EJSIT
European Journal of Science, Innovation and Technology
ISSN: 2786-4936
www.ejsit-journal.com
Volume 5 | Number 5 | 2025

Satellite-Integrated IoT for Underserved Regions: Design, Security, and Implementation Challenges

Mahmoud Matar[1] and Khaled Matar[2]
[1]Shabakkat Cellular Company, Saudi Arabia
[2]Civil Engineering and Geomatics,
Cape Peninsula University of Technology, South Africa

ABSTRACT

Satellite communications combined with IoT promise to bridge the digital divide in remote and underserved regions, supporting applications from environmental monitoring to disaster response. This review synthesizes recent advances in satellite-integrated IoT (SIoT), comparing architectures (direct vs indirect access), enabling LPWAN technologies (e.g., NB-IoT, LoRaWAN), and orbital options (LEO vs GEO). It also examines design trade-offs (latency, Doppler, energy, massive access), identifies principal security threats (jamming, spoofing, key management, device tampering), and surveys practical implementation constraints (cost, regulation, maintenance). Finally, the paper identifies open research issues and outlines future directions for achieving scalable, secure, and high-performance satellite-IoT ecosystems in remote and rural environments.

Keyword: Satellite-Integrated IoT Networks, Satellite-Integrated IoT Network Design, IoT and Satellite Network Integration, Connectivity of Remote and Underserved Regions, IoT Security, System Design Challenges

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative paradigm enabling billions of interconnected devices to sense, process, and exchange information across domains such as smart cities, healthcare, logistics, and environmental monitoring (Atzori, Iera, & Morabito, 2010; Gubbi et al., 2013). However, despite rapid progress in terrestrial networks, connectivity remains highly uneven, particularly in remote and underserved regions where cellular and broadband infrastructure is sparse, economically unfeasible, or technically challenging to deploy (World Bank, 2016; ITU, 2023). This digital divide limits the reach of IoT-enabled services and hinders sustainable development goals in areas such as precision agriculture, disaster response, and wildlife monitoring (Kumar & Choudhary, 2024; Singh & Patel, 2022)

Satellite communication provides a promising solution to extend IoT coverage beyond terrestrial limitations (Clazzer et al., 2022; Centenaro et al., 2016). With the advent of low Earth orbit (LEO) mega-constellations, standardized non-terrestrial networks (NTNs), and lightweight low-power wide-area network (LPWAN) protocols such as NB-IoT and LoRaWAN, satellite-integrated IoT (SIoT) systems are becoming technically and economically viable (3GPP, 2022; LoRa Alliance, 2023). These systems promise global coverage, resilience against terrestrial outages, and support for delay-tolerant applications. Nevertheless, the integration of IoT with satellites raises unique challenges, including intermittent coverage due to satellite mobility, Doppler effects, limited device energy budgets, spectrum regulation, and end-to-end security under constrained resources (ENISA, 2021; GSMA, 2022).

Problem Statement. While prior research has investigated IoT protocols, satellite architectures, or NTN standards individually (Li & Zhang, 2021; Chen et al., 2020), a comprehensive synthesis of design trade-offs, security risks, and implementation challenges for satellite-integrated IoT remains limited. The field is fragmented across telecommunications, networking, and aerospace communities, with inconsistent terminology and scattered empirical evidence. Without a consolidated review, researchers and practitioners face difficulties identifying open research gaps, evaluating competing approaches, and understanding practical deployment barriers.

To address this gap, this paper makes the following contributions:

- Provides a structured taxonomy of SIoT architectures and enabling technologies, including direct-to-satellite and relay-assisted models.
- Surveys key security threats and lightweight countermeasures relevant to constrained SIoT deployments.
- Analyses practical implementation challenges such as spectrum regulation, device maintenance, and cost constraints in remote regions.
- Identifies critical research gaps and outlines a roadmap for future work to support robust and scalable SIoT systems.

2. RELATED WORK

The integration of satellite communication and IoT has been widely studied as a solution to bridge connectivity gaps in remote and underserved regions. This section synthesizes existing research, focusing on architectural approaches, security considerations, and implementation challenges.

2.1 Architectural and Design Approaches

Research on SIoT differentiates two high-level architectural paradigms: direct-to-satellite (DtS) access, where end devices communicate directly with a satellite payload, and relay/ground-assisted models, where local gateways (terrestrial or aerial) aggregate device traffic and forward it to space/ground backhaul (Centenaro et al., 2016; Clazzer et al., 2022). DtS enables the simplest footprint and widest coverage for truly remote devices but introduces severe constraints (visibility windows, Doppler shift, limited link budget, and complex multiple-access problems). Relay models relax radio constraints at the cost of additional local infrastructure and operational complexity; they are attractive where light terrestrial infrastructure or community gateways are feasible (LoRa Alliance, 2023). Several survey papers and system proposals contextualize these architectures and compare their trade-offs (Atzori, Iera, & Morabito, 2010; Gubbi et al., 2013). However, the literature remains fragmented: many studies focus on a single architecture or technology, and few present systematic cross-architecture comparisons under common performance metrics (3GPP, 2022; GSMA, 2022).

2.2 LPWAN Protocols and Their Satellite Adaptation

A central thread in the literature considers how LPWAN technologies principally NB-IoT, LTE-M, LoRaWAN, and Sigfox map to satellite channels. NB-IoT and LTE-M are designed for licensed spectrum and benefit from cellular control-plane features (paging, mobility support, secure SIM-based credentials), making them a natural fit for operator-managed NTN deployments (3GPP, 2021–2023). LoRaWAN and Sigfox, by contrast, operate in unlicensed bands with low-power ALOHA-like uplink access, which raises collision and duty-cycle concerns when stretched over wide footprints or long satellite visibility intervals (Centenaro et al., 2016; LoRa Alliance, 2023). Recent experimental and analytical studies investigate adaptations such as extended preambles, frequency hopping, and modified MAC timers to tolerate Doppler and intermittent connectivity (Clazzer et al., 2022; Raza et al., 2017). Nevertheless, there is limited consensus about which protocol is optimal for which use case:

choice often depends on regulatory constraints, business model (operator vs private network), and application latency/throughput needs (GSMA, 2022).

2.3 Non-Terrestrial Network (NTN) Standards and Regulatory Context

Standardization bodies and industry groups have recently focused on enabling IoT over NTNs. 3GPP has produced technical specifications and study items addressing NTN support for cellular IoT (e.g., NB-IoT over satellite, timing/Doppler compensation techniques), while industry alliances (GSMA, LoRa Alliance) have published deployment guidelines and whitepapers for satellite-backed IoT (3GPP, 2021; GSMA, 2022; LoRa Alliance, 2023). Regulatory issues spectrum allocation, cross-border licensing, and compliance with regional ISM band rules appear frequently in the literature as practical bottlenecks for global deployments (ITU, 2022). Several authors emphasize that successful SIoT rollouts require harmonized standards and coordination between satellite operators, MNOs, and national regulators (Clazzer et al., 2022; GSMA, 2022).

2.4 Security and Reliability Considerations

Security research specific to SIoT has surfaced a set of recurring concerns: secure key management and provisioning for devices with constrained interfaces; eavesdropping and confidentiality over wide-area satellite links; denial-of-service and jamming threats that exploit the broadcast nature of satellite channels; and secure OTA updates and lifecycle management for devices in inaccessible locations (ENISA, 2021; GSMA, 2022). Compared with terrestrial IoT, SIoT magnifies constraints (longer link latencies, intermittent connectivity, and higher cost per byte), which complicates straightforward adoption of heavyweight security protocols. The literature proposes several mitigations lightweight authenticated encryption (e.g., OSCORE-style approaches), use of secure elements and hardware root-of-trust, and diversity/anti-jamming techniques but practical evaluations at scale are sparse (ENISA, 2021; Clazzer et al., 2022). Crucially, few works present an end-to-end SIoT threat model that spans device, satellite payload, ground station, and backend services; this gap limits the ability to compare security solutions systematically.

2.5 Implementation Challenges

A smaller but growing body of empirical work reports prototypes and field trials that evaluate DtS and relay approaches. These studies typically measure link budget feasibility, packet delivery under real Doppler/visibility profiles, and battery lifetime under different duty cycles (Centenaro et al., 2016; Clazzer et al., 2022). Results show that DtS is feasible for sparse, small-payload telemetry (e.g., environmental sensors) with conservative duty cycles, while more frequent or high-throughput use cases still favour gateway-assisted or hybrid models. Yet most experimental studies are limited in scale (tens to low hundreds of devices) and are often tied to a single satellite geometry or vendor testbed making broad generalization difficult. The state-of-the-art lacks large-scale comparative trials across orbital regimes (LEO vs MEO vs GEO) and across LPWAN candidates under identical test conditions.

3. RESEARCH GAPS IN SATELLITE-INTEGRATED IOT

Despite rapid advances in IoT connectivity and the growing interest in satellite integration, the current body of literature remains fragmented and incomplete. Studies have provided valuable insights into architectural designs, protocol adaptations, and emerging standards; however, these works often address individual challenges in isolation and lack a holistic, end-to-end perspective on design, security, and practical implementation.

First, comparative evaluations of direct-to-satellite versus gateway-assisted architectures remain sparse, with limited empirical data from large-scale trials. Most existing results are either simulation-based or tied to vendor-specific testbeds, restricting generalizability. Similarly, while NB-IoT, LoRaWAN, and LTE-M have been proposed for non-terrestrial networks, systematic performance comparisons under real satellite conditions (e.g., Doppler shift, intermittent visibility, energy budget constraints) are lacking.

Second, security and privacy issues in SIoT remain under-explored. Although the literature mentions common threats such as jamming, spoofing, and device tampering, few studies propose lightweight, scalable frameworks for secure key management, authentication, or secure over-the-air (OTA) updates in constrained devices. End-to-end SIoT threat models that include devices, satellites, ground stations, and back-end services are also rare.

Finally, implementation and sustainability challenges including cost models, regulatory compliance, and device lifecycle management in inaccessible regions receive limited attention. Few works examine the long-term feasibility of large-scale deployments, energy-harvesting strategies, or maintenance-free operation for devices expected to last more than a decade in harsh environments.

To make these knowledge gaps explicit, Table 1 summarizes the main research gaps identified from the literature and suggests corresponding research opportunities.

Table 1: Research gaps in satellite-integrated IoT and future opportunities

Research Area	Existing Focus in Literature	Identified Gap	Future Research Opportunities
System Architectures	Individual studies of direct-to-satellite (DtS) or gateway-assisted models (Centenaro et al., 2016; Clazzer et al., 2022)	Lack of comparative studies across architectures and orbital regimes (LEO, MEO, GEO)	Develop unified frameworks and large-scale trials comparing DtS vs gateway-assisted models under real deployment conditions
LPWAN Protocol Adaptation	Analysis of NB-IoT, LTE-M, and LoRaWAN for satellite channels (3GPP, 2022; LoRa Alliance, 2023)	Limited cross-protocol benchmarking under Doppler, intermittent coverage, and spectrum regulations	Conduct empirical evaluations and standardized benchmarks for multiple LPWAN technologies over satellite links
Standards & Regulation	3GPP NTN specifications, GSMA/LoRa guidelines (3GPP, 2022; GSMA, 2022)	Gaps in harmonized spectrum policy and interoperability frameworks	Research into cross-border spectrum harmonization, global roaming, and integration of private SIoT networks with MNO-led NTN systems
Security & Privacy	General threats identified (jamming, spoofing, device tampering) (ENISA, 2021)	Lack of lightweight end-to-end security frameworks and SIoT-specific threat models	Design scalable security architectures: lightweight crypto (OSCORE), secure key lifecycle, trusted hardware, anti-jamming/diversity strategies
Implementation & Operations	Prototype deployments and small-scale trials (Centenaro et al., 2016)	Lack of long-term sustainability studies (energy, maintenance, cost models)	Explore energy-harvesting, predictive maintenance, and business models for decade-long SIoT deployments in remote environments
Performance Evaluation	Limited simulations or vendor-specific trials (Clazzer et al., 2022)	Few large-scale, real-world comparative trials across constellations and protocols	Establish open-access testbeds and collaborative measurement campaigns

4. SATELLITE-INTEGRATED IOT NETWORK ARCHITECTURE

The exclusive attributes of satellite communication networks in the context of the new space era characterized by low-cost launches and the rapid deployment of nanosatellites or CubeSats enable architectural alternatives for IoT networks with a higher degree of scalability and flexibility (Fraire et al., 2019; Chiti et al., 2019). Satellites can be deployed in Geosynchronous Orbits (GEO), where they exhibit a rotation period synchronized with the Earth's rotation. These satellites appear stationary to an observer on Earth and provide uninterrupted network connectivity for a specific region from an altitude of approximately 35,786 km. Conversely, Low Earth Orbit (LEO) satellites operate at altitudes between 160 km and 1,000 km, moving at speeds of about 7 km/s. LEO satellites are designed to provide intermediate and continuous connectivity through frequent revisits, especially when deployed in constellations (Fraire et al., 2019). However, multiple satellites are required to ensure global coverage. Figure 1 illustrates the orbital differences between GEO and LEO satellites.

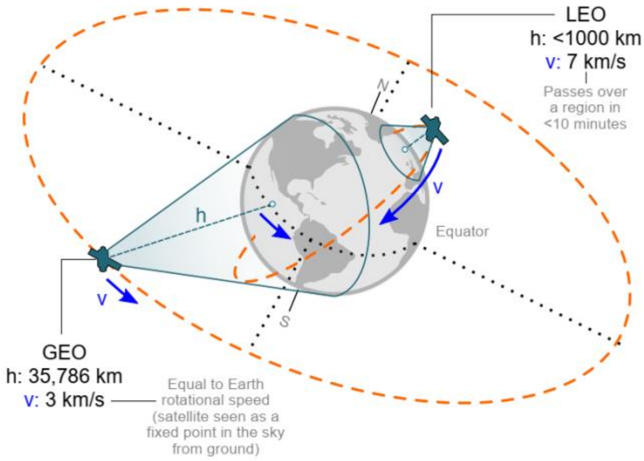

Figure 1: LEO and GEO Orbit Illustration (adapted from Fraire et al., 2022)

The integration of Internet of Things (IoT) devices with these LEO and GEO Satellites, the opportunities for connectivity across the globe especially for remote distanced and yet underserved geographical locations became possible. The revolutionary advancement and innovation in telecommunication ad satellite technologies allow to establish direct communication between Internet of Things (IoT) devices ad satellites using the same technologies used by the terrestrial IoT networks (Fraire, Céspedes, & Accettura, 2019). The most important advancements include LoRa/LoRaWAN and NBIoT for development of long range communication with low power energy consumption up to 18mA and @7dBm.

Satellite-integrated IoT networks are primarily designed to address the universal coverage challenge required for IoT connectivity worldwide, especially in areas lacking terrestrial infrastructure. To achieve this, groups of satellites operate collaboratively as constellations, ensuring continuous communication and resilience against single-satellite failures (Chiti et al., 2019). Unlike short-range wireless technologies such as Bluetooth, Zigbee, and Wi-Fi, satellite-integrated IoT networks overcome coverage limitations and can manage multiple simultaneous connections. Figure 2 presents a reference architecture for satellite-integrated IoT networks, illustrating two deployment scenarios: Indirect and Direct IoT communication, discussed in detail below.

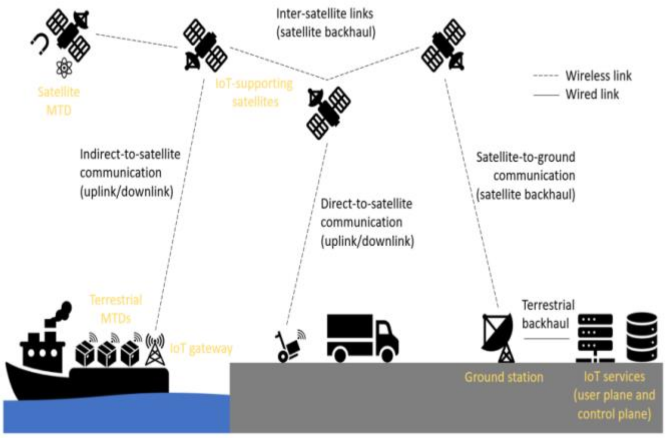

Figure 1: Reference Architecture for Satellite-Integrated IoT Network (adapted from Centenaro et al., 2021)

In above mentioned reference architecture there are two different Satellite-Integrated IoT deployments indirect and direct IoT communication scenarios are presented which are discussed in detail in this section. It is important to view both deployment scenarios as interconnected networks associated with same global network instead of individual deployment scenarios.

4.1 Indirect to Satellite IoT Communication

In rural areas where a high density concentration of IoT devices ca be found justifies the positioning of dedicated ground IoT gateways for serving to connected IoT devices. However, the places where cellular network coverage is not present or laying of Optical Fiber cable is not possible due to terrain and local conditions and availability of communication infrastructure is might not possible to transport data from gateway to core data networks, in such cases the deployment of satellite communication networks are highly suitable solutions for serving as backhaul media for network connectivity using these IoT gateways placed on the ground surface (Fraire et al., 2022). The GEO Satellites kept their position stable in space are considered perfectly apposite for transporting the data from ground gateways using the fixed high-gain antennas. The suitable power source like electric grid, solar or wind turbines make them capable for establishing long range data links with GEO orbit satellites. The end user IoT devices connect with satellite through the deployed IoT gateways instead of direct connection, so such deployment known as the indirect-satellite IoT communication. The communication protocols in indirect-satellite IoT integrated networks are segregated depending on the ground and spare domain, for terrestrial IoT protocols used such as LoRa/LoRaWAN, NB-IoT are used similar deployed between end-devices and IoT Gateways making a few modifications to manage high network delay occurred due to satellite links between IoT gateways and network server. The currently available space-specific technologies and protocols such as CCSDS Protocols can be implement over links between IoT gateways ad satellite (Ground Control, 2023; Mannoni et al., 2021).

4.2 Direct to Satellite IoT Communication

The deployment of IoT gateways on ground is not possible, justified or even considered interference for applications required to function in remote and less accessible regions like hilly areas, seas, and poles with lack of communication infrastructure. In such conditions, IoT devices are directly connected with IoT gateway hosted on the Satellite system. The GEO satellite links are not considered appropriate due to large range and high data transmission delays, while the LEO orbit satellites emerge for addressing such situations due to rotation in

1000Km in the Earth orbit. The communication channels with LEO satellites can be established to attain the margins requisite by the terrestrial IoT protocols even using IoT devices equipped with low-cost antennas. The most recent in-orbit satellite deployments like ThingSat, Sateliot, FossaSat, LacunaSat also endorse the similar methodology (Colavolpe et al., 2019). Furthermore, the low-cost and contemporary Nano-Satellites (LEO) platforms can be utilized for compliance the reduced power and volume IoT gateways requirements.

The major concern associated with direct-to-satellite communication scenario is high speed rotations of IoT gateways hosted on LEO satellites with high speed varying channels over predictable orbit trajectory. More precisely, a Nano-Satellite takes 3 to 10 minutes to pass through a particular region for a perfectly zenithal pass and horizon correspondingly and for this specified time slot the communication channel conditions vary radically from more than 2000Km to real satellite altitude. The Nano-Satellites (LEO) rotates very fast over the coverage regions with a constant speed, so LEO satellites are deployed in constellations for ensuring the continuously availability of services. The LEO satellites are intent to prevent service interruptions for IoT devices on earth surface through revisit rate improvements because when one satellite sets, the other rises. In dense constellation scenarios, if a LEO satellite hides in horizon, another performs job for continuous provisioning of services to IoT devices on earth surface.

Another communication scenario discussed in reference architecture is Inter-Satellite Links (ISL) which permits LEO satellites constellation comprised of hundreds on Nano-Satellites for coordinating and relaying the application data between ground stations connected with the core network. Due to the delay-tolerate nature of IoT applications, this enables supposed Sparse Constellations attributes by massive coverage gaps, and opportunistic Inter-Satellite communication links, such irregular connectivity considerably minimize the satellite fleet size requirements up to dozen of LEO satellite links (Fraire et al., 2020). For such scenarios, new challenges prompt like data should be stored temporarily in satellite or IoT devices till the availability of the satellite link. Another communication scenario exists that is device-to-device communication (Kim & Song, 2018) used to extend the IoT ecosystem coverage for underground or under-roof locations by the help of node mobility and deployment of repeaters.

4.3 Satellite-Integrate IoT Enabling Technologies

There are various communication technologies and protocols which enable the integration of IoT and satellite communication in terrestrial and space networks. In the section the in-depth insight of these technologies presented.

4.3.1 Satellite Based Communication Technologies

Conventionally, the satellite communication was used for reliable transportation of telecommands (TC) to satellite and delivery of spacecraft telemetry (TM) to earth stations. In early 80s, the Consultative Committee for Space Data Systems (CCSDS) developed and introduced low data rate TM/TC protocols for this conventional satellite communication. The S-Band is one of the most used and familiar TM/TC band supports to a limited Mbps data rates that also allows for carrier-based ranging and tracking operations. For transportation of higher data rate like hundreds of Mbps (Gbps) for contemporary data-demanding mission larger bandwidth supporting X-Band and higher bands are being used. The CCSDS point-to-point (P2P) links were also leverage for Inter-Satellite Links (ISL) applications and for the power consumption and high-throughput volume X-band subsystems are stereotypically earmarked for satellite platforms tens of kilograms. Other conventional satellite communication applications include fixed satellite services, provisioning of a global backbone for Internet and Telephony, television and radio broadcasting services, mobile satellite services for maritime and aviation industries, and remote sensing and disaster management services during infrastructure failures due to the wide coverage and resilience features of satellite communication (Duran et al., 2024). Another key application of satellite communication also includes the use for navigation systems such as GPS.

The satellite communication protocols the Proxmity-1 and the most recent protocol Unified Space Data Link Protocol (USLP) allows communication over UHF or S-band for connectivity of spacecraft in orbit though offered low data rates up to few Kbps due to long distance. In context of space, multi-user application specific low power and data volume supportive satellite communication technologies already available, however the Internet of Things (IoT) prominently was not on the list. The protocols for device-to-satellite communication (Fraire, Iova, & Valois, 2022), Argos used for conveying environmental data like telemetry and tele-control to serve weather stations and buoys, Satellite Automatic Identification System (S-AIS) and Satellite Automatic Dependent Surveillance-Broadcast (ADS-B) for vessels and aircraft worldwide data tracking can be used.

4.3.2 Integrated Internet of Things (IoT) Technologies

An efficient and effective Satellite-Integrated IoT communication network can be obtained if terrestrial IoT ported to space domain instead of supplanting terrestrial IoT by the aforesaid space protocols. There are following reasons behind this strategy:

- Satellite-Integrated IoT can be more profitable by taking advantage of mass production and lower costs already achieved by terrestrial IoT particularly for end devices.
- Satellite-Integrated IoT will take advantage from a massive ecosystem and community enhancing the achievable performance with minimum resources
- Satellite-Integrated IoT will flawlessly incorporate with currently available terrestrial satellite deployments.

It is also claimed that thrived satellite-integrated IoT will only successful if it will take advantages from technological enhancements and scalable economies which are already empowered with LPWAN in terrestrial IoT and further connectivity is extended to remote distanced and underserved regions with the help of satellite IoT enabled gateways. In section below IoT technologies (LoRaWAN and NB-IoT) which can contribute and play an important role for integration of IoT with satellite are discussed. Following figure 3 shows the comparison of NB-IoT and LoRa/LoRaWAN technologies.

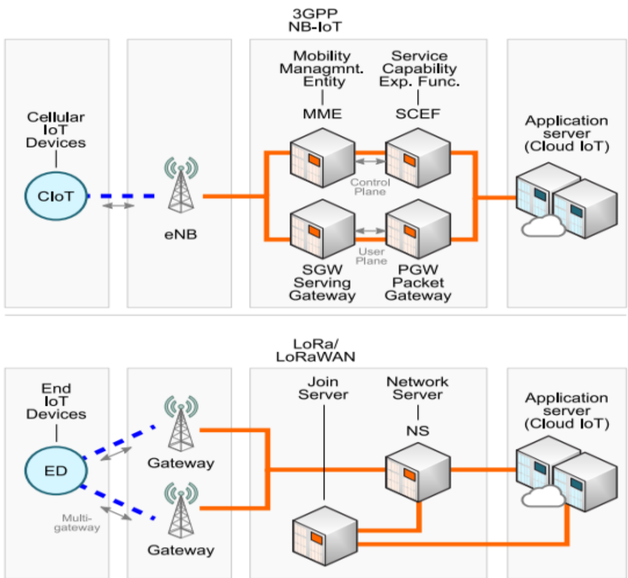

Figure 2: Comparative architectures of NB-IoT and LoRa/LoRaWAN for satellite IoT (adapted from Fraire et al., 2022)

From several available terrestrial IoT technologies, the Low Power Wide Area Networks (LPWANs) can be considered as the best and suitable option for merging space-terrestrial IoT technologies across the globe and particularly in area with lack of communication infrastructure. The LPWAN allows low volume data transportation over long distance with utilization of very low energy consumption for the end-user IoT devices. LPWANs uses the network architecture where in the entire intelligence offered by a centrally located server that allows the development of low cost end-user IoT devices. The Narrow-Band Internet of Things (NB-IoT) developed by the 3GPP (Sinha, Wei, & Hwang, 2017) and LoRa/LoRaWAN (LoRa Radio combined with LoRaWAN protocol) technology are mostly contributed technologies which can contribute for design and deployment of Satellite-Integrated IoT for provisioning of services in remote distanced and underserved regions. Another research work endorses the LoRa/LoRaWAN and NB-IoT integration viability with direct-to-satellite links (Colavolpe et al., 2019). The major difference between both technologies is that when using the NB-IoT an IoT device is considered associated and synchronized with a Narrowband, while the LoRaWAN uses a decoupled Aloha-based Medium Access protocol for connecting IoT devices. The NB-IoT technology depends on a connected mode using the radio resource allocation mechanism and leverage a Quality of Service (QoS) Management, the core network facilitates for ensuring the Quality of Services (QoS) requirements which are pre-requisite for some applications. These enhanced features cost more multifaceted radio access negotiations and core management elements. Furthermore, NB-IoT being a mobile network technology utilized licensed frequency bands which are acquired by the Telecommunication service provide through licensing. Conversely, the LoRaWAN technology relies on non-connected mode with ease of deployment and low complexity that is vital for some users instead of limitation of strict latency or reliability preferences. The LoRaWAN utilizes unlicensed ISM frequency bands shared and adopted by various wireless communication technologies (Centenaro et al., 2021).

4.3.3 Satellite and Internet of Things (IoT) Technologies Convergence

For effective merging of Satellite and IoT technologies, Internet of Things (IoT) enabled devices are Application Servers are required to be on the ground, however eNB gateways either located on earth stations using indirect-to-satellite links (ItS-IoT) or hosted on the Satellite using Direct-to-Satellite links (DtS-IoT) or both in combination. The deployment of core network components either in space and ground network infrastructure using virtualization technologies is another open research challenge. For example, in case of sparse IoT constellation where immediate access to ground is not possible, the LoRa/LoRaWAN servers should be at least specifically deployed on the LEO Satellite for autonomously allowed for access and then switch the data towards the core network components. The main conclusion is that convergence of satellite and IoT technology is viable but comes up with a lot of challenges with respect to networking functionality, network components placement, and parameters optimization.

Furthermore, integration of satellite and IoT networks for provisioning of communication services in remote distanced and underserved regions also comes up with other challenges such as design, security and implementation challenges. In next section, the concerns associated with satellite-integrated IoT with respect to design, security and implementation are explored and elaborated in detail.

In summary, satellite-integrated IoT architectures span indirect (gateway-assisted) and direct-to-satellite models, complemented by inter-satellite links for resilience and global reach. Each option presents trade-offs in terms of coverage, latency, energy consumption, and scalability. These architectural foundations underpin the design, security, and implementation challenges analysed in the following section.

5. DESIGN, SECURITY, AND IMPLEMENTATION CHALLENGES OF SATELLITE-INTEGRATED IOT NETWORKS

Satellite-Integrated IoT allows for solving the issues and enhancing the connectivity in remote, distanced, and underserved regions by utilizing satellite communication to extend Internet and communication services and specifically support IoT applications (GSMA, 2024; 3GPP, 2022; 5G Americas, 2023). The integration of IoT networks using satellite communication comes with various challenges associated with design, security, and implementation, which include integrating satellite and IoT communication infrastructure, handling sensing at scale, and enabling computing in a complex satellite environment (Lin et al., 2021; Vanelli-Coralli et al., 2024; ETSI 6G-NTN, 2024). For successful design and deployment of Satellite-Integrated IoT infrastructure, addressing these challenges is crucial to realize the full potential of satellite and IoT network integration and to achieve benefits in remote and underserved regions (3GPP, 2022; 5G Americas, 2023; GSMA, 2024). In this section, the design, security, and implementation challenges that could be faced by Satellite-Integrated IoT networks are discussed, including orbit-driven latency/Doppler and mobility, energy-constrained terminals, massive/random access at scale, edge/on-orbit processing, and resilient end-to-end security (Kodheli et al., 2020; Sørensen et al., 2021; Wei et al., 2019; Gardill et al., 2023).

5.1 Satellite-Integrated IoT Design Challenges

Satellite-Integrated IoT network design for enhancing connectivity in remote and underserved areas required to deal with several technical constraints for ensuring the network efficiency, reliability and scalability (Abdel-Rahman et al., 2022). The key challenges associated with network design mainly positioned on network architecture, power consumption and data management.

5.1.1 Network Architecture and Latency

The conventional Internet of Things (IoT) networks leverage terrestrial network infrastructure for communication but in remote distance and specifically in underserved regions where telecommunication infrastructure is not viable due to terrain or seas, a hybrid network for communication is essential. Such network infrastructure can be established using integration of ground-based devices by leveraging the satellite constellation. The Low Earth Orbit (LEO) satellite communication considered most suitable with its lower latency features comparing to Geostationary Earth Orbit (GEO) satellites. However, LEO Satellite Constellations also have some limitations including high mobility which will lead to rapid and frequent handovers that will require a complex mechanism for dynamic routing implementation and network link management (Abdel-Rahman et al., 2022). The high mobility in LEO Satellite constellations can cause to create highly time-variant communication channels with high network latency and will make it complicated to manage and maintain network connections stability. By using the LEO satellite constellation, a balanced network coverage and maintaining the network latency for making network architecture suitable for long range Iot services in remote and underserved regions is another vital challenge for Satellite-Integrated IoT networks. The development of a robust and adoptable satellite-integrated IoT network architecture for supporting the dynamic nature of satellite communication environment and diverse IoT Applications can also be faced as the challenge for Satellite and IoT integration.

5.1.2 IoT Devices Energy Consumption and Power

Remote IoT nodes are typically battery-only and expected to last years. Compared with terrestrial links, satellite paths add higher path loss, Doppler, and sometimes repetition, raising energy per delivered bit if not engineered carefully (Kyocera AVX, 2024; GSMA, 2024). NB-IoT leverages PSM/eDRX and coverage-enhancement repetitions within a managed, licensed-spectrum environment; Release-17 NTN profiles bring NB-IoT to LEO/GEO with

RACH, HARQ, and synchronization adaptations (3GPP, 2022). LoRaWAN remains attractive for ultra-low power, with LR-FHSS preserving low terminal power while improving capacity and robustness for direct-to-satellite links (Ullah, Mikhaylov, & Alves, 2021). Practical device design must also consider antenna efficiency in small form factors and the impact of uplink-centric traffic on battery drain (Kyocera AVX, 2024).

5.1.3 Network Scalability and Massive Connectivity

The main objective of Satellite-integrated IoT networks it to connect a large number of IoT Device in remote and underserved regions that can cause for a higher singling overhead when a bulk of connected IoT devices communicate simultaneously. The conventional network access protocols strive hard to manage for identification and authentication of massive IoT devices connected with access network, so the satellite-integrated IoT network architecture should be scalable for accommodating the increasing number of IoT end user devices. These excessively connected IoT devices can strain data processing and satellite network infrastructure resources as well. For supporting and efficient operation of large amount of IoT devices, it becomes more crucial to manage limited network resources more adequately in satellite systems such as network bandwidth and battery power.

5.1.4 Data Processing and Management Issues

The immense data volume and variety produced by IoT devices connected with Satellite-Integrated IoT networks will also pose significant data processing and management challenges. The bulk amount of data generated will make it difficult to gather, store, and process IoT devices data in efficient and timely manners specifically given the inconsistent and small sized data packets originated by the IoT devices. The edge computing in collaboration with IoT allows for local pre-processing of data originated by massively connected IoT devices in satellite-integrated IoT network and can help for reducing the bandwidth choking and network latency through unnecessary data filtration before transmitting over the direct-to-satellite and indirect-to-satellite links. In edge-computing, data is processed on the nearest source (gateway device or on the satellite) before sending to nodes where data have to save. Most recent research works depicts that the involvement of edge computing is increasing to satellite and space communication, in SIOT networks satellite and IoT nodes works as a data pipeline where sensor nodes on ground originates that data, stored and transported to ground stations when on coverage (Denby & Lucia, 2020). From satellite point of view, two main points are considered mostly for edge computing integration IoT nodes and satellite orbit using satellite. The edge computing technology allows for dealing efficiently with the data management and processing challenges in satellite-integrated IoT network architecture.

5.2 Satellite-integrated IoT Security Challenges

The exclusive attributes of Satellite-integration IoT (SIOT) specifically for providing the communication with deployment in remote and underserved regions expands its attack surface and brings up new and critical security challenges. A few of security constraints associated with Satellite-integrated IoT network are elaborated in this section.

5.2.1 Satellite-integrate IoT Physical Security Challenges

When satellite-integrated IoT networks are designed and deployed with intend to provide network connectivity and communication in remote distance and underserved regions, the mostly services providing areas are unmonitored due to remoteness where deployed Internet of Things (IoT) devices become vulnerable with respect to physical security. Any attacker aims to hinder the access network can get physical access to IoT devices to harm the sensitive information like breach it, inject malicious code, and disruption of network functionality and its operation. The unavailability of infrastructure and continuous devices monitoring on remote areas due to isolated locations also makes deployed IoT devices suspicious to physical tempering, theft, or vandalism (Ferreira et al., 2021). Furthermore, hard environmental conditions of remote and underserved areas due to terrain or oceans can also cause to damage or physical destruction of IoT devices hardware.

5.2.2 Data Integrity and Confidentiality Challenges

The 6G communication networks which comprised of satellite, UAVs, underground and undersea communication with context to protect communication must guarantee security, reliability, confidentiality, data integrity, low latency, and secure and efficient communication without breaching the data integrity. The data transporting between remotely deployed IoT devices to satellite and then from satellite to earth stations using either direct-to-satellite or indirect-to-satellite links can be highly vulnerable for eavesdropping and manipulation using the security attacks like man-in-the-middle (MITM) attacks. The advance level of encryption algorithms and hashing mechanism can only ensure the confidentiality and integrity of data transporting between IoT end devices and Satellite and then back to earth stations for data storing. The long range communication links and time fluctuating channels nature of LEO satellite constellations (Chen, Xu, & Shang, 2023) makes difficult the implementation for secure communication protocols and encryption algorithms such as Transport Layer Security and Secure Socket Layer (TSL/SS).

5.2.3 Authentication and Access Control Challenges

Communication links between satellites and earth stations are also considered vulnerable and must be ensured for secure communication links for data transportation to prevent from unauthorized access and data breaches (ENISA, 2025; ENISA, 2023). The implementation and enforcement of strong authentication mechanism in Satellite-integrated IoT networks is also a challenge due to weak or default passwords and fragmented identity frameworks across various technologies. The enforcement of robust access control methodologies for limiting user access to satellite and IoT devices resources and data as well is mandatory for maintaining system and information security. In SOIT with multitude IoT devices making secure to every connection is ultimate challenge and insufficient network segmentation is another factor that permits an attacker to intrude freely in the network if a single device on network found vulnerable. Furthermore, satellite systems are also vulnerable to for cyber security threats which can be addressed by implementing the proactive security measures for mitigating the cybersecurity risks and ensuring network and data integrity.

5.2.4 Extended Attack Surface and Vulnerabilities

In Satellite-integrated IoT specifically deployed for connectivity in remote and underserved areas network encompasses from ground station in remote locations with IoT devices, through space, to earth stations and further to data centres for storing the data received from IoT remote devices. This scenario develops a massive and multifaceted attack surface with various potential breach points. The IoT devices deployed on remote locations mostly lack with robust built-in security defence features and mechanisms that make these devices vulnerable against malware, spoofing attacks and other cybersecurity threats (Hassanzadeh, 2021). The use of vendor specific and legacy hardware equipment in few industrial IoT applications can also cause to make network vulnerable and security complicated because such hardware components might lack with advance encryption and authentication algorithm support.

5.3 Satellite-integrated IoT Implementation Challenges

The designing and implementation of satellite-integrated IoT network for remote and underserved regions demands encountering numerous technical constraints for ensuring efficiency, flexibility, scalability and reliability. The most importance challenges and limitations rely on network architecture, power and energy consumption, security and data management. Following are the potential implementations challenges faced by the satellite-integrated IoT network.

5.3.1 Physical and Environmental Constraints

The implementation of Satellite-integrated IoT network infrastructure in remote and underserved regions mostly have to face environmental challenges like extreme and unfavourable weather conditions, dense foliage, rocky terrain with land sliding, and sea areas with heavy rains and storms. These environmental factors like mountains, trees or undersea can disrupt the line of sight (LOS) for satellite signals and affecting the reception.

5.3.2 Cost and Infrastructure Obstacles

The design and deployment of satellite constellation and establishing required ground stations infrastructure and specifically the deployment and maintaining the IoT devices infrastructure in remote and underserved areas required a massive initial financial requirement that is considered a major challenge. Though the cost of Nano-satellites (CubeSats) has been reduced but still it remains considerable. Moreover, the specialized satellite IoT devices and earth stations equipment cost, uninterruptable power supply with backups, and environmental expenditures are the cost and infrastructure constraints which are prohibitive for implementation of various satellite-integrated IoT applications. The high cost occurred for launching and maintaining the satellites in orbit can also be an obstacle for widespread implementation of satellite-integrated IoT architecture.

5.3.3 Regulatory, Compliance, Standardization, and Interoperability Challenges

For deployment and operating a global satellite network for reaching out the remote and underserved regions in different territories requires navigating complex and complicated international regulations and their compliance challenges. The frequency spectrum allocations and licensing policies also variate across the globe, different countries have different rules, regulations and legal requirements for implementing satellite communication, IoT devices network deployment, data privacy, security, governance, and telecommunications regulatory affairs which can be a major obstacle for design and implementation of satellite-integrated IoT network infrastructure. The interoperability constraints among various satellite and terrestrial technologies across the world is another major concern faced for design and deployment of unified satellite-integrated IoT network architecture. With technological perspective, the development of standardized protocols and interfaces for satellite-based IoT networks is another essential problem prompts for interoperability and reducing the fragmentation. For effective and efficient satellite-integrated IoT network architecture and services clear and precise regulatory frameworks are necessary to establish that can ensure its responsible implementation and to avoid conflicts with currently working terrestrial communication networks.

5.3.4 Operation, Maintenance and Longevity Challenges

The implementation of Satellite-integrated IoT networks with its remote nature makes operation's monitoring and maintenance a complicated, time consuming, costly and challenging task due to obstacles to physically access the deployed IoT devices in remote distanced areas for various maintenance activities like replacement of batteries, repair tasks, preventive and scheduled maintenance works, and implementation of security updates (Shafi, Zafar, & Mehmood, 2023). These challenges emphasising on the deployed IoT device in remote areas should be with long lifespans, least maintenance requirements and capability for implementing the security, hardware and software patches updates over-the-air.

6. DISCUSSION

This review shows that Satellite-Integrated IoT (SIoT) can meaningfully close connectivity gaps in remote and underserved regions when design, security, and implementation choices are made coherently across space, link, and ground segments. In practice, two integration paths dominate: (i) 3GPP NB-IoT over NTN for managed, carrier-grade services integrated with 5G cores, and (ii) LoRaWAN direct-to-satellite (DtS) increasingly with LR-FHSS for ultra-low-power, sparse telemetry and private/hybrid deployments (3GPP, 2022; Lin et al., 2021; GSMA, 2024; 5G Americas, 2023; Ullah et al., 2021; Fraire et al., 2022).

Network architecture and latency. LEO constellations offer order-of-magnitude lower propagation delay than GEO, but real-world performance varies with gateway proximity and inter-satellite link (ISL) routing; frequent handovers and time-varying Doppler require robust synchronization, lightweight mobility, and pass-aware session strategies (Lin et al., 2021; 3GPP, 2022; 5G Americas, 2023). Your Section 4 correctly highlights that latency variance and short visibility windows must be absorbed not only by the radio stack but also by application logic (e.g., idempotent uplinks, tolerant timeouts), which is consistent with current NTN guidance (El Jaafari, 2023; GSMA, 2024).

Energy and device pragmatics. Satellite links increase path loss and may necessitate repetitions and longer synchronization, raising energy per delivered bit if unmanaged. NB-IoT mitigates this via PSM/eDRX and coverage-enhancement repetitions under operator control; LoRaWAN preserves ultra-low terminal power and, with LR-FHSS, gains capacity/collision robustness for DtS (Kyocera AVX, 2024; Ullah et al., 2021). Your emphasis on antenna efficiency in small form factors and uplink-centric traffic aligns with field experience; practical levers include pass-aware duty-cycling, event batching, and link-margin-aware coding/repetition (Kyocera AVX, 2024).

Massive access and scalability. As your text notes under "Network Scalability," ALOHA-style access saturates as populations grow. The literature converges on LR-FHSS, Slotted/Reservation-ALOHA, and IRSA-style schemes to improve throughput and resilience for DtS (Heusse et al., 2023; Ullah et al., 2021; Recayte et al., 2024). For NB-IoT NTN, scaling hinges on RACH parameterization tuned to long RTT/Doppler and on grant-free access techniques both active topics in Rel-17/18 work (Kodheli et al., 2020; El Jaafari, 2023).

Security posture end-to-end or nothing. Your "Security Challenges" section correctly identifies the expanded attack surface spanning device tamper, long-haul links, and ground platforms. For cellular NTN, TS 33.501 provides a robust baseline (AKA/EAP, NAS/AS protection, SBI security) but implementers must still solve device identity, key lifecycle over discontinuous coverage, and country-specific routing/location obligations (3GPP TS 33.501, 2023; 5G Americas, 2023). For LoRaWAN, cryptographic primitives are sound when implemented correctly; risks commonly stem from weak/default passwords, improper key provisioning, and backend misconfiguration precisely the issues you flag (LoRa Alliance, 2017; Loukil et al., 2022; OWASP, 2024; GSMA, 2024). Sector-level threat work further underlines jamming/spoofing and supply-chain/configuration weaknesses across space and ground segments, reinforcing your call for proactive controls (zero-trust segmentation, rate-limited admission, beam/frequency agility, continuous monitoring) (ENISA, 2025; ENISA, 2023; ETSI/6G-NTN, 2024).

Implementation realities. Your "Implementation Challenges" environmental constraints, cost/infrastructure, and the policy stack (spectrum, licensing, cross-border operation) are consistent with the broader NTN picture. NB-IoT NTN benefits from licensed spectrum and MNO core integration but must observe TN/NTN coexistence and location/routing requirements, with Rel-18 adding useful mobility/coverage refinements (El Jaafari, 2023; 3GPP, 2022). LoRaWAN DtS in unlicensed ISM bands requires careful adherence to regional duty-cycle/EIRP rules and evolving satellite-extension guidance (GSMA, 2024; 5G Americas, 2023). For O&M, your points on battery replacement logistics, remote firmware updates, and preventive maintenance match best practice: prioritize OTAs, health beacons, and design-for-serviceability (Wei et al., 2019; Kyocera AVX, 2024).

Synthesis when to use what. A pragmatic pattern is a multi-tier architecture: terrestrial LoRaWAN with satellite backhaul where gateways are viable; DtS LoRaWAN for sparse outliers; and NB-IoT NTN where QoS, mobility, and regulatory alignment are mandatory (utilities, safety-critical, high reliability). Such a hybrid approach balances coverage, energy, cost, and compliance across varied terrains and use cases (GSMA, 2024; 5G Americas, 2023).

7. CONCLUSION

Satellite integration significantly extends IoT coverage into remote and underserved regions, but realizing this potential requires coordinated work across radio design, security engineering, and operational practice. LEO constellations and LPWAN technologies (NB-IoT, LoRaWAN with LR-FHSS) provide complementary trade-offs: NB-IoT suits carrier-grade QoS and mobility, while LoRaWAN supports ultra-low-power, sparse telemetry. Key unresolved challenges include scalable random-access for DtS, secure key lifecycle across discontinuous coverage, cost-effective O&M for battery-powered devices, and harmonized global spectrum/regulatory frameworks. We recommend: (i) empirical studies comparing DtS protocol behaviour in field trials, (ii) development of lightweight end-to-end security frameworks for DtS IoT, and (iii) research on sustainable business/maintenance models for long-life remote deployments.

REFERENCES

3GPP TS 33.501. (2023). *Security architecture and procedures for 5G system*. 3rd Generation Partnership Project.

3GPP. (2021–2023). *Technical specifications on non-terrestrial networks (NTN) and IoT over satellite*. 3rd Generation Partnership Project.

3GPP. (2022). *Release 17 and 18 specifications for NB-IoT over NTN*. 3rd Generation Partnership Project.

5G Americas. (2023). *Non-terrestrial networks in 5G and beyond: Integration of satellite and terrestrial systems*. 5G Americas White Paper.

Abdel-Rahman, A., Al-Mualla, N., Al-Sayed, T., & Al-Maawali, A. (2022). Applications and security concerns of satellite-based IoT networks: A conceptual view. *International Journal of Research and Engineering, 9*(2), 2673–2679.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805.

Centenaro, M., Costa, C. E., Granelli, F., Sacchi, C., & Vangelista, L. (2021). A survey on technologies, standards, and open challenges in satellite IoT. *IEEE Communications Surveys & Tutorials, 23*(3), 1693–1720.

Chen, X., Xu, Z., & Shang, L. (2023). Satellite Internet of Things: Challenges, solutions, and development trends. *Frontiers of Information Technology & Electronic Engineering, 24*(7), 935–944.

Chiti, F., Fantacci, R., & Pierucci, L. (2019). Energy efficient communications for reliable IoT multicast 5G/satellite services. *Future Internet, 11*(8), 164.

Clazzer, F., Munari, A., Bisio, I., Lavagno, L., & Marchese, M. (2022). From 5G to 6G: Satellite integration into IoT. *IEEE Internet of Things Journal, 9*(17), 15907–15921.

Colavolpe, G., Foggi, T., Ricciulli, M., Zanettini, Y., & Mediano-Alameda, J. P. (2019). Reception of LoRa signals from LEO satellites. *IEEE Transactions on Aerospace and Electronic Systems, 55*(6), 3587–3602.

Denby, B., & Lucia, B. (2020, March). Orbital edge computing: Nanosatellite constellations as a new class of computer system. In *Proceedings of the 25th International Conference on Architectural Support for Programming Languages and Operating Systems* (pp. 939–954).

Duran, J., Perez-Vazquez, S. M., Fernandez-Fidalgo, M., & Gonzalez-Alvarez, J. (2024). Multi-layered satellite communications systems for ultra-high availability and resilience. *Electronics, 13*(7), 1269.

El Jaafari, M. (2023). NTN access and mobility management in 5G Release 18. *IEEE Communications Standards Magazine, 7*(3), 22–30.

ENISA. (2021). *Threat landscape for 5G networks*. European Union Agency for Cybersecurity.

ENISA. (2023). *Cybersecurity for space and satellite communication systems*. European Union Agency for Cybersecurity.

ENISA. (2025). *Space threat landscape report 2025*. European Union Agency for Cybersecurity.

ETSI. (2024). *ETSI 6G-NTN report*. European Telecommunications Standards Institute.

Ferreira, P., Antunes, H., Pinto, P., & Monteiro, E. (2021). Physical layer security in satellite-based communication networks. *IEEE Communications Surveys & Tutorials, 23*(1), 583–623.

Fraire, J. A., Céspedes, S., & Accettura, N. (2019, September). Direct-to-satellite IoT: A survey of the state of the art and future research perspectives. In *International Conference on Ad-Hoc Networks and Wireless* (pp. 241–258). Springer.

Fraire, J. A., Henn, S., Dovis, F., Garello, R., & Taricco, G. (2020, December). Sparse satellite constellation design for LoRa-based direct-to-satellite IoT. In *IEEE Global Communications Conference (GLOBECOM)* (pp. 1–6).

Fraire, J. A., Iova, O., & Valois, F. (2022). Space-terrestrial integrated Internet of Things: Challenges and opportunities. *IEEE Communications Magazine, 60*(12), 64–70.

Ground Control. (2023). *Satellite IoT backhaul solutions: Technical overview*. Ground Control White Paper.

GSMA. (2022). *IoT security guidelines*. GSM Association.

GSMA. (2024). *Extending IoT with satellites: Market and technology insights*. GSM Association.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Hassanzadeh, S. (2021). Security challenges in satellite-integrated IoT systems. *IEEE Access, 9*, 12533–12547.

Heusse, M., et al. (2023). Random access schemes for massive IoT over satellite. *IEEE Transactions on Wireless Communications, 22*(11), 7554–7569.

ITU. (2022). *Measuring digital development: Facts and figures*. International Telecommunication Union.

Kim, J., & Song, J. (2018). A secure device-to-device link establishment scheme for LoRaWAN. *IEEE Sensors Journal, 18*(5), 2153–2160.

Kumar, S., & Choudhary, N. (2024). Advancements in satellite communication systems: Enabling seamless connectivity in a hyperconnected world. *Journal of Emerging Communication Technologies, 12*(4), 77–89.

Kyocera AVX. (2024). *Design considerations for low-power satellite IoT devices*. Kyocera AVX Technical Report.

Lin, X., et al. (2021). 5G new radio evolution towards 6G: NTN and IoT perspectives. *IEEE Communications Magazine, 59*(7), 36–42.

LoRa Alliance. (2017). *LoRaWAN security whitepaper*. LoRa Alliance.

LoRa Alliance. (2023). *LoRaWAN for satellite integration: Deployment guidelines*. LoRa Alliance.

Loukil, S., et al. (2022). Security analysis of LoRaWAN-based satellite IoT. *IEEE Access, 10,* 112233–112245.

Mannoni, V., et al. (2021). Enabling technologies for satellite IoT: Protocol adaptations and design insights. *International Journal of Satellite Communications and Networking, 39*(5), 455–472.

Qureshi, A. S. (2022). Applications and security concerns of satellite-based IoT networks: A conceptual view. *International Journal of Computer Applications, 184*(25), 34–40.

Recayte, J., et al. (2024). Scalable random access for direct-to-satellite IoT. *IEEE Internet of Things Journal, 11*(5), 8812–8825.

Shafi, U., Zafar, A., & Mehmood, S. (2023). Analysis of IoT security challenges and solutions using artificial intelligence. *Sensors, 23*(16), 6902.

Sinha, R. S., Wei, Y., & Hwang, S. H. (2017). A survey on LPWA technology: LoRa and NB-IoT. *ICT Express, 3*(1), 14–21.

Sørensen, R., et al. (2021). Delay-tolerant networking in LEO satellite IoT constellations. *IEEE Access, 9,* 145233–145247.

Sweeting, M. N. (2018). Modern small satellites—Changing the economics of space. *Proceedings of the IEEE, 106*(3), 343–361.

Ullah, S., Mikhaylov, K., & Alves, H. (2021). Random access for LoRaWAN in LEO satellite systems. *IEEE Transactions on Wireless Communications, 20*(12), 8231–8244.

Vanelli-Coralli, A., et al. (2024). Satellite IoT integration challenges: From 5G NTN to 6G. *IEEE Vehicular Technology Magazine, 19*(1), 44–56.

Wei, Q., et al. (2019). Design of secure lightweight cryptography for IoT over satellite. *IEEE Internet of Things Journal, 6*(5), 8222–8233.

World Bank. (2016). *World Development Report 2016: Digital dividends*. The World Bank.