN Architecture for 6G Cloud-Edge Environments.

Figure 1 illustrates the three distinct yet connected layers that make up the SAGIN architecture. The Air Layer acts as a dynamic relay to lower latency for mobile users, the Space Layer provides global reach and wide-area backhaul, and the Ground Layer permits high-density IoT connection and localized edge computing. All layers of security are guaranteed via a hybrid Blockchain-ZTA system. Although ZTA uses micro-segmentation to prevent the propagation of lateral threats in the event that a single node, such as an edge server or UAV, is hacked, Blockchain offers a shared, decentralized ledger for identity management across many administrative domains.

*4.2 Mobility, Dynamics, and Topological Variability in SAGIN*

One of SAGIN's unique characteristics is its highly dynamic topology, which is mostly brought about by the mobility of satellites and airborne platforms. While UAVs and HAPS introduce stochastic mobility patterns affected by mission objectives and ambient factors, LEO satellites display predictable but fast orbital motion [5] [2]. This constant movement sets SAGIN apart from comparatively static terrestrial networks by causing regular changes in link availability, network topology, and routing patterns. End-to-end service reliability, connection maintenance, and handover management all face particular difficulties as a result of this mobility. The magnitude and flow of topology changes in SAGIN are too great for conventional mobility management techniques intended for terrestrial cellular systems [2] [9]. In order to reduce service interruption, SAGIN research places a strong emphasis on cross-layer optimization, multi-connectivity techniques, and predictive mobility modeling. From a security standpoint, the dynamic nature of SAGIN undermines perimeter-based defenses and static trust assumptions, highlighting the need for adaptive, identity-centric security models that can function in a context of ongoing topological change [5] [9].

*4.3 Resource Management and Cloud–Edge Integration in SAGIN*

SAGIN is currently under development at a very high rate in conjunction with the cloud-edge computing paradigm in order to meet the challenging requirements of 6G services in terms of the latency requirement and reliability. Such a design spreads network processing and computing load between centralized data centers in clouds, ground station edge servers, and, in some cases, aerial or satellite platforms with onboard computing power [7] [8]. An example of latency-sensitive applications that can be computed nearer to data sources because of this integration is real-time sensing, autonomous control, and mission-critical communications. In SAGIN [6] [8], resource management consists of the collaborative optimization of storage, computation, and communication resources across many levels. When making decisions about work offloading, routing, and resource distribution, the space and aerial platform must consider node mobility, sporadic connectivity, and a lack of lack aboard. This is because these limitations require adaptive orchestration techniques, which can adapt to changing network circumstances and affect service quality. The distributed and multi-domain control of resources also adds to the importance of safe cooperation, uniform execution, and verifiable actions in SAGIN systems.

### *4.4 Security Challenges and Trust Requirements in SAGIN*

A complex security scenario characterized by the absence of perimeters, multiple domain trust relationships, and increased attack surfaces is created by SAGIN. Due to the utilization of multiple administrative domains by SAGIN nodes, particularly in locations where resources are scarce, the nodes are prone to attacks such as spoofing, jamming, replay attacks, and control channel attacks [1] [3]. Moreover, intersatellite communications and wireless connections are the means through which the threats of spying and interference are heightened. In view of the dynamic and distributed nature of SAGIN, it is challenging to scale and evolve the security scenario through traditional centralized security mechanisms. Therefore, in the current research, the need to incorporate the principles of fine-grained access control, trust control, and authentication, as they relate to SAGIN, is emphasized [3] [29]. These requirements are in line with the principles of the novel security paradigms such as ZTA and blockchain-based trust, which are intended to function without implicit trust assumptions while providing unimpeachable security services. In regard to the security and reliability of the upcoming 6G SAGIN systems, the development of such systems is the way forward.

## 5. Blockchain in 6G and Edge Systems

Distributed registry with tamper evident records, distributed consensus, smart contracts, and unchangeable audit trails. In the 6G and cloud-edge environments, where the effectiveness of the traditional centralized protection infrastructures is becoming less and less, blockchain technology emerged as a key enabling technology for distributed trust management and identities. The 6G ecosystem is a combination of heterogeneous components which operate across multiple administrative and trust spheres, including edge devices, IoT sensors, aerial platforms, satellites, and cloud services. Trust anchoring and centralized authentication server in such environments lead to latency over-loads, scalability bottlenecks, and single points of failure, which cannot be supported by 6G speed requirements. Blockchain breaks these limits by providing a decentralized, irreversible and auditable trust infrastructure that can operate over distributed and resource heterogeneous nodes [4] [5] [9]. In 6G cloud-edge architectures, distributed identity management can be supported by blockchain by replacing the ledger-based processes with centralized identification authorities and thereby enabling peer-to-peer establishment of identity, its verification and maintenance. Devices, services, and people can be represented as decentralized identifiers (DID) or cryptographic identities based on the blockchain. This enables secure on boarding and authentication without the need to have constant access to a central authority [1] [8]. This strategy is of particular relevance in edge and non-terrestrial environments, where cross-domain and high mobility, as well as irregular connectivity, are common. Blockchain also enhances assurance of identity and reduces the need to use trusted intermediaries by ensuring identity credentials and trust claims are consistent and verifiable cryptographically throughout the world [5] [2]. Beyond identification, blockchain is essential to distributed trust management because it preserves unchangeable records of transactions, access events, and policy choices over the 6G cloud–edge continuum. The enforcement of authentication, authorization, and accountability standards at the edge nodes and gateways can be done automatically through the integration of trust logic and security regulations in smart contracts [9] [3]. This would be very effective in a multi-operator/multi-domain network scenario where trust relationships between different entities that do not share a common administration domain have to be established on the fly. Apart from providing auditability and non-repudiation, the append-only nature of blockchain ledgers would be very effective in highly distributed networks for analysis after an event [4] [25].

However, integrating blockchain into 6G and edge settings introduces new design challenges. The potential for standard consensus methods to introduce delays inconsistent with ultra-low-latency applications is driving research into edge-assisted blockchain architectures, hierarchical ledgers, and lightweight consensus algorithms [2] [26]. Recent research recommends strategically deploying blockchain services at edge and fog levels, using cloud resources for collaboration and long-term storage, to strike a compromise between trust assurances and performance constraints [8] [3]. Blockchain is an essential architectural component for facilitating decentralized identification and trust in future 6G systems. In spite of these challenges, particularly when combined with complementary ideas like ZTA and AI-driven security orchestration.

### *5.1 Zero Trust Architecture (ZTA)*

The ZTA is based on the paradigm shift of ensuring 6G cloud- edge and NTN by rejecting the old concept of a trusted network perimeter and adopting the new concept of never trust, always verify [30]. The highly dynamic and heterogeneous environment of SAGIN cannot be secured using the static techniques due to the frequent changes of nodes between the space, air and ground domain [31]. To stem out these susceptibilities, ZTA applies a strict authorization and authentication of every subject, device, and flow of data despite its position in the network. This is more critical in 6G design because there is an augmentation of the attack surface by the incorporation of satellites, UAVs, and edge nodes that present issues such as corrupted satellite linkage, identity spoofing, and signal intrusion. ZTA can make the network maintain a strong security posture [30] [32] by means of continuous, context sensitive monitoring which adapts to the ever-changing topology observed in mobile aerial and space platforms.

The principle of least privilege, constant authentication, and micro-segmentation is the keys to ZTA implementation since they limit risks and restrict potential violations. The Principle of Least Privilege (PoLP) can be used to reduce the blast radius in case one node, an edge server or a remotely connected Ioots sensor, is compromised by the attacker by restricting users and devices to the minimum access allowed to perform a specific task [31] [33]. Instead of a single instance of login, constant verification goes further to extend this protection by enforcing a system constantly re-evaluating the degree of trust of an entity in the basis of real-time information, including the physical health of a device, its location, and behavioral patterns, which are often enhanced by AI-based anomaly detection [30] [34]. This is achieved using micro-segmentation which establishes small, remote security zones within the network [32]. These micro-perimeters ensure that a breach in one point in the 6G-NTN continuum, e.g., a specific network slice or a satellite backhaul connection, cannot give an attacker immediate access to the rest of the infrastructure [32]. These Zero Trust ideas, combined with decentralized technologies like blockchain, may offer a verifiable and scalable security architecture that may satisfy the 6G era's high performance and dependability requirements [35].

### *5.2 Regulatory and Governance Frameworks*

The development of non-terrestrial infrastructures, cloud-edge computing, and 6G networks presents intricate regulatory and governance issues that go beyond the conventional procedures associated with telecommunications. These are the settings that necessitate adherence to cybersecurity, data protection, and AI governance systems because they involve large-scale data collection, cross-border data transfers, and AI-assisted decision-making, and decentralized trust frameworks. The EU AI Act, GDPR, and local cybersecurity and data protection laws, including NCA ECC, CCC, and the PDPL of Saudi Arabia, provide the guiding principles of fundamental governance sufficient to design secure 6G cloud-edge-NTN systems [4] [36] [37].

The GDPR offers an extensive data protection framework in distributed 6G architectures where personal and contextual data can be processed in edge, aerial and space nodes because it encompasses the ethical principles of lawfulness, data minimization, purpose limitation, transparency and accountability [38] [39]. Research indicates that additional 6G applications such as ISAC, semantic networking, and AI-native services are a major impediment to GDPR compliance, especially in respect to consent management, cross-border data transfer, and the rights of data subjects in decentralized contexts [40] [41]. Even though there are still governance challenges associated with data immutability and the right to erasure, blockchain-based methods have been explored as being the possible facilitators of GDPR-compliant accountability and auditability [39] [42].

To supplement data protection laws, the EU AI Act that classifies AI applications into four categories such as unacceptable, high-risk, limited-risk, and minimal risk, provides a risk based governance mechanism in AI systems. It is possible to categorize AI-driven capabilities influencing essential rights, safety, or the stable operation of the infrastructure (such as autonomous network control), access decision-making and anomaly detection and behavioral analytics as high-risk AI in the 6G and cloud-edge systems [36] [43]. The mandatory requirements to meet the EU AI act are strong governance mechanisms of transparency, human oversight, data governance, and model accountability, based on recent findings [43] [44]. These specifications are in close sync with the principles of the Zero Trust and the verifiable audit trails based on blockchain in distributed networks.

The operationalization of the requirements of the laws in local contexts at the national level requires cybersecurity and data protection systems. In Saudi Arabia, NCA ECC and CCC establish compulsory requirements regarding monitoring, incident response, identity and access management and third party risk management under cloud and critical infrastructure conditions [45] [24]. Because these controls particularly address risks associated with distributed architectures and collaboration models, they are immediately relevant to 6G cloud-edge and SAGIN deployments. The collection, processing, storage, and international transmission of personal data are all governed concurrently by the Saudi PDPL. It reiterates GDPR-like ideas while reflecting localization requirements and state sovereignty [21].

The security architecture of the future 6G technologies is constructed by these governance and regulatory frameworks, which emphasize privacy-by-design, accountability, continuous risk evaluation, and trust governance. Instead of depending solely on static policies or centralized enforcement mechanisms, research is increasingly acknowledging that technical enforcement in line with regulatory intent-such as ongoing verification and decentralized trust management—is required to achieve compliance [27] [28] [26]. Therefore, integrating ZTA with blockchain-based governance structures is a viable way to reconcile legal compliance with the operational realities of highly distributed, AI-driven 6G cloud-edge-NTN ecosystems.

## 6. Methodology

The methodology here includes the protocol, research questions, search strategy, inclusion/exclusion criteria, study selection, quality assessment, and data extraction/synthesis methods. Following the guidelines for a standard SLR helps to ensure transparency, replicability, and rigor in the process.

### *6.1 Review Protocol and Databases*

This SLR is conducted by following the PRISMA 2020 guidelines, which offer a proper structure for presenting the search procedures, screening, and data synthesis. The protocol of this review has been developed and registered on OSF (Open Science Framework) for improved transparency. The search strategy has been developed to achieve the best possible coverage with the highest relevance. There are three phases in this process:

• Databases Used: IEEE Xplore, ACM Digital Library, Scopus, Web of Science, ScienceDirect (Elsevier), SpringerLink, MDPI Sensors, and Google Scholar.

• Search Strings: (”6G” OR”sixth generation”) AND (”non-terrestrial network*” OR”NTN” OR”satellite network*” OR”SAGIN”) AND (”blockchain” OR”distributed ledger”) AND (”Zero Trust” OR”ZTA” OR”continuous authentication” OR ”access control”) AND (”cloud-edge” OR ”edge computing”).

• Time Period: The period considered for this review was between 2018 and 2025 since blockchain, ZTA, and 6G NTNs are areas of emerging research. Previous studies were excluded because of their lack of relevance.

Using Google Scholar, 237 records in all were first found. 111 records were eliminated prior to screening, including 68 duplicates and 43 entries that automated systems had flagged as ineligible. 38 records were excluded after title and abstract screening of the remaining 126 records. Twenty-four of the 88 reports that were later requested for retrieval were unsuccessful. After 64 reports were evaluated for eligibility, 16 were disqualified for being irrelevant. In the end, 48 papers that satisfied the inclusion requirements were added to the qualitative synthesis.

### *6.2 Inclusion and Exclusion Criteria*

To ensure relevance, quality, and rigor, inclusion and exclusion criteria were created as shown in Table 2.

**Table 2.** Inclusion and exclusion criteria

| **Criteria** | **Inclusion** | **Exclusion** |
|---|---|---|
| Publication type | Peer-reviewed journal, conference paper, or high-impact survey | Editorials, blog posts, non-peer-reviewed articles |
| Language | English | Non-English |
| Relevance | Focused on blockchain, ZTA, or hybrid solutions for NTNs/6G | Not related to NTNs, 6G, or cloud-edge environments |
| Methodology | Empirical, simulation, or conceptual frameworks | Opinion pieces without methodology |
| Availability | Full-text accessible | Abstract-only |
| Year | 2018–2025 | Before 2018 |
| Validation | Demonstrated evaluation, simulation, or case study | No validation or insufficient evidence |
| Duplication | Only one instance per study | Duplicate papers or multiple versions |

*6.3 Data Extraction*

A standardized data extraction form was used to extract consistent data from each study, shown in the Table 3.

**Table 3.** Standardized data extraction form

| Field | Description |
|---|---|
| Authors & Year | Citation details |
| Study Objective | Main research focus |
| NTN Type | Satellite, UAV, HAP, hybrid SAGIN |
| Blockchain Framework | Consensus, smart contracts, sharding |
| ZTA Mechanism | Continuous authentication, micro-segmentation, access policies |
| Dataset/Simulation | Simulation environment, dataset size |
| Metrics | Latency, throughput, energy efficiency, security metrics |
| Key Findings | Security performance, advantages, limitations |
| Research Gaps | Open issues identified by authors |

*6.4 PRISMA Flow Diagram*

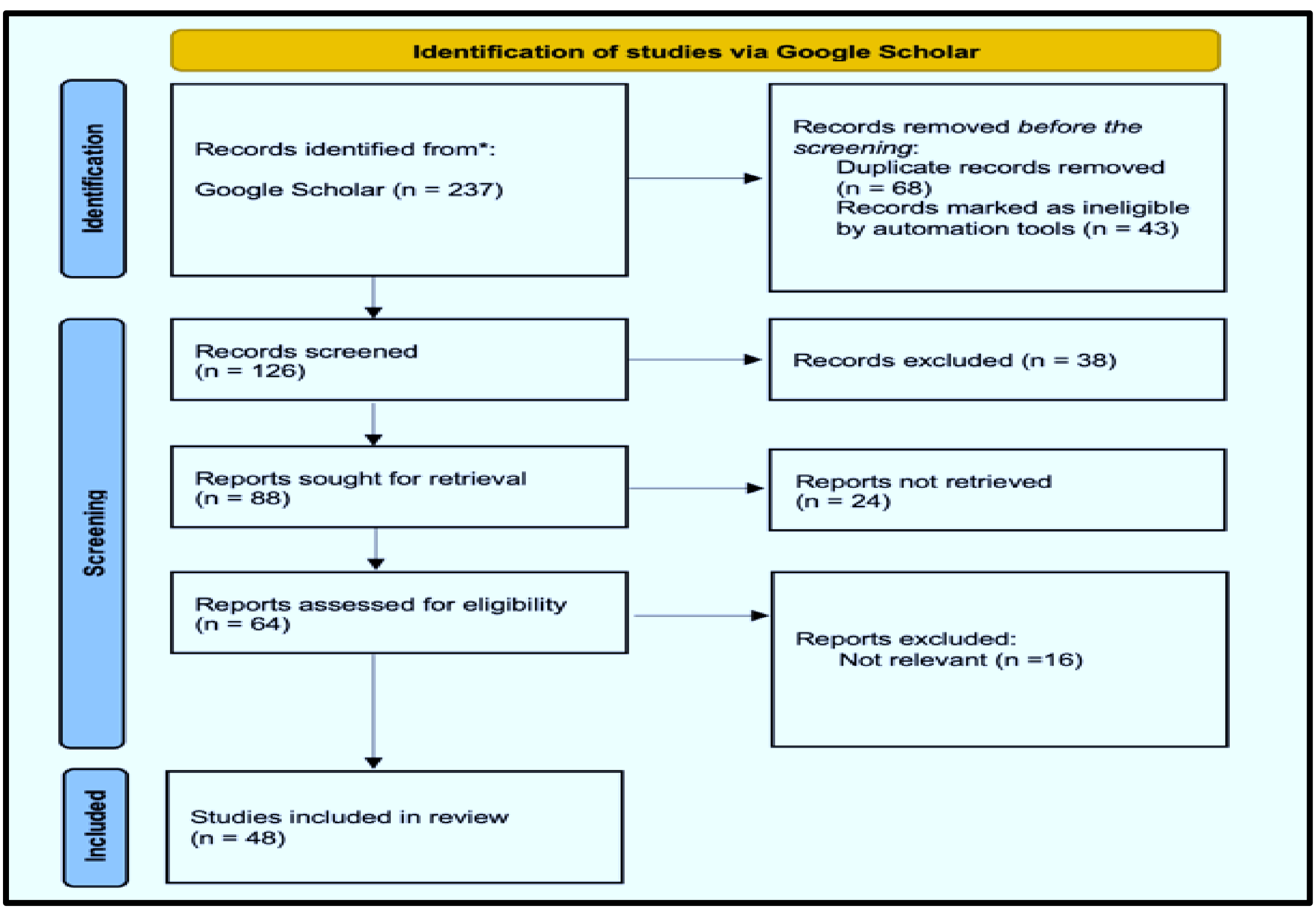



**Figure 2.** Selection of papers for literature review using PRISMA.

The overlap and noise typical of large database searches are reflected in the PRISMA screening process, which shows that roughly 47% of initially detected records were eliminated prior to screening because of duplication or automatic ineligibility filtering. 16 out of 64 full-text publications were disqualified during the eligibility round, mostly for not being sufficiently relevant to 6G NTN security or for not integrating blockchain technology with Zero Trust techniques. The limited number of thoroughly verified studies that specifically deal with the topic of hybrid security architectures for SAGIN systems can be demonstrated through the final selection of 48 studies.

## 7. Literature Review

### *7.1Overview of Selected Studies*

Most studies until 2021 focused on the basic blockchain backbones as well as the concept of Zero Trust in the context of terrestrial IoT networks, while recent studies deal with the topic of integration with SAGIN systems and edge computing platforms [5][26]. The selected studies include a variety of research types:

1) Empirical/Simulation studies (55%): Articles that simulate blockchain consensus protocol, Zero Trust and Hybrid Security Mechanisms in 6G NTN Scenarios [26].
2) Theoretical/Conceptual Studies (25%): Hypotheses of structures, frameworks, and architectures that have not been fully empirically validated yet [1].
3) Survey/Review Paper (20%): One of the Overview Blockchain ZTA and 6G security issues [2]. Thematically, the studies fall into three primary categories:

- Only based on blockchain: Aimed at safe authentication, decentralized trust, data integrity, and access control in NTNs.
- Designs that are based on ZTA: Focus on the dimensions of continuous authentication, micro-segmentation, and adaptive policy-enforcement.
- Hybrid Blockchain and ZTA designs: The architecture entails applying blockchain as a type of trust in a cognitive system to increase the security of 6G networks deployed within multi-domain environments.

There are different methodologies used in different studies. The performance measures that are more commonly used in the blockchain research field are latency, throughput, consensus effectiveness, and energy use. ZTA studies, which require access control policies, frequency of authentication, and attack resistance. Such metrics will most likely be captured in hybrid studies to measure joint security frameworks, including technical metrics and cybersecurity metrics. Regarding the technology emphasis, the articles address diverse heterogeneous components of SAGINs such as LEO/MEO satellites, high-altitude platforms (HAPs), UAVs, and edge computing nodes, which is the disparity of the technology-related elements. The cloud and edge are often simulated to replicate latency-sensitive processes, for example, authentication, sharing, and threat detection of data. This SLR detects trends and gaps:

- Move towards the hybrid security system that will involve the blockchain and ZTA.
- Increased attention to the issue of AI-assisted security checking in the detection of anomalies and optimization of security policies.
- Latency, scalability, and energy efficiency are ongoing issues with the latency, scalability, and energy efficiency of distributed NTNs.
- One of the indicators of the gap in the research carried out on simulation, and its application to practice is the very low number of real-life deployment studies [5] [7].

The quick global adoption of ZT principles reflects this tendency towards empirical confirmation. Recent industry studies indicate that 65% of 6G-related pilot projects already use blockchain as a fundamental requirement for distributed identity management, and 72% of enterprises are either developing or implementing a ZTA. These numbers demonstrate that the hybrid models examined in this SLR are at the forefront of security requirements for the upcoming decade. Altogether, this introduction demonstrates a fast-growing research area where blockchain, ZTA, and new 6G NTNs are becoming increasingly integrated, which offers thematic and quantitative analysis in the following sections

### *7.2 Thematic Classification*

The SLR showed that studies on blockchain and Zero Trust solutions for securing 6G NTNs could be systematized into five main themes. These trends represent architectural methodology, domains of application, and technological innovation throughout the SAGIN architecture. The thematic classification of the studies will enable better comprehension of the research trends, challenges, and gaps.

1) Blockchain-Enabled Security in NTNs

The blockchain solutions are a substantial part of the study under analysis. The aspects of 6G networks where heterogeneous networks are applied are authentication, trust management, secure communication, and decentralized ledger as the key focus of the studies. They are more likely to suggest blockchain architecture, such as PoW, PoS, PBFT, and sharing as the option to offer tamper-resistant validation of transactions and distributed trust between satellite, UAV, and edge nodes [1] [8]. According to the study, data integrity and auditability are improved, and it also presents latency and scaling challenges, as well as consuming energy mostly on NTN nodes that have limited resources.

2) ZTA for 6G Cloud–Edge Networks

ZTA is an idea utilized to complement the traditional perimeter-based security. Presence of continuous verification, micro-segmentation, access control, and cross-domain policy enforcement is mentioned [3]. ZTA models can be particularly used in SAGINs with models of trust that cannot be employed in dynamical models, and in which there is multi-domain ownership. These kinds of studies indicate that ZTA would reduce insider threats and unauthorized access to systems, but the overheads in implementation are a concern in the NTN, which is a latency-sensitive environment.

3) Hybrid Blockchain–ZTA Approaches

There is an increasing body of studies exploring hybrid models involving blockchain and ZTA to exploit the two models' advantages [3] [2]. Blocks. In such models, blockchain serves the role of a trust anchor and ensures that auditable policy enforcement is performed, with the ongoing access checks by ZTA. Cross-domain data sharing, multi-tenant edge computing, and secure satellite communications are proposed areas that have hybrid solutions, indicating improved security and compliance. Nonetheless, they typically must face performance tradeoffs as a result of the computational overheads involved with a consensus mechanism and dynamic policy assessment.

4) AI-Enhanced Security Mechanisms in 6G NTNs

The recent research integrates AI and blockchain as well as ZTA to support the adaptation process of anomaly detection, the prediction of threats, and policy management. The approaches that can realize the existence of malicious activities and alleviate them without jeopardizing the data privacy are federated learning, RL, and GNN [8] [2]. The application of AI is particularly beneficial when it comes to real-time choice making in cloud-edge-NTN systems that are distributed, as it complicates the assurance of the accuracy of the model, its computability, and the heterogeneity of the data set.

5) Cryptographic and Privacy-Preserving Protocols

Another group of literature is devoted to the consideration of advanced cryptography and privacy-preserving protocols. They are inner-product encryption, homomorphic encryption, and post-quantum cryptography, which can be used to secure cross-domain communication and multi-tenant edge/cloud services [3]. The protocols provide confidentiality and integrity of data over untrusted environments, but they are computationally costly and could pose a barrier to real-time data manipulations when using NTN.

### *7.3 Detailed Analysis by Category*

The section gives a detailed discussion of the five main themes that were noted in the SLR, including blockchain-enabled security, ZTA, hybrid blockchain-ZTAs, AI-enhanced security systems, and cryptographic/privacy-preserving protocols. All the themes are analyzed critically regarding methodology, applications, findings, and limitations, and their applicability in ensuring the security of 6G NTNs in cloud-edge architectures.

1) Blockchain-Enabled Security

It is necessary to add that the best solutions, which are based on blockchain, create an enormous concentration on the security of NTNs, as they are naturally decentralized, immutable, and resistant to manipulation. They may include such frameworks as Proofs of Work (PoW), Proofs of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and shards to provide confidence in distributed nodes (satellites, HAPs, and UAVs) and the IoT devices [2]. The uses of NTN in applications include secure authentication of devices, distributed ledger logging, consensus-based access control, and decision making. It has been researched that blockchain will decentralize the source of trust by eliminating points of failure and supplying enhanced trustworthiness to the information within the heterogeneous 6G networks. For example, one of the suggestions [2] made was the flow of IoT communications in the context of SAGINs that were implemented with the help of blockchains, which not only contributed to the enhancement of the credibility of authentication but also provided a chance to share the information in a traceable format. Sometimes, despite these advantages, there are severe problems with the NTN solutions found on blockchain. The PoW and PBFT models take precautions against the presence of latency, which is essential in satellite networks or edge networks that have delays. The problem of the overhead and high computation cost also exists in devices with low energy [8]. Furthermore, implementing blockchain and the current networks of 6G protocols will demand changes, adjustments, and optimization of the networks, and these points are the focus of the recent research.

2) ZTA

ZTA overcomes these drawbacks of the perimeter-based security strategy as it presupposes the unavailability of implicit trust and applies the principles of the very notion of continuous authentication, policy-based access control, and micro-segmentation [26]. ZTA is specifically used in the communication of edge nodes and cloud servers within the NTNs, where traditional security has failed due to the dynamism in the topology and the multi-operative configuration of the NTNs. Important observations allow ZTA to mitigate the attack surface, cross-domain security, and insider threat resiliency. As [8] has shown, they managed to create a blockchain-based architecture of a ZTA that has already integrated continuous verification and enforced secure policies to ensure high-quality access control and auditability. The cloud-edge architecture is used in ZTA implementation to ensure real-time mitigation of anomalous access attempts by making policy changes in real time. Nevertheless, overheads are added to NTNs by ZTA, especially in the distributed and high-latency environment. Introduction of cross-domain policies will cause delays in authentication and authorization, which can be a problem when real-time operation is required. In addition, the high-tech policy management demands some powerful instruments of control and coordination, which are still in progress.

3) Hybrid Blockchain–ZTA Systems

The ZTA frameworks that have hybrid systems incorporate blockchain-based trust anchors to achieve decentralized trust and never-ending verification [1]. They have been explored to be progressively implemented in the cross-domain sharing of data, multi-tenant edge computing, and satellite communication networks, where the dynamically evolving trust relationships and decentralized governance are the norm. Some of these benefits are auditable policy enforcement, decentralized authentication, and increased adherence to security measures. To name an example, the article by [26] gives a sharing blockchain system with ZTA as the means to facilitate the sharing of data between domains on a large scale, and with access control being very efficient. Moreover, another way of enhancing the monitoring capabilities of ZTA is the use of blockchain to store the records of the access events that cannot be removed, as evidenced by [2], which heightens this monitoring ability. However, hybrid systems are expensive. Latency and overhead of resource consumption are the overheads of the application of the blockchain consensus algorithm and constant verification policy. These issues are also made complicated by multi-layered network structures because, with real-time edge and satellite communications, SAGINs are more likely to have this form of network structure.

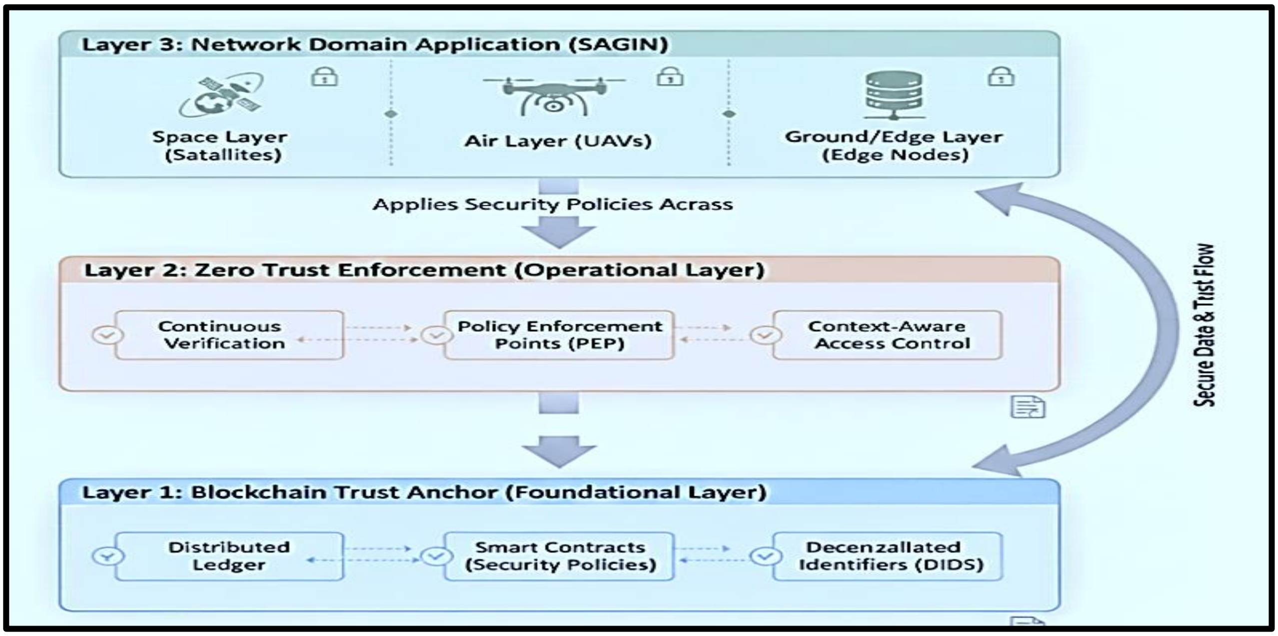



**Figure 3.** Hybrid Blockchain–ZTA Integration for 6G SAGIN.

As shown in Figure 3, the Blockchain Trust Anchor (Layer 1) offers a decentralized basis for identity management and immutable policy storage via smart contracts and decentralized identifiers in the Hybrid Blockchain–ZTA Integration Model, which operates as a multi-layered security architecture. Through this process of continuously verifying requests for access against the blockchain's ledger, this foundation provides support for ZT Enforcement (Layer 2), which is based on the principle of "never trust, always verify." To ensure that attacks are accurately detected within the SAGIN ecosystem defined for 6G, this security is eventually applied across the Network Domain Application (Layer 3), ensuring that communication within the Space, Air, and Ground/Edge layers is secure, context-aware, and protected against lateral movement attacks.

4) AI-Enhanced Security Mechanisms

The blockchain and ZTA models also propose AI-enhanced solutions to increase threat detection, optimization of policies, and prediction of anomalies [29] [27]. These types of techniques, such as federated learning, RL, and graph neural networks (GNNs), may assist the distributed nodes to understand whether there is malicious activity or not without exposing inherent data, preserving privacy in cloud-edge-NTN. According to these articles, AI can minimize false positives, dynamically modify security policies, and improve predictive threat mitigation. The federated learning through blockchain consensus provides an assurance that the individual edge nodes are learning based on the general trends and data integrity, and decentralization. These problems are computational problems, heterogeneity of the data set, and possible privacy violations. Federated learning causes extra overhead in network communication, and AI models need ample training data in a variety of NTN nodes, which can affect the performance of the network in latency-sensitive layers of SAGIN.

5) Cryptographic & Privacy-Preserving Methods

Both complex cryptography and privacy-sensitive protocols also play an important role in the provision of safe exchange of information between the un-trusted domains. Inner-product encryption, homomorphic encryption, and post-quantum cryptography are some of the cryptographic encryption techniques that deliver confidence and integrity and are quantum attack resistant [8]. They include cross-domain communication, multi-tenant edge computing, and satellite-to-ground data sharing. Protocols enhance the ZTA, blockchain architecture, in the sense that the sensitive information is not revealed even in a mistrustful environment. However, because they are computationally costly, they could not be helpful in real-time in NTNs with limited resources. Table 4 presents a comparative analysis of security approaches.

**ISSN: 3079-5354**

**Table 4.** Comparative Analysis of Security Approaches

| Theme | Methods | Pros | Cons | Applications | Key Metrics |
|---|---|---|---|---|---|
| Blockchain-Enabled Security | PoW, PoS, PBFT, Sharding | Decentralized trust, data integrity | Latency, high energy consumption | Satellites, UAVs, IoT nodes | Latency, throughput, energy |
| ZTA | Continuous auth, micro segmentation | Reduced attack surface, flexible policy | Overhead in distributed systems | Cloud, Edge, Multidomain NTNs | Access success rate, policy enforcement time |
| Hybrid Blockchain–ZTA | Blockchain + ZTA | Decentralized trust + continuous verification | Latency, resource overhead | Multitenant edge, cross-domain sharing | Latency, security events logged |
| AI Enhanced Security | FL, GNN, RL | Adaptive, predictive, reduces false positives | Computation, data heterogeneity | Cloud edge NTN anomaly detection | Detection accuracy, false positive rate |
| Cryptographic & Privacy Preserving | Homomorphic, Inner product, PQ crypto | Data confidentiality, quantum resistance | Computational cost, real-time limits | Secure communication, multidomain sharing | Encryption time, throughput, privacy leakage |

Figure 4 integrated flow shows how several security strategies work in concert to meet the particular difficulties faced by 6G NTNs.

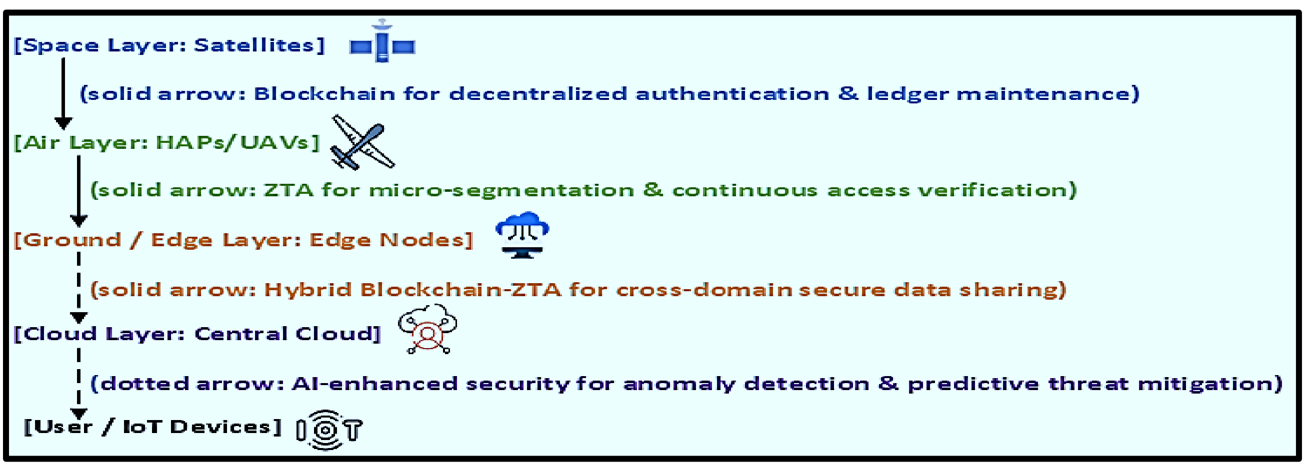



**Figure 4.** Flow Diagram.

- **Space Layer:** Blockchain is used by satellite nodes for decentralized ledger management and authentication.
- **Air Layer:** Continuous access verification and micro segmentation are achieved by HAPs and UAVs using ZTA.
- **Ground/Edge Layer:** Edge nodes integrate hybrid blockchain-ZTA systems for secure cross-domain data sharing.
- **Cloud Layer:** AI models optimize policy enforcement, anomaly detection, and predictive threat mitigation.

*7.4 Quantitative Analysis*

Quantitative analysis in the context of Blockchain and Zero Trust towards 6G NTNs, Insights into performance trade- offs, scalability, and security efficiency across heterogeneous network components. A variety of metrics have been extracted from the selected studies: latency, throughput, energy efficiency, security performance, and scalability, which represent the technical feasibility of proposed solutions in space-air ground/cloud/edge integrated networks [8] [3] [2]

 ISSN: 3079-5354

1) Latency

The latency is again a significant measure in the NTN security case, as the propagation delay among the satellite communications and the HAP communications is high. Blockchain-based solutions are latency-variable, most of which are required to be related to consensus mechanisms. Research demonstrates that the convergences in PoW consensus introduce the longest delay that frequently exceeds hundreds of milliseconds, and PBFT and shard-based approaches are lowering the delay significantly to achieve the improved viability of operations of edge-assisted NTN applications [1]. There is an addition of extra verification latency by the Zero Trusts in the case of distributed and cross-system. Additional time on the transaction of 50-150 ms of continuous authentication and policy-related evaluation can be added based on the complexity of micro-segmentation policies and the size of the network [3]. This makes use of hybrid blockchain - ZTA systems that combine the two above with the overheads alongside a focus on a trade-off between decentralized trust and control, with the right access in real-time, and thus necessitates optimization strategies in the case of a latency-sensitive application.

2) Throughput

Throughput analysis is concerned with blockchain transfers and NTN link defense. In the conditions of simulated NTN, PoW blockchain performs about 2030 TPS, compared to PBFT and shared blockchains having a hundred thousand TPS, permitting more data throughput in terms of authentication records and cross-domain interaction [8]. ZTA models exhibit low effects on data throughput because policy enforcement is localized; at the same time, the hybrid systems can insignificantly decrease throughput because blockchain and ZTA interact with each other [2].

3) Energy Efficiency

Energy efficiency is especially applicable to UAV, HAP, and satellite nodes, which are low-power applications. PoW mechanisms in blockchain require large amounts of energy, as they use 50100 W of energy per node when simulated, which is very high, whereas PoS and sharing use much less energy [1]. ZTA has little overhead in energy consumption; it is also linked mainly with policy evaluation and authentication checks. The hybrid scheme enforces more energy needs yet can be handled using an adaptive consensus protocol and selective verification scheme.

4) Security Performance

Security effectiveness is determined by the detection of attacks, and attacks that are real and even false positives. In NTN simulations, blockchain solutions are highly tamper-resilient and auditable, and are able to detect 90-95 percent of the malicious NTN. ZTA increases insider attacks and unauthorized access, as 85-92 percent of the detection rates depend on the fineness of the policies [3]. Hybrid models can never be inferior to the other standalone models with a great accuracy of about 97 percent to detect counterfeits, and in some instances, false positives could be attributed to multiple verification processes [2].

5) Scalability

Scalability can be measured by the number of devices and nodes that the technology will support, and the capacity of integration at the cloud-edge level. Scalability is a bottleneck due to the inability of PoW networks to support more than 1, 0005,000 nodes in NTN-like conditions, and sharing-based solutions being able to support tens of thousands of nodes [8]. ZTA is an efficient metric on both the edge and cloud levels, but experiences difficulties in implementing multi-operator NTN. Intermediate scalability is witnessed in hybrid systems, which are limited by the blockchain consensus and have access to distributed policy enforcement provided by ZTA. Table 5 presents a comparative analysis of Blockchain, ZTA, and Hybrid approaches, focusing specifically on latency, throughput, and energy consumption of various consensus mechanisms.

**Table 5.** Comparative Performance of Blockchain, ZTA, and Hybrid Approaches

| **Metric** | **Blockchain** | **ZTA** | **Hybrid Blockchain-ZTA** |
|---|---|---|---|
| Latency | High (PoW: 200–500 ms) | Moderate (50–150 ms) | High-Moderate (150–300 ms) |

| | | | |
|---|---|---|---|
| Throughput | Low–Moderate (20–1000 TPS) | High | Moderate-High |
| Energy Efficiency | Low (PoW high) | High | Moderate |

An explicit architectural comparison of Blockchain-only, ZTA-only, and Hybrid models is provided in Table 6.

**Table 6.** Explicit Architectural Comparison

| **Feature** | **Blockchain-Only** | **ZTA-Only** | **Hybrid Blockchain–ZTA** |
|---|---|---|---|
| Trust Model | Decentralized ledger | Identity-centric continuous verification | Decentralized + continuous verification |
| Authentication | Ledger-based identity validation | Continuous contextual authentication | Combined decentralized + dynamic |
| Insider Threat Protection | Moderate | High | Very High |
| Latency | High (consensus delay) | Moderate | Moderate–High |
| Scalability | Limited by consensus | High | Moderate |
| Auditability | Strong (immutable ledger) | Limited logging | Strong + policy traceability |
| NTN Suitability | Good for identity & logging | Good for micro-segmentation | Best overall balance |

Figure 5 shows Average Latency across Blockchain Consensus Mechanisms, the PoW: Highest latency, PoS: Moderate latency, and PBFT/Sharding: Lowest latency. Illustrates tradeoffs between decentralization and speed.

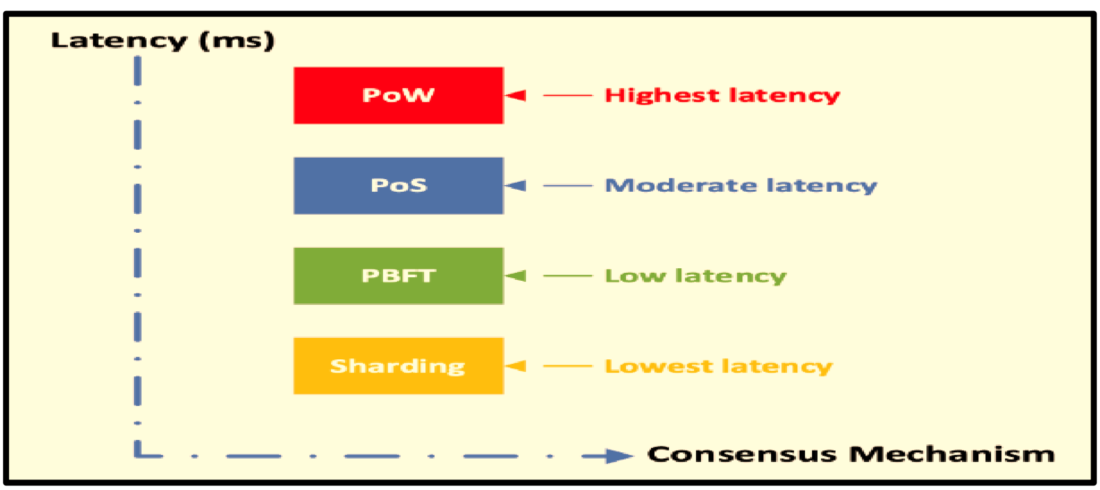



**Figure 5.** Average Latency across Blockchain Consensus Mechanisms.

6) Discussion of Trade-Offs and Limitations

Quantitative analysis demonstrates the trade-off between security/performance. Blockchain is a form of operation that guarantees an operation that cannot be tampered with, but it has a cost in terms of latency and energy usage. ZTA has solid access control at a lower overhead, though it requires extensive policy management. Hybrid and AI-enhanced models can be used to enhance the general security, although such implementations should be optimized very carefully to maintain a balance between the throughput, latency, and energy consumption. The limitations regarding methodology also have an influence on generalizability. Since most studies use simulated networks rather than real-world NTNs, the results may be skewed by different assumptions about network layout, node capabilities, and traffic patterns. To achieve a trustworthy performance evaluation, future research must involve standardizing benchmarking and comprehending real-world SAGIN implementations.

### 7.5 Tools, Datasets, and Benchmarks

In the analyzed literature, it can be found that a variety of tools, datasets, and benchmarking strategies are evaluated to assess blockchain, ZTA, and hybrid security mechanisms in 6G NTNs. Knowledge of these tools is the key to replicability, performance comparison, and methodological rigor in future research studies.

1) Simulation & Development Tools

Most of the research is based on simulation settings to create a model of the complex SAGIN architectures because the NTN implementation in the real world is quite problematic in practice. Commonly used tools include:

• **NS-3:** A network simulator that is based on discrete events (simulation) is often integrated with blockchain modules to simulate the behavior of the latency with throughput and consensus to model the satellite, UAV, and edge communications [8].

• **OMNeT++:** Emulates network multi-layers and can be utilized to evaluate the ZTA and hybrid blockchain-ZTA systems as a blend of heterogeneous nodes [1].

• **MATLAB/Simulink:** The instrument will be applied to prototype a new algorithm, analyze cryptography, and define the energy efficiency of the blockchain and ZTA deployment.

• **Hyperledger:** Hyperledger Fabric and Ethereum Test nets: Hyperledger Fabric and Ethereum Test nets are used to support testing of blockchain systems and include PoS, PBFT, and shard systems to the NTN applications [26].

The tools enable researchers to model large-scale SAGIN networks with denser variable node density and network traffic and attack conditions, to give measurable performance indicators, which include latency, throughput, and associated energy consumption.

2) Datasets

Since there is not much data available on actual NTN, several studies use synthetic data or benchmark datasets that are customized to the IoT and satellite communication sphere:

• **IoT-6G Traffic Datasets:** Synthetic data that constructs the heterogeneous communication of IoT devices in space-air-ground networks [2].

• **UAV Satellite Communication Logs:** Simulated with NS-3 or OMNeT++ to simulate the mobility, change of location, and variability of links.

• **Security and Attack Datasets:** Get synthetic logs of unauthorized access attempts, intrusions, and policy violations, and test ZTA and hybrid frameworks.

These datasets do not accurately represent the unpredictability of real-world NTNs due to unknown satellite connections stalling, etc., even with the option to control the experiment.

3) Benchmark Metrics

In research, comparable performance metrics are used:

- Latency: Blockchain agreement stalling, ZTA verification time.
- Throughput: Capacity of network link (TPS).
- Energy Saving: the power consumption of UAVs, satellites, and edge nodes.
- Security Performance: Detection, False positive.
- Scalability: Performance, cross-domain integration, and node limit support.

The hybrid performance index, which is a customized benchmark for multi-layer NTN, including security, energy, and latency metrics, is also a suggestion made by many researchers. A comprehensive summary of the simulation tools, datasets, and specific benchmarks utilized across these reviewed studies is presented in Table 7.

**Table 7.** Summary of Tools, Datasets, and Benchmarks in Reviewed Studies

| Tool / Dataset | Purpose | Representative Studies | Metrics Evaluated |
|---|---|---|---|
| NS-3 | Network simulation for SAGIN | [8] | Latency, Throughput, Energy |
| OMNeT++ | Multi-layer network simulation | [1] | Latency, Scalability |

| | | | |
|---|---|---|---|
| MATLAB / Simulink | Algorithm prototyping, cryptography | [3] | Energy, Throughput, Security |
| Hyperledger Fabric / Ethereum | Blockchain framework testing | [26] | Latency, TPS, Security |
| IoT-6G Traffic Dataset | Simulated IoT communication | [2] | Throughput, Scalability |
| UAV & Satellite Logs | Node mobility & link simulation | [8] | Latency, Energy |
| Synthetic Security Logs | Policy violations, intrusion events | [3] | Detection Accuracy, False Positives |

The results show that the benefit of simulation-based evaluation is predominant in the field due to the logistics involved in the practical deployment of 6G NTNs in a real-world setting. Although these tools offer certain insights regarding security and performance, for future research, certain aspects could be improved by integrating blockchain with ZTA in a real-world setting, working on actual datasets, and testbeds, and also by adopting certain standard metrics to ensure the development of robust, scalable, and energy-efficient security frameworks for 6G NTNs.

## 8. Results and Discussion

### *8.1 Synthesis of Key Findings*

This section gives a brief summary of the results of the study of the SLR, trends, efficacy, and solutions of blockchain, ZTA, hybrid systems, AI-enhanced solutions, and cryptographic solutions in securing 6G NTNs. It discusses the key gaps, challenges, and limitations that are identified by the studies reviewed. This is to give a general overview of the state-of-the-art and help in future studies in the development of secure and scalable SAGIN

#### *8.1.1 Trends in Security Approaches*

Based on the reviewed literature, the following are the distinct trends in the security of 6G NTNs:

- Blockchain Adoption: There is an ever-increasing interest in decentralized systems of security that use the concept of blockchain for the enhancement of trust and integrity of the data sent to the satellite, HAP, UAV, and IoT nodes [1] [8]. The most used blockchain in heterogeneous layers of SAGIN entails tamper-proof logging, decentralized authentication, and distributed ledger management.
- ZTA: According to recent studies, ZTA represents one of the essential approaches to the implementation of continuous authentication, micro-segmentation, and policy-based access management in cloud-edge-NTN networks. ZTA is a tool to overcome the threat of insiders as well as unauthorized access in a dynamic 6G, which encompasses many domains [3].
- Blockchain-ZTA architectures Hybrid models: It has been seen that the hybrid models of blockchain with ZTA can offer cross-domain trust, auditable transactions, and fine-grained access control. It has been reported that hybrid protocols are more efficient and confident in terms of security as compared to single blockchain or ZTA protocols [26] [1].
- AI-provided security: FL, RL, and GNN are used in conjunction with blockchain and ZTA to predict threats, identity abnormalities, and optimize security strategies. Threat detection is enhanced with the involvement of AI because there are fewer false positives [8] [2].

#### *8.1.2 Methods and Mechanisms*

**Blockchain mechanisms:**

- PoW is commonly considered a decentralized consensus that is energy-consuming and latency-biased.
- Evidence-based approaches of PoS and sharing are desirable with edge-cloud integrated SAGIN environments because of enhanced energy efficiency and throughput.
- Multi-node NTN applications are related to the use of PBFT in deterministic consensus [1].

**ZTA mechanisms:**

- Verification ensures that all requests to access are verified.
- Micro-segmentation isolates the networks into small areas in order to limit how the attackers will move in the future.

- Access control is enforced by the cross-domain engines at the cloud, edge, and NTN layers [3] .

**Hybrid integration:**

- Blockchain is part of distributed ZTA policies.
- Hybrid systems are audit-able, have decentralized authentication and policy enforcement, and AI modules are maximizing the predictive security [26].

**Cryptography and Privacy-Preserving Techniques:**

- Homomorphic encryption and inner-product encryption can be used to make cross-domain computations safe.
- The future quantum threats are tackled through postquantum cryptography.

*8.1.3 Effectiveness of Approaches*

**Security performance:**

- Blockchain alone achieves 90–95% attack detection in simulation scenarios.
- ZTA improves resilience against insider threats, achieving 85–92% detection rates.
- Hybrid blockchain-ZTA systems consistently achieve 97% detection accuracy while maintaining auditability [2].

**Latency and throughput:**

- PoW consensus introduces latency (200–500 ms), whereas PBFT and sharding reduce delays to 50–150 ms = [8].
- ZTA adds 50–150 ms verification delay depending on policy complexity.
- For the hybrid systems, intermediate latency is observed, but the throughput is optimized for the SAGIN layers.

**Energy efficiency:**

- PoW consumes the most energy; PoS and sharding mechanisms are significantly more efficient.
- ZTA consumes minimal energy for policy verification.
- Hybrid systems require moderate energy but remain feasible for UAV and edge devices [1].

**Scalability:**

- The scalability of the blockchain is hindered by the overhead of the consensus mechanism.
- The scalability of the ZTA is observed, but challenges arise in the multi-operator NTN scenario.
- The hybrid systems have optimized the scalability of the network with tens of thousands of nodes in the network [26].

A summary of the comparative performance and security metrics of each of these paradigms, including their respective integrations of AI enhancements, is provided in Table 8

**Table 8.** Summary of Key Findings across Security Approaches

| Metric | Blockchain | ZTA | Hybrid Blockchain-ZTA | AI Enhanced |
|---|---|---|---|---|
| Security Performance | 90–95% | 85–92% | 97% | 95–98% |
| Latency (ms) | 200–500 | 50–150 | 150–300 | 150–250 |
| Throughput (TPS) | 20–1000 | High | Moderate-High | Moderate-High |
| Energy Efficiency | Low | High | Moderate | Moderate |
| Scalability (Nodes) | 1k–10k | High | Moderate-High | High |

*8.1.4 Gaps in Literature*

- **Real-world deployment gaps:** Most studies are based on simulation models rather than using live SAGIN testbeds. Real-world satellite, UAV, and edge environments are known to have unpredictable latency, jitter, and link failures that are difficult to simulate [2].
- **Latency-energy trade-offs:** There are very few studies that have quantitatively evaluated the performance of HB-ZTA systems for real-time NTN applications [8].

- **Scalability constraints:** Blockchain-based systems are known to have scalability constraints for expanding the number of nodes in the network using PoW-based blockchain systems. ZTA also has scalability problems in terms of enforcing policies in a multi-domain heterogeneous network.
- **Cross-domain policy enforcement:** ZTA systems do not take into account the issue of cross-domain policies.
- **Privacy-preserving gaps:** Homomorphic encryption and post-quantum cryptography are computationally expensive, making them difficult to deploy in low-power NTN devices [26].
- **AI integration gaps:** FL and anomaly detection mechanisms for the entire SAGIN layers are still an open research problem. A comparative overview of the key literature gaps, as they relate to the specific key issues, is presented in Table 9.

**Table 9.** Literature Gaps vs. Reviewed Studies

| Gap | Representative Studies | Key Issue |
|---|---|---|
| Real-world deployment | [8] [2] | Simulation only, limited field trials |
| Latency-energy trade-off | [1] | Consensus and ZTA verification overhead |
| Scalability | [26] | Node expansion is limited by PoW and policy complexity |
| Cross-domain policy | [3] | Regulatory & operator heterogeneity |
| Privacy-preserving | [2] | Computation-heavy encryption methods |
| AI integration | [8] | Federated learning and anomaly detection gaps |

*8.1.5 Challenges in the Domain*

1) **Heterogeneous Network Topology:** The network topology of the NTN includes satellites, UAVs, HAPs, edge nodes, and cloud infrastructure, making the security protocol development challenging due to topology dynamics and propagation delay [8].
2) **Resource Limitations:** The energy, memory, and processing capabilities of the satellite and UAVs limit the consensus of the blockchain and AI processing [1].
3) **Security vs. Performance Trade-off:** High security features may result in lower speed, i.e., (load). However, the hybrid approach with the involvement of AI aims at achieving the trade-off between security and performance, but optimization is required in this regard [3].
4) **Multi-operator Governance:** It is challenging to manage access policies for multiple satellite systems, edge cloud nodes, and satellite operators [2].
5) **Integration with Legacy Systems:** The blockchain/ZTA-based security protocols may not support legacy IoT devices and 5G networks, where backwards compatibility is an essential criterion [6].
6) **AI Deployment Challenges:** Federated learning is required in the deployment of AI in the NTN, where the availability of distributed data is essential, while the updates in the AI model may be cached in the NTN due to high latency in the connections.

*8.1.6 Why Hybrid Systems Outperform Standalone Architectures*

Due to the fact that they incorporate two distinct security aspects, the hybrid model outperforms the standalone approach in terms of security. It is important to note that, although the Blockchain approach does not offer adaptive real-time access control, it does offer decentralized trust anchoring and immutability. On the other hand, the ZTA approach is based on trusted identity backbones but demands constant contextual verification. In the hybrid model, the dynamic least privilege access regulations are enforced by the ZTA, while the use of the Blockchain approach ensures the availability of an audit trail, as well as verifiable identification. Spoofing, insider, and cross-domain attacks are also better countered in the hybrid model than in the standalone approach. Quantified data shows that the hybrid model can successfully identify objects with an accuracy of up to 97%, while the standalone Blockchain model can achieve 90-95%, and the standalone ZTA model can achieve 85-92%. In the context of the SAGIN, the hybrid model offers a reasonable compromise between operational viability, constant verification, and decentralization, while minimizing the latency and overhead associated with the use of the Blockchain approach.

### *8.1.7 Critical Comparative Analysis beyond Synthesis*

While previous studies summarised blockchain or Zero Trust solutions separately, this research adds to the field by closely evaluating architectural fit, performance trade-offs, and deployment practicality inside 6G NTN–SAGIN settings. This SLR's main analytical finding is that blockchain-only strategies are more like trust-anchoring methods than whole security systems. They don't have adaptive runtime access control, but they do have distributed logging and immutability. On the other hand, ZTA-only models are excellent at enforcing fine-grained access, but they depend on centralized or semi-centralized trust anchors, which could cause inefficiencies in multi-domain NTN installations. Because hybrid Blockchain–ZTA architectures combine continuous contextual verification with immutable decentralized identity anchoring, they perform better than standalone models. However, especially in UAV and satellite nodes with limited resources, this improvement comes at the expense of higher latency and processing overhead. Therefore, rather than only combining performance measurements, this evaluation is unique in that it finds architectural complementarities.

### *8.1.8 Practical Validity and Deployment Constraints*

The extensive reliance on simulation-based validation is a major weakness found in all of the analyzed research. In order to adequately replicate real-world NTN conditions such orbital mobility dynamics, sporadic satellite connectivity, atmospheric interference, and unpredictable link jitter, the majority of assessments were carried out using NS-3, OMNeT++, MATLAB, or synthetic datasets. Because there are still few real-world SAGIN implementations, findings about latency, scalability, and energy efficiency need to be interpreted with caution. Hybrid architectures would be more reliably validated through field tests using edge-cloud orchestration, UAV swarms, and LEO constellations. Therefore, even though hybrid Blockchain–ZTA models show better security metrics in simulation, more empirical research is needed to confirm their operational viability in ultra-low-latency (<1 ms) 6G scenarios.

### *8.2 Analyzing Performance Measures in the Face of Experimental Heterogeneity*

The values of parameters such as latency, throughput, energy efficiency, accuracy of detection, and scalability are presented in Tables V and VIII, but it is essential to interpret these values carefully. The values are based on heterogeneous experimental results, including different types of consensus schemes, modeling tools, densities of nodes, propagation delay, and types of threats. For example, network topology, types of consensus schemes, and simulated satellite altitude, such as LEO and GEO, are significant factors for evaluating delay-based parameters. Analogously, thresholds for anomaly detection, behavior of adversaries, and datasets are also significant for evaluating accuracy-based parameters. Therefore, the range of clean values presented for comparative purposes should be considered to show trends across architectural categories rather than to be considered as equivalent performance metrics. It is also essential to conduct research on standardizing benchmark frameworks for evaluating security aspects of 6G NTN-SAGIN systems.

## 9. Limitations

There are various limitations to this study. First, there is a potential for a performance bias, considering that most of the research are based on simulation validation rather than actual implementation of the NTN. Second, there is a difficulty in making a direct comparison, considering that parameters for latency and scalability vary based on simulation assumptions. Third, industry reports on testbeds may not be considered for evaluation, considering that this paper is based on publications that are Google Scholar-indexed. Fourth, actual SAGIN infrastructures failed to benchmark implementation complexities of hybrid security approaches. Lastly, there is a potential for a consensus model to be obsolete considering that there are rapid technological advancements for 6G.

## 10. Future Directions

This is an SLR with a critical analysis of the state of the art on Blockchain, ZTA, AI-based security, and advanced cryptographic solutions for 6G NTNs SAGIN architectures. Whilst the review does demonstrate promising trajectories, it also shows there are severe shortcomings in aspects of scalability, energy efficiency, real-world deployment, and cross-domain interoperability. Therefore, future research directions and some practical advice are presented in this section, as well as a summary of conclusions to guide and facilitate future researchers, network architects, and industry practitioners to pursue future 6G-SAGIN systems that are secure, scalable, and efficient.

### *10.1 Real World Deployment and Testbeds*

Most of the current research is either in the form of a simulation or theoretical, and there are currently limited real-life use cases [30] [31]. Simulation does not account for practical limitations like variable latency in satellite links, link failures, signal attenuation, mobility, and energy limitations of UAVs or HAPs, or environmental interference fully. The proposed research direction is to develop hybrid Blockchain -ZTA testbeds for SAGIN that have realistic components such as low Earth orbit (LEO) or medium Earth orbit (MEO) Satellites, HAPs/UAVs, Edge servers, Ground/cloud infrastructure. Through such prototypes, researchers can measure actual performance in terms of latency, throughput, energy consumption, reliability, and security under actual network dynamics. This will serve to validate the outcomes of the simulation-based results and to identify integration and interoperability problems (such as secure handover, cross-layer authentication delays), which can be addressed as required for deployment scenarios.

### *10.2 Scalability & Consensus Optimization*

Scalability is one of the challenges in the list of challenges. The classical PBFT (and RAFT) model, particularly the PoW, is not easily scalable in the presence of high density in the number of nodes, high mobility, and resource-constrained NTN nodes [22] [6].Research Directions:

- Lightweight and Adaptive Consensus: New forms of consensus mechanisms that are energy-aware, hierarchical/shared ledger, or shared ledger in the form of Directed Acyclic Graph (DAG) are to be developed to scale the resource-constrained NTNs [22].
- Hybrid Ledger Models: Local edge-ledgers have to be used to enable real-time operations while regularly synchronizing with the global ledger.
- Hierarchical blockchain architecture: Divide the network into units (e.g., each satellite constellation or each physical area on the ground), in each unit, there is a local blockchain implemented via sub-leaders, who regularly engage in a universal chain.

These optimizations can be used to support ultra-large-scale deployments, with thousands or tens of thousands of nodes, with minimal latency, energy, and consensus overhead.

### *10.3 Cross Domain & Multi Operator Security Frameworks*

NTNs and 6G SAGIN are multi-operation and cross-domain in nature. Satellite operators as well as terrestrial network providers, cloud/edge vendors, and IoT service providers may get involved. Existing ZTA or blockchain proposals often make assumptions on the existence of a single administrative domain [30] [31]. Proposed research:

- Standardized, interoperable policy framework: Implement blockchain as a decentralized identity, trust, and access control policy in the domain.
- In a broader sense, the security areas encompass exploitability: self-reliance, Federated identity should have the ability to roam between devices and operators without the integrity of the authentication and access records being compromised.
- Cross-domain compliance plan: Considerations include regulations, spectrum licensing, privacy laws, and differences in the level of trust required per region or operator.

Secures the possibility of communication and resource sharing among many administrative domains to enhance the viability of global 6G-SAGIN rollouts.

### *10.4 AI Enhanced Security & Distributed Trust Analytics*

AI and ML can substantially supplement blockchain/ZTA frameworks and allow adaptive, predictive, and context-aware security mechanisms. To illustrate, new articles suggest that Zero Trust could be used with AI-driven anomaly detection in 6G CPS and NTNs [31]. Research directions:

- Federated learning + blockchain + ZTA: Distributed nodes (edge, cloud, NTN) are used to train threat detection models without having access to raw data, blockchain makes model updates integrity and trustworthy.

- GNNs to learn dynamic threat modeling: Learn to predict abnormal flows or trust violations in real-time by modelling the space-air-ground communication graph.
- Automated policy configuration: ZTA policies are dynamically updated in real time based on security events (e.g., anomaly detection), and blockchain logs provide an auditing history in the form of an audio record.

Some challenges need to be addressed, such as synchronization across high-latency links, heterogeneous node capabilities, privacy of training data, and adversarial robustness of ML models.

### *10.5 Privacy Preserving & Quantum Resilient Cryptography*

The level of confidentiality in the solutions to global IoT, satellite imaging, and industry communications is required to be high since the information is sensitive, and the ability to mitigate future quantum threats is required. More cryptographic defenses, such as, but not limited to, homomorphic encryption, inner-product encryption, and postquantum algorithms, are implied [30] [32]. Research directions:

- Post Quantum Cryptography (PQC): Consider lattice-based key exchange, quantum-safe signatures, quantum-resistant key distribution, and blockchain, as well as ZTA.
- Privacy-conscious computation protocols: Integrated homomorphic encryption (or secure multi-party computation) protocols could be utilized as a type of sharing and computation of data securely between edge-cloud-NTN nodes without having access to raw data.
- Performance optimization: Further squeeze out of cryptographic schemes on resource-constrained devices (e.g., satellites, UAVs, and IoT) to get real-time secure communications.

Provides 6G systems with long-term security and privacy, i.e., protection against quantum attacks in the future and compliance with data-protection laws

### *10.6 Energy Efficient & Low Latency Security Protocols*

Critical factors that apply to NTN nodes, including satellites, UAVs, or HAPs, are resource constraints (energy, power, computational capacity) and are receptive to latency variations. Most of the current protocols do not optimize these constraints adequately. Proposed research:

- Adaptive security protocols: Dynamically adjust consensus participation, verification frequency, and logging based on node energy state, network load, and latency requirements.
- Hybrid on-chain/off-chain solutions: Heavy data, logs, or non-critical transactions can be handled off-chain or batched, while essential transactions remain on-chain — reducing communication overhead, energy consumption, and latency.
- Edge-centric verification modules: Verification and access control should be implemented at the HAP nodes to minimize the latency for delay-sensitive 6G/NTN applications (e.g., IoT control applications, satellite data relays).

Achieves an optimal balance between security, performance, and resource efficiency, which are vital for the sustainability of NTN.

### *10.7 Standardization, Benchmarking & Interoperability*

With the increase of research activities related to blockchain/ZTA in 6G, it is also desirable that standardization be considered to prevent the risk of fragmentation, as well as provide interoperability between different vendors, operators, and applications. Proposed research directions:

- Participate with standardization bodies such as 3GPP, ETSI, IEEE to specify security protocols, identity models, as well as compliance models to 6G-SAGIN.
- Creation of benchmark models and best tools of assessment (latency, throughput, energy usage, security detection rates, scalability) so that the proposals could be subject to a level of fair evaluation.
- Increase interoperable security stack promotion - blockchain, ZTA, cryptography, and AI modules should be able to be updated, replaced, or extended eventually.

Ensures uptake, neutrality between vendors, cross-domain interoperability, and long-term evolvability of secure 6G systems.

## 11. Conclusion

*11.1 Summary of Findings*

**• Blockchain-enabled Security in NTNs:** The most important features of the blockchain are decentralized trust, record of inevitable transactions, and auditability, which are important when it comes to multi-domain SAGIN networks [2]. Different versions of consensus mechanisms (PoW, PoS, PBFT, sharing) were investigated, and sharing and hierarchical ledgers were potential ways of making NTN deployments saleable. Nevertheless, blockchain has the challenges of latency, expensive computational energy consumption, specifically for UAVs, satellites, and edge nodes [22] [33].
• **ZTA of 6G Cloud-edge Networks:** ZTA has the policies of constant verification, micro-segmentation, and cross- domain access control [26]. Its usage will promote resistance to internal assault and cut down on the surface of the assault. Nevertheless, due to the dynamicity of SAGIN networks, cross-domain policy enforcement and distributed authentication overhead a problem that has to be resolved to make the networks usable.
**• Hybrid Blockchain:** ZTA Systems, there are benefits of using blockchain as a trust anchor in the frameworks of ZTA. It has the advantages of decentralized verification and continuous security policies [8] [1]. This cross-domain solution improves cross-domain trust management, auditability, and access control. However, challenges in latency and resource limitations still pose a major challenge, especially in multi-layered networks.
**• AI-Enhanced Security Mechanisms:** AI, federated learning, RL, and GNNs can be used to enhance the anomaly detection, threat prediction, and policy adaptation in 6G NTN [31] [30]. AI reduces false positives and increases security systems' response. Nevertheless, there are challenges with adversarial robustness, processing cost, model correctness, and data privacy.
• **Cryptographic and Privacy:** Observing Protocols The use of sophisticated cryptographic techniques, such as homomorphic encryption, inner product encryption, and quantum robust cryptography, might enhance safe cross-domain data access and reduce the risk of becoming a target of a quantum assault in the future [6] [34]. Although these protocols work well, their processing burden prevents real-time implementation in energy-constrained NTNs.
• **Quantitative Performance Analysis:** Performance analysis of the examined studies revealed trade-offs between operational efficiency and security. Throughput, latency, scalability, energy efficiency, and security efficacy were all synthesized parameters. Increased security may often be achieved by hybrid blockchain-ZTA solutions at the cost of increased latency and processing load [1] [22]. The advancements made in AI, which can facilitate both adaptive policy management and predictive security, partially address the restrictions.

*11.2 Value of the Review*

The state of the art in 6G NTN security is discussed in this study. To create a basis for how these advancements can be applied to ensure safe 6G communications infrastructures, it particularly deals with the gap between Blockchain and ZTA. More significantly, the review can be viewed as a diagnostic tool that reveals gaps in research that must be overcome in order to apply its findings. The biggest challenges identified in applying its findings are energy inefficiencies, lack of interoperability, and the imminent need to implement quantum-resistant encryption. It must be noted that, by highlighting these gaps, the article can be viewed as a roadmap to future research that will identify a thematic classification of hybrid solutions like scalable SAGIN architectures and AI-based security solutions. Finally, the analysis offers industry leaders and policymakers useful recommendations and standards guidelines. It recommends modifying the threats in order to give the systems adaptability to modular security architecture and lightweight procedures. The review will concur with such global standards as ETSI, and by offering standard bench- marking indicators to such metrics as latency, throughput, and energy consumption, it will become easier to compare and implement secure 6G technologies on a broad scale across the industry.

*11.3 Final Remarks*

In conclusion, it is noteworthy that the literature study highlights the importance of ZTA and blockchain in protecting the 6G NTN and offers the chance to employ AI and quantum-resistant encryption. Despite the innovative architecture and frameworks, there are still concerns about energy efficiency, real-world implementation, and benchmarking standards, among other things. The review summarizes all of the gaps and study directions of the studies, making it both scientific and useful. The action plan focuses on the practical implementation, scalability, standardization, and integration of AI, quantum-safe security, teamwork, and interdisciplinary workforce required to deliver effective, realistic, safe, and globally deployable 6G SAGIN networks. Finally, the review offers a source of further study that will enable scholars, industry players, and policymakers to develop robust, scalable, and dependable 6G infrastructures. The next generation of secure global connection is what lies ahead.

**Corresponding author**
Dr.Abdullah Albuali.
aabuali@kfu.edu.sa

**Acknowledgements**
The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT No. KFUXXXXXX]. The authors would like to sincerely thank the anonymous reviewers who contributed to guiding us scientifically to improve the quality of the paper.

**Funding**
No funding.

**Contributions**
All authors contributed to the development and completion of the entire manuscript.

**Ethics declarations**
This article does not contain any studies with human participants or animals performed by any of the authors.

**Consent for publication**
Not applicable.

**Competing interests**
All authors declare no competing interests.

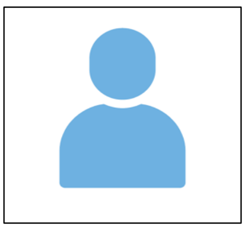
## References

[1] Y. Zhang, P. Zhang, M. Guizani, J. Zhang, J. Wang, H. Zhu, K. K. Igore-vich, and H. Shi, "Blockchain-based secure communication of internet of things in space–air–ground integrated network," Future Generation Computer Systems, vol. 158, pp. 391–399, 2024.https://doi.org/10.1016/j.future.2024.04.024
[2] W. Zhao, S. Yang, and X. Luo, "Blockchain-facilitated cybersecurity for ubiquitous internet of things with space–air–ground integrated networks: A survey," Sensors, vol. 25, no. 2, p. 383, 2025.https://doi.org/10.3390/s25020383
[3] S. Nie, J. Ren, R. Wu, P. Han, Z. Han, and W. Wan, "Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment," Sensors, vol. 25, no. 2, p. 550, 2025. https://doi.org/10.3390/s25020550
[4] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" Nature Electronics, vol. 3, no. 1, pp. 20–29, 2020.https://doi.org/10.1038/s41928-019-0355-6
[5] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," IEEE network, vol. 35, no. 2, pp. 244–251, 2020.https://doi.org/10.1109/mnet.011.2000493
[6] H. Cui, J. Zhang, Y. Geng, Z. Xiao, T. Sun, N. Zhang, J. Liu, Q. Wu, and X. Cao, "Space-air-ground integrated network (sagin) for 6g: Requirements, architecture and challenges," China Communications, vol. 19, no. 2, pp. 90–108, 2022.https://doi.org/10.23919/jcc.2022.02.008
[7] M. Satyanarayanan, "The emergence of edge computing," Computer, vol. 50, no. 1, pp. 30–39, 2017.https://doi.org/10.1109/mc.2017.9
[8] Y. Liu, S. Peng, M. Zhang, S. Shi, and J. Fu, "Towards secure and efficient integration of blockchain and 6g networks," Plos one, vol. 19, no. 4, p. e0302052, 2024.https://doi.org/10.1371/journal.pone.0302052
[9] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas et al., "On the road to 6g: Visions, requirements, key technologies, and testbeds," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 905–974, 2023.https://doi.org/10.1109/comst.2023.3249835
[10] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," IEEE vehicular technology magazine, vol. 14, no. 3, pp. 28–41, 2019.https://doi.org/10.1109/mvt.2019.2921208
[11] W. Saad, M. Bennis, and M. Chen, "A vision of 6g wireless systems: Applications, trends, technologies, and open research problems," IEEE network, vol. 34, no. 3, pp. 134–142, 2019. https://doi.org/10.1109/mnet.001.1900287
[12] I. F. Akyildiz, C. Han, Z. Hu, S. Nie, and J. M. Jornet, "Terahertz band communication: An old problem revisited and research directions for the next decade," IEEE Transactions on Communications, vol. 70, no. 6, pp. 4250–4285, 2022.https://doi.org/10.1109/tcomm.2022.3171800
[13] H. Chen, H. Sarieddeen, T. Ballal, H. Wymeersch, M.-S. Alouini, and

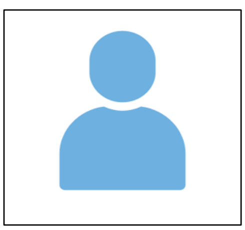
T. Y. Al-Naffouri, “A tutorial on terahertz-band localization for 6g communication systems,” IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1780–1815, 2022.https://doi.org/10.1109/comst.2022.3178209
[14] M. Ahmed, A. Wahid, W. U. Khan, F. Khan, A. Ihsan, Z. Ali, K. M. Rabie, T. Shongwe, and Z. Han, “A survey on ris advances in terahertz communications: Emerging paradigms and research frontiers,” IEEE Access, vol. 12, pp. 173 867–173 901, 2024.https://doi.org/10.1109/access.2024.3482564
[15] M. N. A. Siddiky, M. E. Rahman, M. S. Uzzal, and H. D. Kabir, “A comprehensive exploration of 6g wireless communication technologies,” Computers, vol. 14, no. 1, p. 15, 2025.https://doi.org/10.3390/computers14010015
[16] K. Meng, C. Masouros, K.-K. Wong, A. P. Petropulu, and L. Hanzo, “Integrated sensing and communication meets smart propagation engineering: Opportunities and challenges,” IEEE Network, 2025.https://doi.org/10.1109/mnet.2025.3527130
[17] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, “Enabling joint communication and radar sensing in mobile networks—a survey,” IEEE Communications Surveys & Tutorials, vol. 24, no. 1, pp. 306–345, 2021.https://doi.org/10.1109/comst.2021.3122519
[18] E. Shtaiwi, A. Abdelhadi, H. Li, Z. Han, and H. V. Poor, “Orthogonal time frequency space for integrated sensing and communication: A survey,” arXiv preprint arXiv:2402.09637, 2024. https://doi.org/10.48550/arXiv.2402.09637
[19] S. N. Sur, A. K. Singh, H. Q. Tran, P. Vishwakarma, A. L. Imoize, and C.-T. Li, “A state-of-the-art survey on irs-noma for integrated sensing and communication,” IEEE Access, 2024.https://doi.org/10.1109/access.2024.3512998
[20] A. H. Alaraj, “Advancing cloud adoption in the saudi public sector: Challenges, global insights, and strategic policy recommendations,” ESI Preprints (European Scientific Journal, ESJ), vol. 41, pp. 627–627, 2025. https://doi.org/10.19044/esipreprint.5.2025.p627
[21] R. B. Alzahrani, “An overview of ai data protection in the context of saudi arabia,” International Journal for Scientific Research, vol. 3, no. 3, pp. 199–218, 2024.https://doi.org/10.59992/ijsr.2024.v3n3p8
[22] H. Luo, X. Yang, H. Yu, G. Sun, B. Lei, and M. Guizani, “Performance analysis and comparison of nonideal wireless pbft and raft consensus networks in 6g communications,” IEEE Internet of Things Journal, vol. 11, no. 6, pp. 9752–9765, 2023.https://doi.org/10.1109/jiot.2023.3323492
[23] F. A. Dicandia, N. J. Fonseca, M. Bacco, S. Mugnaini, and S. Genovesi, “Space-air-ground integrated 6g wireless communication networks: A review of antenna technologies and application scenarios,” Sensors, vol. 22, no. 9, p. 3136, 2022.https://doi.org/10.3390/s22093136
[24] F. Wang, S. Zhang, H. Yang, and T. Q. Quek, “Non-terrestrial networking for 6g: Evolution, opportunities, and future directions,” Engineering, 2025. https://doi.org/10.1016/j.eng.2025.05.013
[25] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, “Security requirements and challenges of 6g technologies and applications,” Sensors, vol. 22, no. 5, p. 1969, 2022.https://doi.org/10.3390/s22051969
[26] Y. Liu, X. Xing, Z. Tong, X. Lin, J. Chen, Z. Guan, Q. Wu, and W. Susilo, “Secure and scalable cross-domain data sharing in zero-trust cloud-edge-end environment based on sharding blockchain,” IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 2603–2618, 2023.https://doi.org/10.1109/tdsc.2023.3313799
[27] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, “Privacy-preserving blockchain-based federated learning for iot devices,” IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1817–1829, 2020. https://doi.org/10.1109/jiot.2020.3017377
[28] R. Radu, “Steering the governance of artificial intelligence: national strategies in perspective,” Policy and society, vol. 40, no. 2, pp. 178–193, 2021.https://doi.org/10.1080/14494035.2021.1929728
[29] X. Chen, W. Feng, N. Ge, and Y. Zhang, “Zero trust architecture for 6g security,” IEEE network, vol. 38, no. 4, pp. 224–232, 2023.https://doi.org/10.1109/mnet.2023.3326356
[30] A. Hussain, S. Li, T. Hussain, R. W. Attar, A. Alhomoud, R. Alsagri, and A. A. Alzubi, “Blockchain-enabled zero trust-based secure and energy efficient scheme for 6g-enabled uasns,” Journal of Cloud Computing, vol. 14, no. 1, p. 21, 2025.https://doi.org/10.1186/s13677-025-00744-x
[31] H. Sedjelmaci, K. Tourki, and N. Ansari, “Enabling 6g security: The synergy of zero trust architecture and artificial intelligence,” IEEE Network, vol. 38, no. 3, pp. 171–177, 2023. https://doi.org/10.1109/mnet.2023.3326003
[32] T. N. Turnip, B. Andersen, and C. Vargas-Rosales, “Towards 6g authentication and key agreement protocol: A survey on hybrid post quantum cryptography,” IEEE Communications Surveys & Tutorials, 2025. https://doi.org/10.1109/comst.2025.3567439
[33] A. Ali and I. Khan, “Skytrust: Blockchain-enhanced uav security for ntns with dynamic trust and energy-aware consensus,” arXiv preprint arXiv:2508.18735, 2025.https://doi.org/10.22541/au.175559616.64842559/v1
[34] F. Raheman, “From standard policy-based zero trust to absolute zero trust (azt): a quantum leap to q-day security,” Journal of Computer and Communications, vol. 12, no. 3, pp. 252–282, 2024.https://doi.org/10.4236/jcc.2024.123016
[35] A. Ali, “Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks,” STAP Journal of Security Risk Management, vol. 2024, no. 1, pp. 45–56, 2024, doi: 10.63180/jsrm.thestap.2024.1.3.
[36] Chandak, A., & Chandak, P. (2026). Blockchain technology in health care an extensive scoping review of the existing applications, challenges, and future directions. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[37] S. R. Addula, S. Norozpour, and M. Amin, “Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing,” Jordanian Journal of Informatics and Computing, vol. 2025, no. 1, pp. 38–48, 2025, doi: 10.63180/jjic.thestap.2025.1.5.
[38] D. Abu Laila, “Responsive Machine Learning Framework and Lightweight Utensil of Prevention of Evasion Attacks in the IoT-Based IDS,” STAP Journal of Security Risk Management, vol. 2025, no. 1, pp. 59–70, 2025, doi: 10.63180/jsrm.thestap.2025.1.3.
[39] Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A Secure and Scalable IoT Home Automation Architecture with Web and Biometric Control. International Journal of Cybersecurity Engineering and Innovation, 2026(1).

[40] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering," Jordanian Journal of Informatics and Computing, vol. 2025, no. 1, pp. 27–36, 2025. doi: 10.63180/jjic.thestap.2025.1.4.
[41] D. Abu Laila, M. Aljawarneh, Q. Al-Na'amneh, and R. Bin Sulaiman, "Optimizing intrusion detection systems through benchmarking of ensemble classifiers on diverse network attacks," STAP Journal of Security Risk Management, vol. 2025, no. 1, pp. 71–84, 2025. doi: 10.63180/jsrm.thestap.2025.1.4.
[42] Alsahaim, S., Almaiah, M. A., & Sulaiman, R. B. (2023). Security Threats in Mobile Phones: Challenges, Countermeasures, and the Importance of User Awareness. International Journal of Cybersecurity Engineering and Innovation, 2023(1).
[43] K. Audah Kareem and M. A. Al-Shareeda, "A Low-Complexity Li-Fi Communication Framework for Short-Range Text Transmission," Jordanian Journal of Informatics and Computing, vol. 2026, no. 1, pp. 15–24, 2026, doi: 10.63180/jjic.thestap.2026.1.2.
[44] Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights. International Journal of Cybersecurity Engineering and Innovation, 2026(1).
[45] Q. Al-Na'amneh, M. Aljawarneh, A. S. Alhazaimeh, R. Hazaymih, and S. M. Shah, "Securing trust: Rule-based defense against on/off and collusion attacks in cloud environments," STAP Journal of Security Risk Management, vol. 2025, no. 1, pp. 85–114, 2025. doi: 10.63180/jsrm.thestap.2025.1.5.

## Biographies



**HUDA O. ALDAWGHAN** received a bachelor's degree in computer networks and communications in 2023 and is currently pursuing a master's degree in cybersecurity at King Faisal University. She has a strong interest in various areas, including machine learning, artificial intelligence, cybersecurity, Internet of Things, blockchain technology, cloud computing, and network forensics. 225002215@student.kfu.edu.sa



**ASHWA M. ALOTAIBI** received a bachelor's degree in computer networks and communications and is currently pursuing a master's degree in Cybersecurity at King Faisal University. Her interests focus on strengthening secure digital infrastructures, with particular attention to cyber defense strategies, intelligent threat detection, and modern network protection techniques. She is also engaged in exploring secure IoT environments, data protection approaches, and the integration of emerging technologies to improve system resilience and operational security. 225000514@student.kfu.edu.sa

**ABDULLAH ALBUALI** (Member, IEEE) received the B.S. degree in computer science from King Faisal University, Saudi Arabia, in 2009, and the M.S. and Ph.D. degrees in computer science, with specialization in security and networking, from Southern Illinois University, USA, in 2014 and 2021, respectively. He is currently an Assistant Professor with the College of Computer Science and Information Technology, King Faisal University. His research interests include zero trust architecture, AI-enabled cybersecurity, cloud and edge computing security, Internet of Things (IoT) systems, drone and autonomous networks, digital forensics, volunteer and distributed computing, and blockchain-based security. Aabuali@kfu.edu.sa