Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.074678

REVIEW

Machine Learning-Enabled NTN-Assisted IoT: Mapping the Security Landscape

Oluwatosin Ahmed Amodu[1], Zurina Mohd Hanapi[1,*], Raja Azlina Raja Mahmood[1], Faten A. Saif[2], Huda Althumali[3], Chedia Jarray[4], Umar Ali Bukar[5] and Mohammed Sani Adam[6]

[1]Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, UPM, Serdang, Selangor, Malaysia
[2]Department of Information Technology, Gulf Colleges, Hafar Al Batin, Saudi Arabia
[3]Computer Science Department, Faculty of Science and Humanities, Imam Abdulrahman bin Faisal University, Jubail, Saudi Arabia
[4]Systems Modeling, Analysis, and Control Research Laboratory (MACS), University of Gabes, Avenue Omar Ibn El Khattab, Zrig Eddakhlania, Zrig Gabes, Tunisia
[5]Department of Computer Science, Faculty of Computing and Artificial Intelligence, Taraba State University, ATC, Jalingo, Nigeria
[6]Department of Electrical, Electronics & Systems Engineering, Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia, UKM, Bangi, Selangor, Malaysia

*Corresponding Author: Zurina Mohd Hanapi. Email: zurinamh@upm.edu.my

Received: 15 October 2025; Accepted: 26 December 2025; Published: 08 May 2026

ABSTRACT: Non-terrestrial networks (NTNs), encompassing unmanned aerial vehicles (UAVs), low-/high-altitude platforms (LAPs/HAPs), and satellite systems, are increasingly enabling Internet of Things (IoT) applications beyond the limits of terrestrial infrastructure. By combining UAV mobility with satellite and HAP coverage, NTN-assisted IoT supports diverse use cases, including remote sensing, smart cities, intelligent transportation, and emergency response. This paper presents a systematic mapping of machine learning (ML) research in NTN-assisted IoT with a focus on security-related aspects. A keyword co-occurrence analysis of over 2000 publications identifies twelve thematic clusters, including three clusters directly related to security, privacy, and trust. Cluster interconnections are analyzed to reveal dominant research trends and technological dependencies. The first security-focused cluster addresses access control, authentication, privacy preservation, and ML-based intrusion detection in Internet of Drones (IoD) and satellite-enabled systems, while also highlighting feature selection and energy-aware design. The second cluster centers on edge computing-enabled localization and privacy, linking technologies such as GPS, RSSI, LoRaWAN, and differential privacy for smart-city deployments. The third cluster emphasizes blockchain-enabled trust mechanisms, integrating blockchain with aerial image classification, intrusion detection, and secure coordination in IoD environments. Using a connectivity-driven analysis, anchor keywords with strong intra-cluster associations are identified and discussed alongside representative literature. Finally, emerging low-frequency themes are used to outline future directions, including AI-enabled security, trustworthy edge intelligence, autonomous and resilient robotic systems, predictive cyber resilience, and secure cognitive communication for next-generation NTN-assisted IoT.

KEYWORDS: Non-terrestrial networks; Internet of Things; Internet of Drones; satellites; UAVs; edge computing; localization; intrusion detection; privacy; federated learning; blockchain

1 Introduction

Non-terrestrial networks (NTNs) integrate aerial and spaceborne communication platforms, including unmanned aerial vehicles (UAVs), high- and low-altitude platforms (HAPs/LAPs), and satellites, into modern communication infrastructures. By extending connectivity beyond traditional terrestrial systems,

NTNs offer advantages such as flexible deployment, resilience to ground-based disruptions, and wide-area coverage across urban, rural, remote, and maritime environments. These capabilities have made NTNs increasingly central to applications in public safety, healthcare, agriculture, environmental monitoring, industrial automation, transportation, and smart-city systems [1].

The convergence of NTNs with Internet of Things (IoT) architectures has significantly expanded application possibilities. For instance, Satellite-Aerial-Ground Integrated Networks (SAGINs) support emergency communication by coordinating distributed aerial base stations, IoT terminals, and multi-orbit satellite constellations [2]. NTN-assisted IoT systems are now being applied in precision agriculture, autonomous navigation, mobile edge computing, localization and tracking, environmental sensing, and collaborative UAV-assisted data collection.

However, deploying NTN to support IoT introduces several technical challenges, with security being one of the most critical. NTN systems rely on highly dynamic and often heterogeneous aerial and satellite platforms to support resource-constrained IoT devices. This combination increases the system's vulnerability to security breaches, making secure communication a crucial requirement for NTN-assisted IoT.

Therefore, robust security measures, such as authentication mechanisms, physical-layer security, anti-jamming techniques, intrusion detection systems, access control, hardware security, privacy preservation, anomaly detection, and blockchain, are essential in these networks. Addressing these challenges requires adaptive and intelligent security solutions capable of mitigating diverse attacks, including jamming, denial-of-service, mobile security threats, data-privacy violations, and other cybersecurity risks, while adapting to the varying network and operating conditions characteristic of NTN-assisted IoT environments.

Machine learning (ML) has thus become a critical enabler of NTN-IoT advancement. A wide spectrum of ML approaches, including supervised, unsupervised, self/semi-supervised learning, deep learning, reinforcement learning (RL/DRL), and federated learning (FL), is being used to optimize performance indicators such as throughput, latency, energy efficiency, trajectory planning, and scheduling. ML techniques are increasingly being used to enhance security in NTN-assisted IoT architectures, helping to address a wide range of cybersecurity challenges such as authentication, data privacy protection, jamming mitigation, anomaly detection, denial-of-service attacks, and network intrusions. These security needs arise across several key NTN applications, such as network connectivity, coverage provisioning, data collection, and computation offloading. In these scenarios, one or more UAVs, satellites, or IoT devices forming the aerial-terrestrial network may rely on ML-based methods to provide strong security guarantees and protect the network environment.

This study focuses on security-enabled clusters in our comprehensive bibliometric mapping and thematic review project of ML-based NTN-assisted IoT research using a dataset of over 2000 publications. Through a detailed keyword co-occurrence analysis, twelve thematic clusters were identified in this project, indicating several research directions, interdependent and interwoven technologies, as well as indicators pointing to fundamental and emerging challenges. Among these, three clusters form the core focus of this paper: (i) *Security and Privacy in NTN-IoT (Security and Access Control)*, covering access control, authentication, intrusion detection, privacy preservation, and ML-driven protection mechanisms in IoD and satellite environments; (ii) *Edge Computing, Localization, and Privacy (Edge Localization and Privacy)*, covering differential privacy, edge intelligence, fingerprinting, LoRaWAN/GPS-based localization, and smart-city security. (iii) *Blockchain Security, Aerial Image Classification, and IDS for the Internet of Drones (Blockchain-Enabled IoD Security)*, covering blockchain-based security, aerial image classification, lidar-enabled perception, intrusion detection systems, power control techniques, and communication technologies that support IoD services and performance requirements.

These research domains represent nuanced opportunities and include both high-level and granular directions that are often difficult to uncover using traditional review methods without examining hundreds of publications. The identified clusters illuminate several existing and emerging research pathways, particularly those centered on applying machine learning to enhance security in UAV, satellite, and NTN-assisted IoT networks across diverse rural and urban applications, including computing, connectivity and coverage, and data collection. They also serve as a precursor to the future research directions derived from the low-occurrence keyword analysis, such as AI-enabled NTN security, trustworthy edge intelligence, autonomous and resilient robotic systems, predictive cyber resilience, and cognitive secure communication.

This paper makes the following contributions:

- **Comprehensive Security Mapping:** Systematic, data-driven mapping of security-related research in ML-based NTN-assisted IoT using keyword co-occurrence analysis.
- **Inter-cluster Mapping Framework:** Development of a mapping framework illustrating how security, localization, edge intelligence, and privacy-preserving mechanisms, blockchain, and intrusion detection systems interconnect across NTN-IoT ecosystems.
- **Emerging Research Directions:** Identification of gaps and opportunities related to AI-enhanced NTN security, trustworthy edge intelligence, autonomous robotic systems, predictive intelligence, and cognitive secure communication.

Paper Organization. Section 2 reviews related surveys and positions the novelty of this work. Section 3 describes the bibliometric methodology and the associated workflow. Section 4 outlines the derived clusters and keyword constituents. Sections 5–7 analyze the three security-related domains in depth. Section 8 synthesizes key contributions from the literature. Section 9 discusses emerging themes, while Section 10 maps identified challenges to future research opportunities. Section 11 concludes the paper. A summary of the outline is shown in Fig. 1.

2 Related Reviews

A wide range of surveys has explored individual components of NTN-assisted IoT systems, including UAV communication, satellite security, intrusion detection, localization, and edge intelligence. However, these studies primarily address isolated technologies or application domains and do not provide an integrated mapping of how machine learning (ML) supports security, privacy, and edge intelligence across multi-layer NTN-IoT ecosystems. In contrast, this study uniquely combines bibliometric analysis based on keyword co-occurrence to provide a thematic synthesis to connect security-, privacy-, and localization as well as its associated technologies related to ML research across drones, UAV and satellite communication, and edge computing domains. To clearly position this work, this section discusses the most relevant review studies and situates their scope relative to the comprehensive mapping developed in this paper.

2.1 IoD/UAV Security, IDS, and Blockchain

Surveys such as [3] provide an overview of the Internet of Drones (IoD), covering privacy protection, authentication mechanisms, blockchain frameworks, neural-network-based solutions, and optimization techniques. Other works examine intrusion detection systems (IDS) in domain-specific IoT settings. For instance, Ferrag et al. [4] review IDS solutions for Agriculture 4.0, identifying major threats, existing IDS frameworks, evaluation metrics, and publicly available datasets. Their survey evaluates IDS approaches across emerging technologies such as cloud, fog/edge computing, network virtualization, autonomous tractors, drones, IoT-enabled agriculture, and smart grids, and outlines future research challenges for securing next-generation agricultural systems.

- Organization of this paper
  - Introduction
  - Related Reviews
  - Methodology
    - Data Collection
    - Keyword Extraction and Data Cleaning
    - Co-occurrence Network Construction
    - Cluster Extraction and Validation: A Novel Connectivity-Based Method
    - Interpretation and Thematic Mapping
  - Thematic Clusters and Key Findings
    - Security and Access Control
    - Edge Localization and Privacy
    - Blockchain-Enabled IoD Security
  - Security, Privacy, and Access Control in NTN-Assisted IoT Systems (Security and Access Control)
    - Security and Privacy in NTN-Assisted IoT Networks
    - Security and Its Interconnections
    - Access Control and Authentication
    - Cybersecurity and Intrusion Detection
    - Privacy and Feature Selection
    - Internet of Drones and LEO Satellites
    - Energy Harvesting and Secure System Design
  - Edge Computing, Localization, and Privacy in NTN-Assisted IoT Systems (Edge Localization and Privacy)
    - Edge Computing and Localization in NTN-Assisted IoT
    - Edge Computing as a Core Enabler
    - Privacy and Differential Privacy
    - Localization Technologies
  - Blockchain Security for Aerial Image Classification and IDS for Internet of Drones and Service Quality (Blockchain-Enabled IoD Security)
    - Internet of Drones
    - Image Classification
    - Blockchain and Applications
    - Communication, Related Aspects, and Technologies
  - Highlights of Research Linked to Selected Keywords
    - Machine Learning-Based Security Approaches for IoT-Assisted UAV Networks
    - Edge Computing, Localization, and Privacy
    - Security and Service Quality in Aerial Image Classification and Internet of Drones
  - Discussion, Research Outlook, and Case Studies
    - Discussion and Research Outlook
    - Real-World Case Studies Validating Thematic Domains
  - Future Directions
    - AI-Enhanced Security and Intelligence for Next-Generation NTN-Assisted IoT
    - AI-Driven Predictive Intelligence and Cyber Resilience in NTN-Assisted IoT Systems
    - Cognitive and Secure Communication for Energy-Efficient NTN-Assisted IoT Networks
    - Trustworthy and Secure Edge Intelligence for Industrial NTN-Assisted IoT Systems
    - Autonomous, Secure, and Resilient Robotic Intelligence in NTN-Assisted IoT Systems
  - Conclusion

Figure 1: Organization of this paper.

UAV communication technologies are also widely studied. Sharma et al. [5] provide a comprehensive review of communication modules, antenna designs, resource platforms, and network architectures for UAV systems. They discuss ML-based path planning, secure communication strategies, encryption techniques,

and power-efficient mechanisms. Their survey also highlights key UAV applications, including navigation, surveillance, URLLC, edge computing, and AI-based services, along with open challenges in drone-to-drone communication.

Security within UAV swarms has received growing attention. Kou et al. [6] present a systematic review of key-agreement protocols for intelligent UAV swarms, addressing the unique security challenges of highly dynamic multi-UAV environments. They classify protocols according to autonomy levels and computational capabilities, and define core security requirements and threat models for swarm dynamics. Their work further categorizes swarm communication architectures (end-to-end ground-UAV, decentralized peer-to-peer multi-UAV, and hierarchical large-scale swarms) and proposes a novel *cryptographic automaton* architecture for for autonomous security management that supports dynamic key generation and context-aware adjustments in real time.

Blockchain applications for UAV networks are discussed extensively in [7–9]. Alladi et al. [7] review blockchain techniques for UAV security, including decentralized data storage, network security enhancement, surveillance, and inventory management, while identifying integration challenges and research trends. Mehta et al. [8] survey security issues for 5G-enabled UAVs and propose a blockchain-based security architecture, presenting a taxonomy of threats and a case study demonstrating blockchain-supported industrial UAV applications. Wang et al. [9], motivated by advancements in space-air-ground integrated networks (SAGIN), analyze the role of UAVs within SAGIN and propose a blockchain-assisted secure architecture to address vulnerabilities in traditional UAV communication systems. Their survey introduces key applications of blockchain-enabled UAV networks and outlines open research problems and future challenges in this emerging domain. Collectively, these studies affirm the significance of security in UAV systems. Yet, for the broader NTN ecosystem, including satellite-enabled IoT, a comprehensive security-focused investigation is still absent. Even research specifically addressing machine-learning-driven solutions remains lacking.

More recent contributions take a deeper look into the security and ML perspectives. The findings of Ogab et al. [10] reinforce these limitations through a systematic review of ML-based IDS for IoD networks. They show that hybrid and deep learning models dominate current research, while meta-heuristic algorithms are often used for feature selection and parameter tuning. Python is the most common implementation language, though the authors stress the need for real-world testing to validate practical feasibility. Ogab et al. also note that although performance is typically measured using accuracy, precision, recall, and F1-score, many studies overlook IoD-specific constraints such as limited computation, energy restrictions, mobility, and real-time requirements. Multi-class classification remains common but is computationally expensive, making binary classification more suitable for resource-limited drones. The authors further highlight that widely used datasets are outdated, imbalanced, and not representative of IoD traffic, underscoring the need for new IoD-specific datasets. Key challenges identified include latency in real-time detection, limited onboard resources, scalability issues, vulnerability to adversarial attacks, and the absence of standardized protocols. Future directions suggested by Ogab et al. include federated learning, edge-based detection, robust hybrid models for proactive intrusion prevention, and exploratory work on quantum computing to handle complex threat scenarios.

Considering the diverse landscape of low-altitude infrastructures, including the broader low-altitude economy that encompasses urban air mobility, sub-200-meter aerial surveillance, and drone logistics, security is paramount. Intelligent infrastructures are required to manage the complex operations involving multiple stakeholders. Ye et al. [11] survey the integration of IoT, AI-driven decision making, and blockchain-based trust mechanisms, which together form the foundational pillars of next-generation low-altitude systems. In such architectures, system components play distinct roles. IoT sensors are deployed on the ground and at ground stations, while UAVs and vertiports generate a real-time data fabric that

captures variables ranging from environmental conditions to air-traffic density. AI models rely on these data streams to perform predictive analytics, computer vision, multi-agent reinforcement learning, and large-language-model-based reasoning, supporting tasks such as flight-path optimization, anomaly detection, and autonomous coordination of UAV swarms. Blockchain provides immutable audit trails for regulatory compliance, secure device authentication through decentralized identities, and automation of contractual exchanges for services such as payload delivery or airspace leasing. The review by Ye et al. examines existing research and practical deployments, demonstrating how the synergy of IoT, AI, and blockchain technologies can enhance operational efficiency, resilience, and trustworthiness across low-altitude platforms. While their study focuses on emerging low-altitude and IoD ecosystems, it remains narrower in scope than the present work, which examines the broader NTN-IoT landscape and its major security dimensions using detailed keyword co-occurrence analysis and cluster-level insights to reveal research trends and thematic domains.

2.2 Satellite/Aerial-Terrestrial Integrated IoT Security

Surveys devoted to satellite IoT and aerial-terrestrial integrated networks identify several key vulnerabilities. Stojnic et al. [12] analyze cyber threats including spoofing, jamming, and DoS attacks. Physical-layer security techniques for satellite communication are reviewed in [13,14], highlighting intelligent reflecting surfaces, covert communication, and cooperative transmission for enhancing secrecy capacity.

Satellite communication has become a promising extension of terrestrial networks, offering wide-area coverage in remote regions and supporting high data rates for 6G and heterogeneous network research. However, because satellite links operate over a shared medium, they remain vulnerable to attacks such as eavesdropping, spoofing, and jamming. Abdelsalam et al. [15] investigate the use of physical layer security (PLS) to address these vulnerabilities, particularly for resource-limited devices in satellite-assisted IoT communication. PLS is considered a promising approach because it leverages inherent physical-layer characteristics to provide security without relying on computationally intensive cryptographic methods. The authors present a comprehensive review of PLS solutions for securing satellite communication and categorize applications into satellite-terrestrial systems, satellite-based IoT, satellite navigation systems, inter-satellite links, and free-space optical (FSO) communication. Their study discusses how PLS can enhance overall system security, with emphasis on its ability to resist various attack types. In addition, the authors identify several research gaps and open challenges, including the need for advanced threat models, improved uplink secrecy techniques, authentication and integrity mechanisms, and PLS frameworks for inter-satellite links. They also highlight the emerging role of machine learning in strengthening physical layer security.

In another related work, motivated by the growing role of the Artificial Intelligence of Things (AIoT), which integrates AI technologies with IoT infrastructures in satellite communication and mega-constellation systems, Massimi et al. [16] explore the use of deep learning for space situational awareness (SSA) in satellite-based IoT networks. Their objective is to reduce the risk of space collisions and address emerging threats to the sustainability and operational safety of space-based IoT infrastructures. The authors provide a systematic survey of the challenges and future perspectives associated with applying deep learning to SSA object detection and classification. They outline a variety of deep learning models and AI algorithms used to identify the nature and type of spatial objects based on radar-processed signals. Furthermore, they present a taxonomy of deep-learning-based methods for SSA object detection and classification, detailing their characteristics, capabilities, and implementation challenges. While these studies offer valuable insights into the prospects, challenges, and potential solutions within satellite, specific communication, including some security-related issues, they do not provide cross-cutting perspectives that encompass edge intelligence, access control, and blockchain security in the Internet of Drones. These themes emerge more clearly from the bibliometric mapping and cluster analysis presented in this paper.

2.3 Localization and Positioning (Indoor/Outdoor)

Localization surveys such as [17] examine ML-based fingerprinting techniques for indoor environments where GPS signals are unavailable, comparing different approaches in terms of energy consumption, accuracy, latency, and computational complexity, and outlining key challenges and future research directions. Similarly, reference [18] provides an extensive overview of RF-, BLE-, UWB-, Wi-Fi-, ZigBee-, and GNSS-based positioning methods. Hybrid secure localization models have also been explored in vehicular networks, as in [19], which proposes an access-control–driven approach to improve both localization security and system efficiency in IoT- and 5G-enabled vehicle environments. Although technically diverse and comprehensive, these works do not explicitly situate localization within the context of NTN-assisted IoT, and therefore primarily offer general insights into localization technologies. In contrast, our cluster analysis reveals strong co-occurrence patterns that highlight the close relationship between localization, differential privacy, edge computing, and LoRaWAN/GPS-based smart-city applications.

2.4 Smart-City Architectures and 5G-LPWAN Integration

Works such as [20] examine the role of AI, ML, and deep reinforcement learning in enabling smart-city services, offering detailed insights into applications in intelligent transportation systems, cybersecurity, energy-efficient smart grids, UAV-assisted 5G/beyond 5G (B5G) services, and smart healthcare. The authors also outline key research challenges and future directions for advancing AI-driven urban infrastructures. Similarly, reference [21] discusses the integration of 5G and Low Power Wide Area Network (LPWAN) technologies to support ubiquitous connectivity in both urban and underserved rural environments. Their review highlights limitations of deploying these technologies in isolation and argues for hybrid architectures that enhance flexibility, reduce interference, and improve Quality of Service (QoS)/Quality of Experience (QoE). They also examine security challenges, network slicing via SDN/NFV, and propose unified 5G-LPWAN-IoT frameworks with potential extensions toward LEO satellite integration for resilient and scalable smart-city connectivity. Other complementary reviews on drones and IoT for smart cities [22,23] further emphasize the importance of secure, context-aware urban sensing infrastructures.

The study in [22] identifies advanced collaborative technologies, such as AI, IoT, robotics, and multi-agent coordination, as essential enablers for improving smart-city connectivity, energy efficiency, and quality of service. Many of their observations align with the themes captured in our Smart City cluster, thereby validating the positioning of this cluster through traditional review methods. The authors highlight that collaborative drones and IoT systems play critical roles in a wide range of smart-city applications, including transportation, communication, public safety, disaster mitigation, agriculture, weather monitoring, healthcare, and e-waste reduction. Their survey provides an overview of techniques and applications that enhance the "smartness" of smart cities through real-time collaborative drone-IoT deployments. In contrast, our work adopts a broader scope and a more novel analytical approach by using keyword co-occurrence mapping to reveal how these components relate to active security dimensions within the smart-city context.

Given the wide applicability of UAVs across military, medical, security, traffic monitoring, and surveillance domains, the authors of [23] note that substantial investment has been directed toward the development of UAV and multi-UAV systems capable of performing complex missions collaboratively and efficiently. They highlight the significant potential of 4G and 5G technologies in enabling UAVs, equipped with GPS receivers, sensors, and cameras, to deliver IoT services from the air. However, the review also identifies critical security and privacy challenges that arise in these deployments. Motivated by these gaps, the authors analyze UAV-IoT and UAV-5G applications, outline sensor and communication requirements, and discuss solutions for fleet management, privacy protection, and security enforcement in aerial networks. They

conclude by proposing an architectural framework that supports secure, collaborative UAV operations within a networked IoT environment.

These studies provide useful background that aligns with several patterns identified in this paper. They highlight the application-driven potential of UAVs and IoT in smart cities and reinforce our findings regarding the importance of security and the persistence of security challenges in this domain. However, they do not explore other critical security dimensions, such as those involving localization, edge privacy, and related intersections, that emerge clearly only through detailed keyword co-occurrence analysis and clustering, as presented in this work.

2.5 Edge/Hardware ML for Security

Sze et al. [24] review the challenges of deploying ML models on hardware-constrained IoT devices, discussing latency, privacy, and energy consumption. Their analysis spans neural accelerators, embedded platforms, and mixed-signal circuits. Given that MEC has emerged as an effective way to bring cloud-computing capabilities closer to end users, addressing challenges related to computation-intensive task offloading and latency, Yazid et al. [25] present a comprehensive review of UAV-enabled and UAV-assisted MEC architectures, highlighting their relevance for emerging IoT applications. Their survey explains how deep learning (DL) and ML techniques support UAV-based MEC by mitigating limitations related to latency, task allocation, energy consumption, and security, while also outlining the advantages, challenges, and future prospects of integrating AI into UAV-MEC systems.

Hussain et al. [26] provide an extensive study of UAV technologies with a particular emphasis on LiDAR-based 3D point-cloud compression and transmission, an important component of aerial computing and information exchange. Their review covers autonomous navigation, video-streaming challenges, QoE enhancement, and future research avenues. They further examine a wide range of UAV applications and technologies, including wireless communication protocols, routing, security mechanisms, blockchain use cases, healthcare applications, and the integration of AI, ML, DL, and IoT. The authors also discuss the foundational role of LiDAR 3D point clouds in UAV systems, their predictive modeling under mobility, and broader prospects for UAV-based solutions.

With the rapid expansion of IoT devices placing increasing pressure on terrestrial infrastructure to maintain high-quality service delivery, UAVs provide a flexible and cost-effective means of augmenting IoT networks by offering wireless access and supporting applications such as pesticide spraying, cargo transport, and video surveillance. However, the rising complexity of UAV-assisted IoT networks has created a need for advanced AI-driven scheduling and orchestration. Cheng et al. [27] address this by offering a detailed analysis of how modern AI models and architectures influence various aspects of UAV-IoT systems. Their review also identifies key challenges and outlines future directions for developing robust, scalable, and intelligent AI-assisted UAV-IoT networks. These studies offer useful precursors to several of the keyword associations identified in this paper, but they provide only a partial and fragmented view of the broader research landscape. Together, they indicate that the clusters highlighted in this work, such as security and access control, edge-computing security, blockchain mechanisms, and IDSs for IoD environments, indeed fall under the overarching domain of ML-assisted NTN-IoT security, even though prior reviews do not connect these themes in an integrated manner.

2.6 Comparative Summary of Existing Reviews

A summary of the most relevant surveys that cover portions of the research landscape mapped in this paper, and that help position this work as a blueprint for navigating key research directions, is presented in Table 1. This comparison highlights that prior studies often provide deep but narrowly scoped perspectives

or concentrate on isolated technologies within a single research domain. In contrast, this paper offers a broader coverage that integrates multiple domains under the umbrella of machine-learning-supported NTN-assisted IoT systems. In summary, existing reviews offer valuable but fragmented insights into the vast ML-driven NTN-IoT landscape, which is difficult to capture comprehensively in any single survey. Our work adopts a novel perspective by using fine-grained keyword co-occurrence analysis to reveal meaningful connections among keywords within a domain-based framework. This approach holistically maps diverse security dimensions alongside their associated applications and technologies, while systematically identifying emerging research directions and future prospects for enhancing security, privacy preservation, and localization in NTN-assisted IoT systems. It is also noteworthy that several research hotspots and clusters identified in this study extend beyond traditional security themes, highlighting the importance of localization and edge intelligence within the broader NTN-IoT ecosystem.

Table 1: Comparison of representative review studies with the present work.

Ref.	Primary Focus	Key Limitations	Relation to This Work
[3]	Internet of Drones (IoD), including authentication, privacy, blockchain, neural networks, and optimization techniques	Focuses primarily on IoD architectures; limited discussion of satellite-assisted NTN and edge intelligence	Security-related themes are reflected in Security and Access Control domain and extended here to NTNassisted IoT using bibliometric analysis
[5]	UAV communication architectures, antenna designs, ML-based path planning, and secure communication	Emphasis on UAV communication technologies; does not address NTN-wide security or satellite-edge integration	Positioned as a precursor to UAV-related security topics identified in Security and Access Control domain
[6]	Key-agreement protocols and security architectures for intelligent UAV swarms	Focused on cryptographic protocols for UAV swarms; lacks integration with IoT, edge computing, or NTN layers	Complements Security and Access Control domain by highlighting swarmsecurity challenges not explicitly mapped in NTNIoT contexts
[10]	Machine-learning-based intrusion detection systems for Internet of Drones	Relies on outdated or non-IoD-specific datasets; limited consideration of NTN constraints and satellite links	Integrated into Security and Access Control domain to contextualize IDS research within broader NTN-assisted IoT security trends

(Continued)

Table 1 (continued)

Ref.	Primary Focus	Key Limitations	Relation to This Work
[13]	Physical-layer security techniques for satellite communications	Concentrates on the physical layer; minimal discussion of higher-layer security or IoT integration	Related to Security and Access Control domain as complementary background on satellite-layer security
[15]	State-of-the-art physical-layer security for satellite-assisted IoT	PLS-centric; does not integrate localization, edge intelligence, or blockchain security	Positioned within Security and Access Control domain to highlight gaps bridged by ML-based NTN security approaches
[17]	ML-based indoor localization and fingerprinting techniques	Localization studied independently; limited focus on privacy or NTN integration	Connected to Edge Localization and Privacy domain, revealing links between localization, edge computing, and privacy
[18]	Survey of RF-, BLE-, UWB-, Wi-Fi-, ZigBee-, and GNSS-based localization methods	Primarily technology-centric; lacks NTN-assisted IoT perspective	Provides background for localization themes identified in Edge Localization and Privacy domain
[20]	AI- and ML-driven smart-city services over 5G and B5G networks	Limited attention to satellite or NTN-assisted IoT security	Mapped to smart-city and edge-intelligence themes in Edge Localization and Privacy domain
[21]	Integration of 5G and LPWAN technologies for IoT connectivity	Security and NTN integration discussed at a high level only	Supports cross-links between smart cities, LPWAN, and edge computing in Edge Localization and Privacy domain
[22]	Collaborative UAV and IoT technologies for smart-city applications	Does not explicitly address NTN or ML-driven security mechanisms	Validates smart-city UAVIoT associations revealed in Edge Localization and Privacy domain

(Continued)

Table 1 (continued)

Ref.	Primary Focus	Key Limitations	Relation to This Work
[24]	Machine learning on embedded and edge hardware platforms	No explicit NTN or satellite-assisted IoT context	Positioned within Edge Localization and Privacy domain to inform edge intelligence constraints in NTNIoT systems
[26]	LiDAR-based UAV systems, 3D point clouds, and AI-enabled applications	Broad scope; limited focus on security or NTN integration	Related to sensing and edge-processing themes intersecting with Blockchain-Enabled IoD Security domain
[27]	AI-driven scheduling and orchestration in UAV-IoT networks	Fragmented view of security across layers; no unified NTN perspective	Supports AI-assisted orchestration aspects linked to edge and security clusters
This study	**ML-enabled security, privacy, localization, and edge intelligence in NTN-assisted IoT**	**Provides an integrated bibliometric and cluster-based mapping across UAVs, satellites, edge computing, localization, and ML-driven security, offering a unified view of NTN-assistedIoT research themes.**	

3 Methodology

This paper employs a systematic methodology to provide a comprehensive overview of ML-based NTN-assisted IoT research with a focus on security-related clusters. We collect data from the Scopus database and use VOSviewer to perform keyword co-occurrence analysis, enabling the identification of research trends, influential topics, and thematic structures. Fig. 2 illustrates the multi-stage workflow adopted for data collection, cleaning, mapping, and interpretation.

3.1 Data Collection

The data for this study was gathered from the Scopus database on 4/02/2025. The search terms include

```
(TITLE-ABS-KEY("machine learning" OR "supervised learning"
OR "unsupervised learning" OR "semi-supervised learning" OR
"self-supervised learning" OR "deep learning" OR "neural networks" OR
"deep reinforcement learning" OR "drl" OR "reinforcement learning" OR
"federated learning" OR "Edge AI" OR "Edge Learning")) AND ("UAV" OR
"Unmanned Aerial Vehicles" OR "drone" OR "Aerial Platforms" OR "NTN" OR
"Non-Terrestrial Networks" OR "HAPS" OR "satellite" OR "LEO" OR "MEO"
OR GEO") AND ("IoT" OR "Internet of Things" OR "sensor networks" OR
"WSN").
```

The search yielded 3139 results, which were filtered by excluding non-English content (Chinese-31, Spanish-2, Russian-1, French-1), conference reviews (631), and retracted papers (4). This resulted in a total of 2469 entries exported to CSV format after the filtering process. All subsequent analyses are based on the results downloaded and obtained from this process.

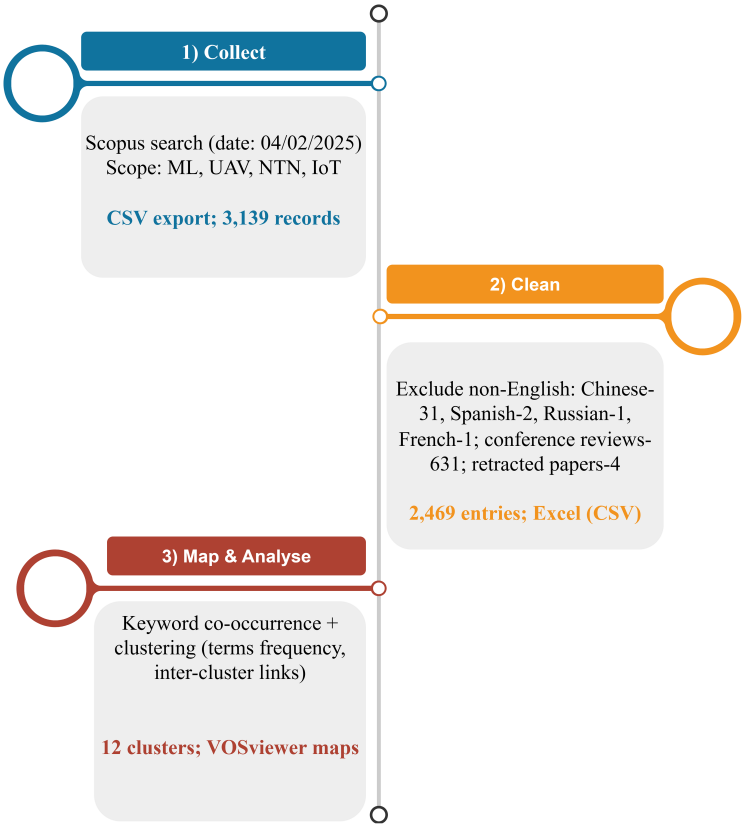

Figure 2: Three-step workflow for bibliometric data collection, cleaning, and analysis.

3.2 Keyword Extraction and Data Cleaning

The dataset comprises 25 metadata fields, including authorship information; bibliographic details (title, year, source, volume, and issue); citation metrics; identifiers (DOI and author ID); affiliations; keywords; abstracts; publication attributes; and access status (open-access indicators). Keyword extraction was performed using author-provided keywords available in the Scopus metadata.

To support data cleaning and improve visualization quality, terms with spelling variants were removed from the keyword map as shown in Table 2. Many of the excluded terms correspond to machine learning algorithms, whose interconnections are examined separately in another phase of analysis without exclusion. Important insights derived from this extended analysis are discussed in the discussion section.

For the main co-occurrence analysis, a minimum keyword occurrence threshold of five was applied. In addition, non-technical or generic terms, such as “survey,” were excluded to ensure clearer visualization and more meaningful cluster extraction.

Table 2: Sorted Term Frequency of the ML-based NTN-assisted IoT Dataset (excluded from the visualization for cleaner clustering).

Term	Freq.	Term	Freq.
Attention Mechanism	5	Edge AI	5
Graph Neural Networks	5	IoT Network	5
Machine Learning Algorithms	5	Non-Terrestrial Networks	5
Sensor Network	5	Survey	5
UAS	5	Actor-Critic	6
Fuzzy Logic	6	IIoT	6
IoT Networks	6	IoT Platform	6
Long Short Term Memory (LSTM)	6	Random Forest	6
Satellites	6	Transformer	6
DRL	7	Ensemble Learning	7
Review	7	Satellite Networks	7
UAV Networks	7	Autonomous Vehicles	8
Deep Deterministic Policy Gradient	8	Wireless Sensor Network (WSN)	8
Deep Neural Network (DNN)	9	Industrial Internet of Things (IIoT)	9
Multiagent Reinforcement Learning (MARL)	9	Satellite Communication	9
Satellite Communications	9	Support Vector Machine	9
Internet-of-Things	10	LSTM	10
Sensor	10	Artificial Neural Network	11
Satellite Internet of Things	11	Wireless Sensor Networks (WSNs)	11
Deep Neural Networks	12	Edge Intelligence	12
Artificial Neural Networks	13	Convolutional Neural Networks	14
Deep Neural Network	14	Multi-Agent Reinforcement Learning	14
Convolutional Neural Network (CNN)	16	Sensor Networks	16
Multi-Agent Deep Reinforcement Learning	17	WSN	18
Q-Learning	19	Transfer Learning	19
Convolutional Neural Network	20	Federated Learning (FL)	20
Deep Learning (DL)	22	Reinforcement Learning (RL)	22
Neural Network	23	Wireless Sensor Network	28
Neural Networks	29	Machine Learning (ML)	35
Artificial Intelligence (AI)	34	UAVs	39
Wireless Sensor Networks	44	Drone	55
Unmanned Aerial Vehicles (UAVs)	64	Drones	68
Deep Reinforcement Learning (DRL)	72	Federated Learning	81
Reinforcement Learning	111	Unmanned Aerial Vehicle	111
Unmanned Aerial Vehicles	119	Unmanned Aerial Vehicle (UAV)	143

(Continued)

Table 2 (continued)

Term	Freq.	Term	Freq.
Artificial Intelligence	146	Internet of Things (IoT)	162
Deep Reinforcement Learning	169	UAV	187
IoT	234	Deep Learning	252
Internet of Things	262	Machine Learning	366

3.3 Co-Occurrence Network Construction

The cleaned dataset was processed in VOSviewer to generate a keyword co-occurrence network as shown in Fig. 3. Considering a bibliometric mapping for datasets of this scale and the level of detail we aim to capture, a minimum occurrence threshold of five was applied. Co-occurrence strengths were computed using the full counting method, and VOSviewer's algorithm was used to form clusters.

This process yielded 12 distinct clusters representing different thematic areas in ML-based NTN-assisted IoT research. Search-related terms and outliers (e.g., "Stakelberg game") were excluded from visualization. The keywords in each cluster are provided in Figs. 4 and 5 and are extracted from images taken from VosViewer and extracted using Gemini. However, the focus of this paper is on the three focal thematic domains: Security and Access Control, Edge Localization and Privacy, and Blockchain-Enabled IoD Security which corresponds to Clusters 9–11, respectively. Other works would be dedicated to other clusters.

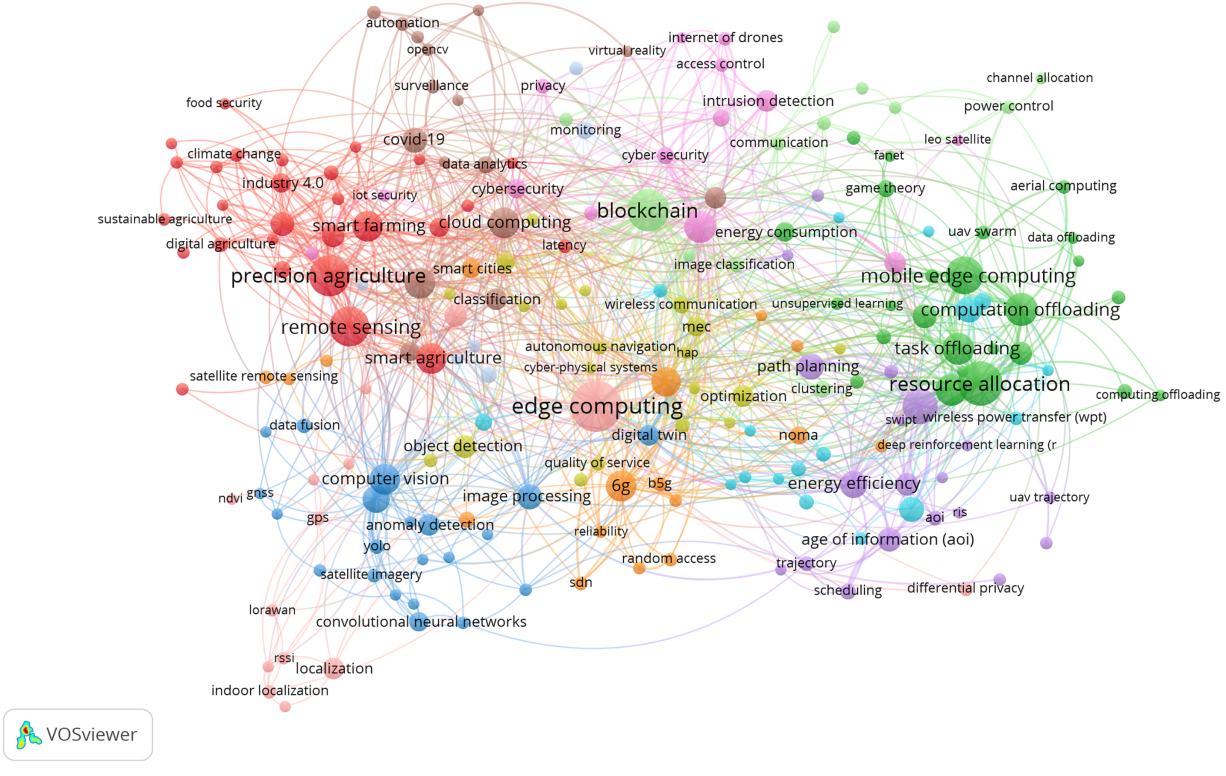

Figure 3: Visualization of the keyword co-occurrence network excluding search-related terms. The magenta, light coral, and seafoam green clusters identify the specific security themes analyzed in this paper; in-depth treatment of other thematic clusters is beyond the current scope and is addressed in separate works.

C1: Smart Agriculture

agriculture, agriculture 4.0, big data analytics, climate change, cloud, crop monitoring, decision support system, digital agriculture, digital transformation, earth observation, environmental monitoring, food security, forest fire detection, industry 4.0, IoT sensors, latency, precision agriculture, precision farming, predictive analytics, remote sensing, resource optimization, semantic segmentation, smart agriculture, smart farming, smart sensors, sustainability, sustainable agriculture, sustainable farming.

C2: Edge Resources

aerial computing, age of information, bandwidth allocation, beamforming, computation offloading, computing offloading, data offloading, energy consumption, FANET, game theory, intelligent reflecting surface, mobile edge computing, mobile-edge computing, multi-access edge computing, multi-UAV, non-orthogonal multiple access, physical layer security, power allocation, resource allocation, task offloading, trajectory design, UAV swarm, unsupervised learning, wireless networks, wireless power transfer.

C3: Visual Intelligence

anomaly detection, CNN, computer vision, convolutional neural network, data fusion, data mining, digital twin, drone identification, embedded systems, feature extraction, GNSS, image processing, industry 5.0, ML, plant disease, predictive maintenance, satellite imagery, sensor fusion, signal processing, TinyML, YOLO.

C4: Autonomous Robotics

autonomous aerial vehicles, autonomous navigation, autonomous systems, cyber-physical systems, HAP, machine vision, MEC, object detection, obstacle avoidance, optimization, pest detection, QOS, quality of service, Raspberry Pi, resource management, review, robotics, satellite communications, satellite IoT, wireless communication.

C5: UAV Optimization

age of information (AoI), AoI, collision avoidance, data acquisition, data collection, deep reinforcement learning, energy efficiency, Lyapunov optimization, mobile edge computing, offloading, path planning, RIS, satellite network, scheduling, smart grid, SWIPT, trajectory, trajectory prediction, UAV trajectory.

Figure 4: Thematic clusters and corresponding keywords for applications and UAV control, C1–C5.

C6: NextG Optimization

5G networks, blockchain technology, cognitive radio (CR), data analysis, disaster management, energy efficiency (EE), fairness, intelligent reflecting surface (RIS), joint optimization, mobile-edge computing, non-orthogonal multiple access, nonorthogonal multiple access (NOMA), reconfigurable intelligent surface (RIS), task scheduling, trajectory optimization, trajectory planning, wireless power transfer (WPT).

C7: Advanced Networks

5G, 6G, air pollution, B5G, decision tree, LORA, Markov decision process, NB-IoT, network slicing, NOMA, random access, reconfigurable intelligent surface, reliability, satellite remote sensing, SDN, smart cities, wireless communication.

C8: IoT Applications

applications, Arduino, augmented reality, automation, big data, classification, cloud computing, COVID-19, data analytics, fog computing, forest fire, healthcare, OpenCV, robots, surveillance, virtual reality.

C9: System Security

access control, authentication, cyber security, cybersecurity, data science, energy harvesting, feature selection, internet of drones, intrusion detection, intrusion detection system, IoT security, LEO satellite, privacy, security.

C10: Geo Privacy

cyber-security, data augmentation, differential privacy, distributed systems, edge computing, fingerprinting, GIS, GPS, indoor localization, localization, LoRaWAN, NDVI, RSSI, smart city.

C11: System Control

5G network, blockchain, channel allocation, clustering, communication, image classification, internet of drones (IoD), intrusion detection system (IDS), Lidar, power control, quality of service (QoS), technology.

C12: Real-time Monitoring

embedded devices, energy, forecasting, monitoring, real-time.

Figure 5: Thematic clusters and corresponding keywords for advanced networking, security, and system management, (C6–C12).

3.4 Cluster Extraction and Validation: A Novel Connectivity-Based Method

Conventional bibliometric studies often interpret clusters broadly from visual bibliometric maps. However, such interpretations are inherently subjective and may overlook the major structural interconnections within each cluster. These internal link patterns become visible only when all keyword connections are explicitly extracted, counted and their inter-relationships mapped. To address this limitation, this study introduces a *novel connectivity-driven cluster validation method* that evaluates clusters based on their intra-cluster link structure. Uniquely, we record all connections for each keyword, both within and outside the cluster. Although the discussion focuses primarily on the dominant keywords in each cluster, this project is, to the best of our knowledge, the first attempt to formalize cluster validation using intra-cluster degree as an objective criterion for identifying representative keywords.

For each cluster, we extracted: (1) the occurrences of every keyword (as obtained from VOSviewer), and (2) the *intra-cluster degree*, defined as the number of direct links a keyword has to other keywords within the same cluster. Keywords that scored highly inter-cluster degree were designated as *anchor keywords*. These anchor terms occupy the most connected regions of the cluster's co-occurrence network and thus serve as the most reliable indicators of the cluster's conceptual focus.

Cluster interpretation and labeling were therefore guided primarily by these anchor keywords rather than subjective visual inspection. This connectivity-based validation procedure reduces interpretive bias, enhances reproducibility, and grounds thematic labeling directly in the structural properties of the bibliometric network. It also ensures that cluster labels reflect research areas most strongly supported by empirical co-occurrence patterns. Notably, security-related themes appear most prominently in the first cluster, followed by the second and third. As such, *the Security and Access Control, Edge Localization and Privacy, and Blockchain-Enabled IoD Security domains* were selected for detailed analysis because they exhibit the strongest thematic alignment with this study's scope, namely security, privacy, edge intelligence, and localization.

3.5 Interpretation and Thematic Mapping

In the final stage, thematic labeling was conducted by examining anchor keywords together with their strongest intra- and inter-cluster linkages. This structural perspective enabled the construction of an integrated thematic map that connects ML-driven security, privacy preservation, intrusion detection, localization, GPS/LoRaWAN positioning, edge computing, and satellite/UAV intelligence across the NTN-IoT ecosystem. In this regard, the most intra-connected keywords and their linkages are provided in Tables 3–5, respectively.

This combined bibliometric-thematic methodology provides a rigorous framework for analyzing research landscapes and represents an advancement over purely narrative reviews by grounding interpretations in quantitative network structure.

Table 3: Keyword connections across Clusters.

SN	Keyword	Internal Connections	External Connections
Security and Access Control: Top connected keywords and their connections			
1	**Authentication**	Internet of drones, access control, privacy, security	Monitoring, blockchain, security, 5G network, privacy

(Continued)

Table 3 (continued)

SN	Keyword	Internal Connections	External Connections
2	**Cybersecurity**	Privacy, intrusion detection, security, IDS; feature selection, security, IoT security	Communication, unsupervised learning, fog computing, wireless communication, 5G, digital twin, 6G, smart agriculture, big data, Agriculture 4.0, technology, monitoring; Smart farming, precision farming, big data, smart cities, 6G, 5G, digital twin, 5G network, blockchain
3	**Energy Harvesting**	LEO satellite, SWIPT, security	Energy efficiency, internet of drones, QoS, power control, game theory, MEC, computation offloading, task offloading, resource allocation, WPT, trajectory optimization, RIS, NOMA, resource management, optimization, HAP, wireless communication, energy consumption, security, blockchain, IoT sensors
4	**Feature Selection**	Intrusion detection, internet of drones, cybersecurity, IDS, security	Wireless network, data analysis, classification, smart city, smart farming
5	**IDS**	Cybersecurity, security, feature selection, internet of drones	Blockchain technology, autonomous navigation, smart agriculture, Agriculture 4.0
7	**Internet of Drones**	Authentication, access control, intrusion detection, feature selection, IDS	Blockchain
8	**Intrusion Detection**	Internet of drones, privacy, LEO satellite, security, feature selection, cybersecurity	Blockchain, smart grid, smart city, big data, smart farming, precision agriculture
9	**IoT Security**	Cybersecurity, data science	Edge computing
10	**Privacy**	Authentication, intrusion detection, cybersecurity, security	Big data, cloud computing, edge computing, blockchain

(Continued)

Table 3 (continued)

SN	Keyword	Internal Connections	External Connections
11	**Security**	Internet of drones, access control, feature selection, intrusion detection, privacy, cybersecurity, energy harvesting, authentication	Internet of drones, communication, aerial computing, data offloading, game theory, resource allocation, data collection, clustering, NOMA, energy efficiency, 5G network, wireless communication, MEC, HAP, QoS, satellite communication, 6G, reliability, SDN, edge computing, 5G, smart city, cloud computing, data analytics, automation, monitoring, IDS, blockchain, blockchain technology

Table 4: Keyword connections across Clusters.

SN	Keyword	Internal Connections	External Connections
Edge Localization and Privacy: Top connected keywords and their connections			
1	**Edge Computing**	GPS, LoRaWAN, fingerprinting, indoor localization, differential privacy, distributed system	MEC, 5G network, wireless communication, autonomous system, smart city, smart agriculture, computer vision, CNN, tinyML, image processing, embedded systems, sensor fusion, reliability, 6G, network slicing, joint optimization, UAV trajectory, AoI, energy efficiency, RIS, computing offloading, resource allocation, path planning, task offloading, computation offloading, game theory, energy consumption, fog computing, blockchain, access control, privacy, forest fire, data analytics, Covid-19, robotics, cloud, IoT security, smart farming, climate change, forest fire detection, big data, CPS, NOMA, security, environmental monitoring, WPT, trajectory planning, autonomous systems, satellite communication, review
2	**Fingerprinting**	Indoor localization, localization, LoRaWAN, GPS, edge computing, RSSI	CNN
3	**GPS**	NDVI, cybersecurity, GIS, LoRaWAN, RSSI, edge computing, fingerprinting	Big data, remote sensing, Raspberry Pi, disaster management, image processing
4	**Indoor Localization**	Data augmentation, RSSI, fingerprinting, LoRaWAN, edge computing	CNN
5	**LoRaWAN**	GPS, fingerprinting, indoor localization, edge computing	Computer vision, anomaly detection

(Continued)

Table 4 (continued)

SN	Keyword	Internal Connections	External Connections
6	**RSSI**	Indoor localization, fingerprinting, GPS	6G
7	**Smart City**	GIS, cybersecurity, distributed systems, edge computing	Covid-19, application, data analytics, big data, Industry 4.0, energy, computer vision, image processing, autonomous navigation, security, blockchain, feature selection, intrusion detection

Table 5: Keyword connections across Clusters.

SN	Keyword	Internal Connections	External Connections
Blockchain-Enabled IoD Security: Top connected keywords and their connections			
1	5G	QoS, communication	
2	Blockchain	IDS, IoD, Technology	Augmented reality, robot, virtual reality, COVID-19, data analytics, cloud computing, big data, healthcare, automation, environmental monitoring, industry 4.0, crop monitoring, agriculture, resource optimization, smart farming, precision farming, remote sensing, cloud, smart city, smart cities, IoT sensors, cybersecurity, robotics, energy, edge computing, LoRa, reliability, SDN, random access, network slicing, digital twin, 5G, MEC, wireless communication, 5G network, mobile edge computing, energy efficiency, NOMA, RIS, differential privacy, resource allocation, computation offloading, MEC, game theory, satellite network, intrusion detection, IDS, image classification, monitoring
3	Channel allocation	Power control	
4	Clustering	Blockchain, image classification	Security, task offloading, data collection, AoI, NOMA
5	Communication	5G Network, Technology	MEC, Task offloading, path planning, wireless communication, 5G, Autonomous navigation, security, cybersecurity, monitoring, smart farming
6	Image classification	Internet of Drones, Lidar, clustering, blockchain	Remote sensing
7	Internet of Drones (IoD)	Intrusion detection systems, QoS, power control, blockchain, image classification	Computation offloading, Energy harvesting, energy consumption, fog computing, security, smart cities

(Continued)

Table 5 (continued)

SN	Keyword	Internal Connections	External Connections
8	Intrusion detection system (IDS)	Internet of Drones, Blockchain	
9	LIDAR	Image classification, big data	
10	Power control	Channel allocation, QoS, Internet of Drones	Fog Computing, energy harvesting, computation offloading, trajectory design, fairness
11	QoS (Quality of Service)	5G Network, power control, Internet of Drones	Fog computing, Energy harvesting, Computation offloading
12	Technology	Communication, Blockchain	Cybersecurity, Covid-19, Big data analytics, big data

4 Thematic Clusters and Key Findings

This section introduces the thematic clusters derived from the VOSviewer-based bibliometric analysis and briefly discusses their contributions, interconnections, and emerging directions. The goal is to provide the reader with an overview of what to expect in the main sections of this paper and a broad outline of the thematic landscape surrounding ML-supported NTN–IoT security research. In total, twelve clusters were identified after uploading the entire NTN–IoT dataset described in the methodology section. These clusters reflect diverse aspects of ML-enabled NTN-assisted IoT, spanning security and privacy, enabling technologies, agricultural applications, edge intelligence, and UAV-assisted communication. However, given the breadth of this thematic space, a comprehensive discussion on all keywords in the selected clusters would significantly increase the length of this paper. Similarly an indepth analysis and review of all clusters is beyond the scope of a single paper. Therefore, this study focuses on most connected keywords on representative clusters that capture key directions of interest: security and privacy (Security and Access Control), edge intelligence and smart-city integration (Edge Localization and Privacy), and blockchain and intrusion detection systems for IoDs (Blockchain-Enabled IoD Security).

Based on the new connectivity-driven cluster validation method introduced in Section 3, cluster interpretation in this section is guided by anchor keywords—those exhibiting high intra-cluster connectivity. These anchor terms represent conceptually central themes within each cluster and motivate the deeper thematic exploration presented in subsequent sections.

4.1 Security and Access Control

The Security and Access Control domain comprises 14 keywords primarily related to access control and security. These include *access control, authentication, cybersecurity*[1]*, data science, energy harvesting, feature selection, internet of drones, intrusion detection, intrusion detection system, IoT security, LEO satellite, privacy*, and *security*.

The concentration of these keywords indicates that security is a central concern in NTN-assisted IoT applications, particularly those involving drones and LEO satellites. Within this context, data science and machine learning play a key role in strengthening cybersecurity through mechanisms such as access control,

[1]which includes both cybersecurity and cyber security

authentication, intrusion detection, and privacy preservation. These approaches are essential for ensuring trustworthy IoT operations and resilient communication in heterogeneous and resource-constrained NTN environments.

Based on the keyword analysis shown in Table 6, *security* (8 connections), *cybersecurity* (7 connections) and *intrusion detection* (6 connections), and emerge as the top three security-related terms with the highest number of intra-cluster links. In fact, the two most connected terms are *security* and *intrusion detection*, while *cybersecurity* shares the same level of connectivity as "internet of drones" and "feature selection." Together, these three terms form the conceptual backbone of the cluster, and their high intra-cluster connectivity indicates that they represent central themes within ML-driven NTN–IoT security research.

Table 6: Security and Access Control: Keyword statistics.

Keyword	# Connected	Occ.
Security	8	40
Cybersecurity*	7	27
Intrusion detection	6	19
Feature selection	5	11
Internet of drones	5	8
Intrusion Detection System	4	8
Privacy	4	9
Authentication	4	5
Energy harvesting	3	19

Note: Cybersecurity* combines cyber security and cybersecurity keywords.

Intrusion detection and cybersecurity solutions are particularly crucial across UAV-based systems such as the Internet of Drones (IoD), as well as satellite-assisted IoT and sensor networks. The prominence of "internet of drones" among the highly connected keywords underscores the vulnerability of such platforms to cybersecurity threats. This observation aligns with findings in the literature, which highlight the importance of intrusion detection systems (IDS) for IoD environments and emphasize the need to address security challenges in drone-assisted IoT ecosystems.

The cluster also reveals a strong association with *energy harvesting*, reflecting a growing research trend toward secure, energy-aware, and sustainable IoT solutions. In NTN-supported systems, including UAVs and satellites, machine learning is increasingly leveraged to optimize resource-constrained devices while meeting stringent security requirements.

4.2 Edge Localization and Privacy

The Edge Localization and Privacy domain comprises 14 keywords related to the technologies and applications of machine learning, as well as supporting hardware components. These include *cybersecurity, data augmentation, differential privacy, distributed systems, edge computing, fingerprinting, GIS, GPS, indoor localization, localization, LoRaWAN, NDVI, RSSI*, and *smart city*.

This cluster highlights the role of data augmentation in improving localization tasks and the use of wireless technologies such as LoRaWAN for NTN-enabled localization. A notable link is observed between indoor localization and edge computing, reflecting the need to offload computationally intensive localization processes to edge devices. The role of GPS in supporting both outdoor and indoor positioning is also evident.

Applications of ML-based NTN-assisted IoT in cybersecurity within smart-city environments are also represented in this cluster. The combination of the normalized difference vegetation index (NDVI), which measures vegetation health from satellite imagery, and GPS indicates the integration of remote sensing for environmental monitoring. Additionally, the relationship between RSSI and indoor localization suggests alternative positioning approaches where GPS signals are unavailable.

As shown in Table 7, the anchor keywords of this cluster, *edge computing*, *GPS*, and *smart city*, highlight its central focus: enabling secure, privacy-aware, and efficient localization within intelligent urban environments. The prominence of *differential privacy* and *distributed systems* suggests that privacy-preserving machine learning on resource-constrained edge devices is a major research direction, particularly for location-sensitive IoT deployments using LoRaWAN. Furthermore, the presence of *RSSI*, *fingerprinting*, and *LoRaWAN* indicates that RSSI-based fingerprinting constitutes a promising localization technique in LoRaWAN networks, especially when supported by aerial or satellite infrastructures and optimized through machine-learning models. Together, these themes underscore the relevance of robust localization for terrestrial IoT and smart-city applications.

Table 7: Edge Localization and Privacy: Keyword statistics.

Keyword	# Connected	Occ.
Edge computing	6	98
GPS	6	8
Fingerprinting	6	5
Indoor localization	5	7
LoRaWAN	4	6
RSSI	3	6
Smart city	3	20

4.3 Blockchain-Enabled IoD Security

The Blockchain-Enabled IoD Security domain consists of 12 keywords representing a combination of security mechanisms, image intelligence, communication optimization, and Internet of Drones (IoD) operations. These include *blockchain, image classification, Internet of Drones (IoD), intrusion detection system (IDS), power control, QoS, clustering, LiDAR, communication, channel allocation, 5G network*, and *technology*. The relationships between these terms highlight how machine learning, secure communication, and performance optimization intersect within NTN-assisted IoT systems. Based on the connectivity-based validation approach introduced in Section 3, Table 8 shows that *Internet of Drones (IoD)*, *image classification*, and *blockchain* emerge as anchor keywords due to their strong intra-cluster connectivity. This suggests that the cluster revolves around secure communication in distributed IoD networks, machine-learning approaches for image classification using aerial or LiDAR images captured by drones, as well as other communication-oriented solutions. Interconnections among the keywords further point to research topics such as QoS optimization and power-control mechanisms for IoD communications.

Table 8: Blockchain-Enabled IoD Security: Keyword statistics.

Keyword	# Connected	Occ.
Blockchain	3	67
Image classification	4	7

(Continued)

Table 8 (continued)

Keyword	# Connected	Occ.
Power control	3	8
Quality of service (QoS)	3	6
Technology	2	8
Clustering	2	12
Internet of drones (IoD)	5	8
Communication	2	
Lidar	2	6
Channel allocation	1	5
5G Network	2	6
Intrusion detection system (IDS)	2	6

Blockchain appears as a fundamental security mechanism for distributed systems and can support IoD applications by ensuring data integrity. It may also complement intrusion detection systems to enhance security in aerial networks. The presence of *image classification* highlights the importance of aerial imagery collected by UAVs, along with imagery provided by other NTN entities such as satellites.

Terms such as *IoD*, *IDS*, *power control*, and *QoS* indicate the importance of reliable and secure IoD communication. Effective channel allocation and power-control techniques are essential for improving QoS in NTN-supported IoT systems.

Collectively, these clusters illustrate three major security-focused research areas within the NTN-IoT landscape. In particular, they indicate that current research efforts revolve around addressing cybersecurity challenges such as intrusion detection, privacy preservation, authentication, security of edge devices, and blockchain-based trust management, especially in IoD-enabled systems. These clusters therefore highlight the principal research directions in machine-learning-assisted, NTN-supported IoT for security enhancement. Further details on these domains are provided in the subsequent sections.

5 Security, Privacy, and Access Control in NTN-Assisted IoT Systems

Fig. 6 illustrates the keyword distribution for this domain based on keywords with the highest intra-cluster connections. The prevalence of *security*-related terms shows that security is a central concern in NTN-assisted IoT applications, particularly in drone- and satellite-enabled systems. The cluster highlights the integration of machine learning and data science for tasks such as access control, authentication, intrusion detection, and privacy protection, which are essential for maintaining trust and resilience in distributed IoT architectures. Fig. 7 shows the top 10 connected keywords in this cluster and their connected keywords within the same cluster.

Fig. 8 presents a hierarchical framework illustrating how ML and FL are orchestrated across multi-tier NTNs to support secure and privacy-preserving IoT applications. The framework is organized into four primary layers: the Ground IoT Tier, the UAV Tier, the LEO Tier, and the GEO Tier. Each tier plays a distinct yet interconnected role in the overall learning and orchestration pipeline.

In the Ground IoT Tier, distributed IoT devices, such as smart cameras, vehicles, sensors, and meters, independently train local ML models using their private data. To preserve user privacy, local model updates (gradients) are encrypted and obfuscated through mechanisms such as differential privacy and

homomorphic encryption before being transmitted to upper tiers. These encrypted local updates are then uploaded to the UAV Tier, which serves as the first level of aggregation.

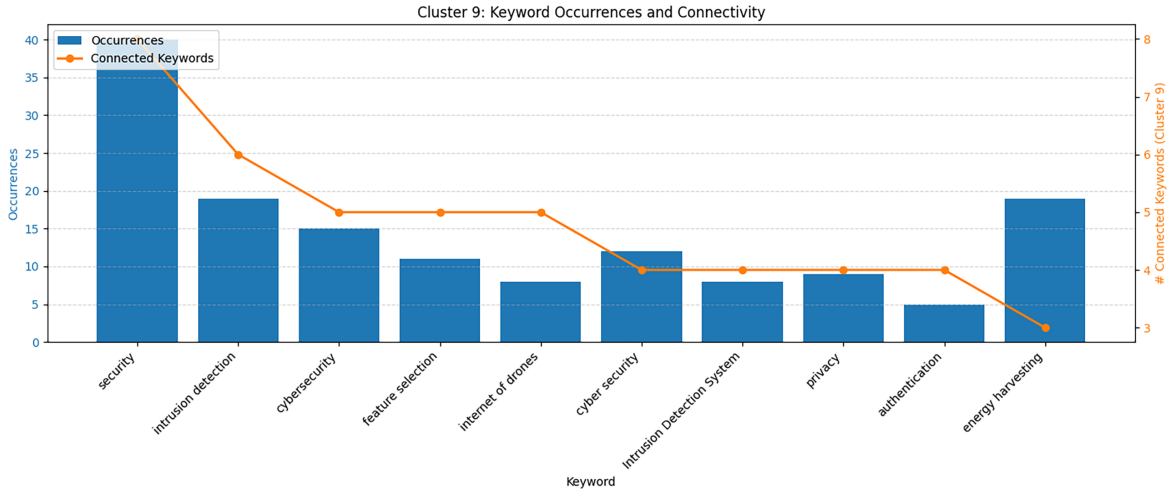

Figure 6: Security and Access Control: Keyword distribution and connectivity.

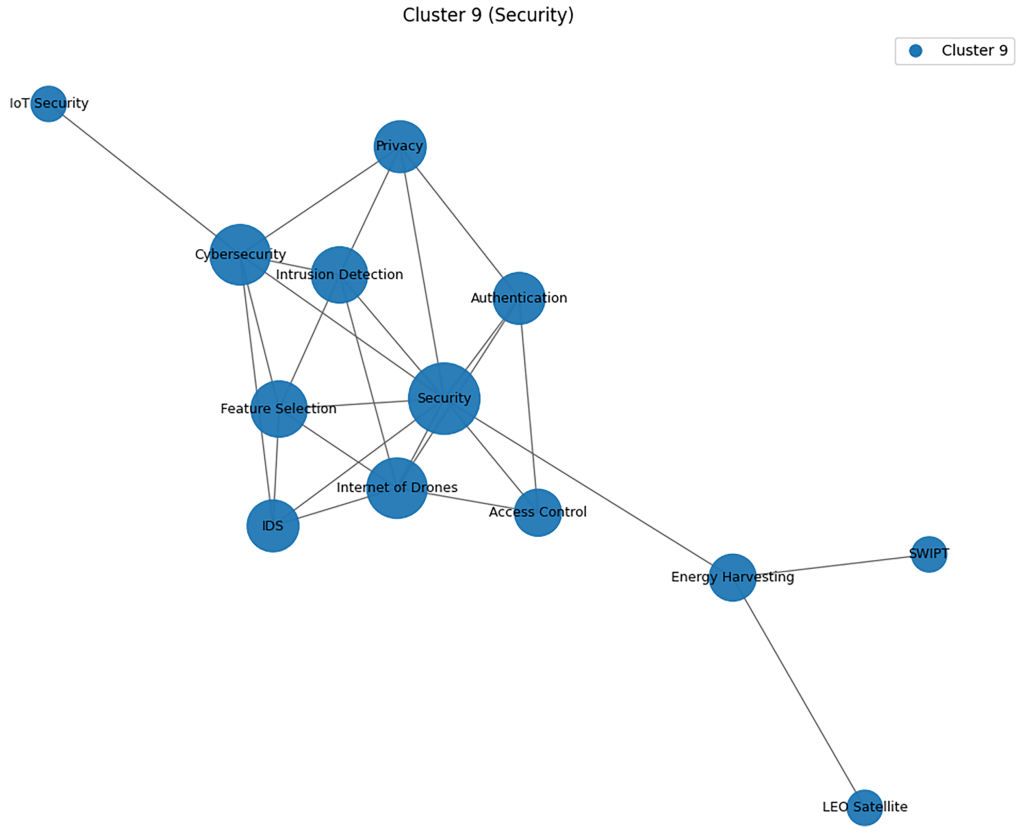

Figure 7: Network-based mapping of the top ten most connected keywords Security and Access Control, illustrating their intra-cluster relationships.

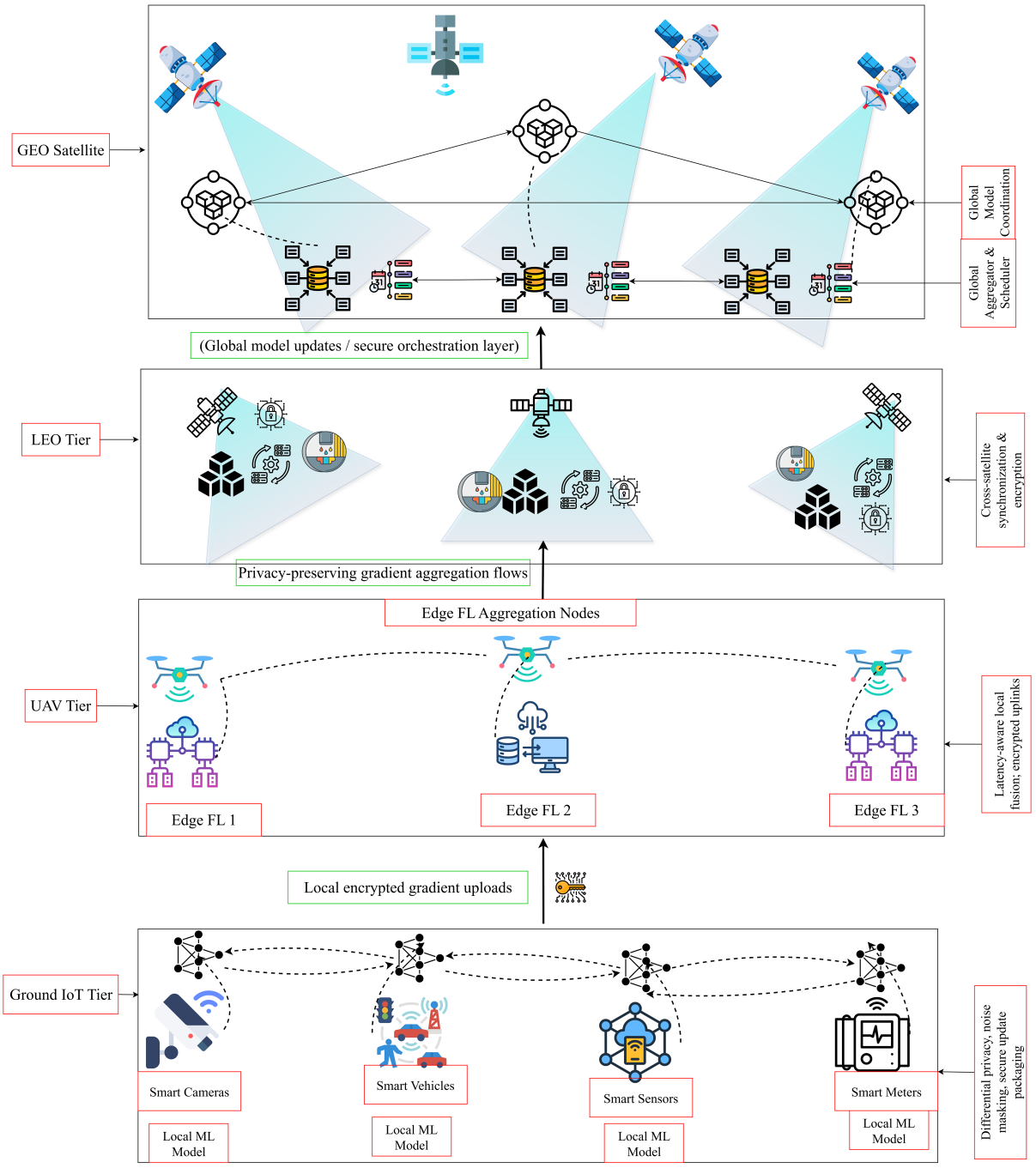

Figure 8: Hierarchical FL orchestration across NTN tiers.

The UAV Tier functions as an *edge FL aggregation node*. Here, unmanned aerial vehicles collect encrypted gradients from multiple IoT clusters and perform intermediate aggregation to reduce bandwidth usage and communication overhead. This intermediate processing also allows latency-sensitive applications, such as smart city monitoring or precision agriculture, to benefit from near-real-time learning updates. The aggregated results are securely transmitted to the LEO satellites for further processing.

In the LEO Tier, satellites serve as regional coordinators that aggregate updates from multiple UAV clusters. This layer employs privacy-preserving gradient aggregation flows and cross-satellite synchronization to ensure model consistency across distributed segments of the network. The LEO tier thus enables scalable coordination between multiple UAV and ground networks while maintaining strict privacy guarantees.

At the top of the hierarchy, the GEO Satellite Tier operates as a global orchestrator, integrating aggregated gradients received from LEO satellites to update the global ML model. This global model is then disseminated back through the hierarchy to lower tiers, LEO satellites, UAVs, and IoT devices, enabling continuous model improvement and adaptive intelligence throughout the NTN-IoT ecosystem. The GEO tier also ensures global synchronization and stakeholder coordination within the secure orchestration layer.

Overall, Fig. 8 demonstrates how FL-based NTN architectures can achieve end-to-end security, scalability, and privacy preservation by distributing learning tasks across spatially separated layers. This hierarchical structure minimizes communication bottlenecks, improves robustness against single-point failures, and aligns with the emerging paradigm of secure and intelligent NTN-assisted IoT systems discussed in Sections 5 and 6.

5.1 Security and Privacy in NTN-Assisted IoT Networks

The Security and Access Control domain is primarily centered on *security and privacy* within NTN-assisted IoT architectures. The keyword *security* exhibits the highest number of connections, emphasizing the need to protect data, communications, and system integrity. Strongly associated concepts include *intrusion detection*, *cybersecurity*, *privacy*, *authentication*, and *feature selection*, reflecting multiple layers of IoT protection. The inclusion of *Internet of Drones (IoD)*, *LEO satellites*, and *energy harvesting* demonstrates that security in NTN systems extends across physical, architectural, and algorithmic dimensions.

5.2 Security and Its Interconnections

Within the cluster, *security* connects closely with *Internet of Drones*, *access control*, *feature selection*, *intrusion detection*, *privacy*, *cybersecurity*, *authentication*, and *energy harvesting*. These links illustrate how security spans architectural (IoD), algorithmic (feature selection, intrusion detection), and operational (access control, authentication) aspects. Externally, it connects with a broad range of technologies, including *blockchain*, *cloud/edge computing*, *5G/6G*, *NOMA*, *MEC*, and *smart city* systems, indicating its foundational importance. Game theory, SDN, and data analytics further contribute to secure and optimized NTN-IoT designs.

5.2.1 Access Control and Authentication

Access control, a critical component for preventing unauthorized access, is linked internally to *authentication* and *IoD*, and externally to *blockchain*, *monitoring*, *edge computing*, and *5G networks*. These associations underscore its importance in drone and edge-based deployments that operate in dynamic and latency-sensitive environments. Similarly, *authentication* is strongly related to *privacy* and *security*, reinforcing the need for robust identity management in mission-critical IoT scenarios such as surveillance, healthcare, and precision agriculture.

5.2.2 Cybersecurity and Intrusion Detection

Cybersecurity and *intrusion detection* are central to safeguarding NTN-IoT networks from internal and external threats. *Cybersecurity* is closely associated with *privacy*, *intrusion detection*, and *IDS*, and externally connected to technologies such as *5G/6G*, *fog computing*, *digital twins*, and *smart agriculture*. These

relationships highlight the need to secure communication, synchronization, and analytics in next-generation IoT environments. *Intrusion detection* is strongly linked internally to *IoD*, *LEO satellites*, *privacy*, *feature selection*, and *cybersecurity*, while its external ties to *smart cities*, *smart grids*, and *blockchain* reveal its essential role in maintaining data trustworthiness and resilience across large-scale networks.

5.2.3 Privacy and Feature Selection

Privacy is a recurrent theme, with strong connections to *authentication*, *intrusion detection*, and *cybersecurity*. External links to *big data*, *cloud computing*, *edge computing*, and *blockchain* underscore the ongoing need for privacy-preserving computation in hybrid processing environments. *Feature selection*, often used in ML-based intrusion detection and anomaly detection systems, connects internally to *IDS*, *IoD*, and *cybersecurity*, and externally to *wireless networks*, *smart cities*, and *smart farming*, indicating its value for both data-driven security and application-specific optimization.

5.2.4 Internet of Drones and LEO Satellites

The *IoD* is a key architectural element in this cluster, linked to *authentication*, *access control*, *intrusion detection*, *feature selection*, and *IDS*. Its external connection to *blockchain* suggests decentralized approaches to secure drone coordination and communication. Similarly, *LEO satellites* connect to *intrusion detection* and *energy harvesting*, with external links to *computation offloading*, highlighting their dual function as secure relays and processing nodes in NTN-IoT systems.

5.2.5 Energy Harvesting and Secure System Design

Energy harvesting (EH) is connected internally to *LEO satellites*, *security*, and *SWIPT* (Simultaneous Wireless Information and Power Transfer), and externally to *energy efficiency*, *resource allocation*, *trajectory optimization*, and technologies like *RIS*, *WPT*, and *blockchain*. These interconnections emphasize that security and energy efficiency are interdependent in mobile and distributed IoT environments, particularly in airborne and space-based platforms where power availability is limited. EH is also studied alongside *NOMA* and *MEC*, which enable scalable and energy-aware NTN-IoT architectures.

Overall, this cluster shows that machine learning can play a significant role in authentication, intrusion detection, access control, and privacy preservation in integrated NTN-IoT networks, including NTN-assisted IoT systems. In particular, ML techniques are relevant for IoD and other drone architectures, as well as LEO-satellite-assisted IoT networks. The findings also indicate that, in addition to security guarantees, meeting QoS requirements and ensuring energy efficiency are vital aspects of NTN-IoT systems, areas where machine learning can also make a substantial impact.

6 Edge Computing, Localization, and Privacy in NTN-Assisted IoT Systems

Fig. 9 illustrates the keyword distribution for this domain based on keywords with the highest intra-cluster connections. The keywords are related to machine learning applications, hardware technologies, localization mechanisms, and privacy-preserving approaches in NTN-assisted IoT environments, especially for smart cities.

6.1 Edge Computing and Localization in NTN-Assisted IoT

The Edge Localization and Privacy domain centers on the integration of *edge computing*, *localization technologies*, and *privacy mechanisms* in distributed IoT networks. The dominant keyword, *edge computing*,

exhibits the highest connectivity, underlining its central role in enabling decentralized, real-time, and energy-efficient data processing. Closely linked keywords such as *GPS*, *fingerprinting*, *indoor localization*, *LoRaWAN*, and *RSSI* emphasize the importance of lightweight, low-latency edge platforms for accurate positioning and sensing in resource-constrained environments. Fig. 10 shows the top 10 connected keywords in this cluster and their connected keywords within the same cluster.

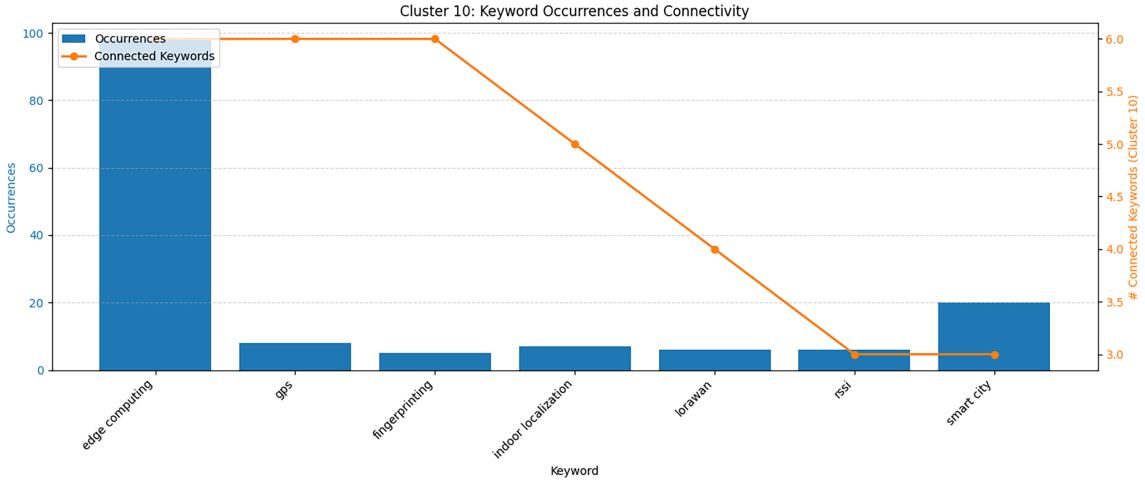

Figure 9: Edge Localization and Privacy: Keyword distribution and connectivity.

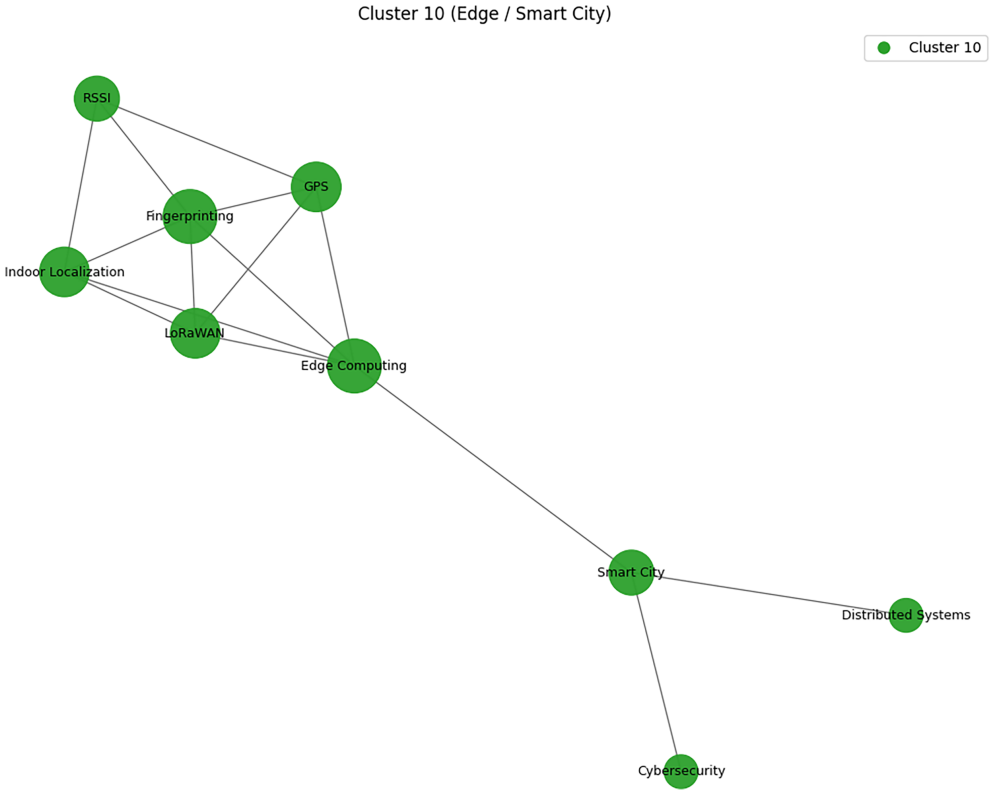

Figure 10: Network-based mapping of the top ten most connected keywords in Edge Localization and Privacy, illustrating their intra-cluster relationships.

Using the intra-cluster connectivity-based validation approach described in Section 3, and as shown in Fig. 9, edge computing emerges as the most central keyword in this cluster. This is followed by GPS, fingerprinting, and indoor localization, with LoRaWAN appearing next, and RSSI and smart city showing comparable levels of connectivity. In terms of intra-cluster connectivity, this ranking is based on the number of linked or connected nodes each keyword has within the same cluster. This pattern reflects traditional terrestrial IoT localization research, which frequently relies on RSSI, LoRaWAN, and GPS, as demonstrated in studies such as RSSI-based fingerprint localization in LoRaWAN networks using CNNs [28] and SNR/RSSI-based indoor localization using optimized machine-learning models [29]. Reviews such as [30] further recognize this as a well-established domain. Within the NTN-focused context of this cluster, the mapping highlights edge computing, localization, and their security implications for IoT-enabled smart cities as its thematic core.

6.2 Edge Computing as a Core Enabler

Edge computing connects internally with *GPS*, *LoRaWAN*, *fingerprinting*, *indoor localization*, *differential privacy*, and *distributed systems*. These connections highlight its pivotal role in supporting privacy-aware, low-latency computation for time-critical IoT tasks. Externally, it is associated with technologies and applications such as *MEC*, *5G/6G*, *autonomous systems*, *image processing*, *tinyML*, *RIS*, *blockchain*, and *fog computing*. This breadth of connections underscores the foundational role of edge computing in real-time analytics and ML-driven decision-making across NTN-assisted IoT domains.

Fingerprinting-based indoor localization using RSS is widely studied due to its simplicity and low deployment cost. Deep learning has further strengthened interest in this area because of its strong feature-extraction capabilities and its ability to automate the classification of RSS fingerprints. However, repeatedly training deep learning models on large volumes of RSS data in cloud environments presents important challenges. First, RSS fingerprinting datasets often contain sensitive user information, raising significant privacy concerns when transmitted to or stored in untrusted cloud servers. Second, sending such data to remote cloud infrastructure can introduce non-negligible transmission delays, which is detrimental for real-time localization. To address these limitations, differentially private learning models deployed at the edge have emerged as a promising alternative. By leveraging edge-computing-enabled federated learning and lightweight CNN-based localization architectures, these approaches can improve localization accuracy, reduce communication delays, and protect users' privacy during both the offline training phase and the online localization process [31]. Edge computing is therefore well positioned as a key enabler of low-latency, privacy-preserving intelligence across NTN-enabled IoT and smart-city applications.

6.2.1 Privacy and Differential Privacy

Differential privacy appears as a key enabler of privacy preservation in this cluster. Internally linked with *edge computing* and externally connected to *blockchain* and *computation offloading*, it reflects growing interest in protecting sensitive data processed at the edge. Such techniques are critical for applications involving personal or environmental data, such as healthcare monitoring, disaster response, and smart city management, where data utility and privacy must coexist.

The co-occurrence between differential privacy, localization, and edge processing highlights a growing focus on privacy-preserving approaches to RSS-based indoor localization, where federated and edge-based deep learning models operate without exposing raw RSS data, thereby reducing transmission delays and mitigating privacy risks as shown in [31].

6.2.2 Localization Technologies

Localization forms another major theme, represented by *GPS*, *indoor localization*, *fingerprinting*, and *RSSI*. *GPS* connects internally to *LoRaWAN*, *RSSI*, *fingerprinting*, and *edge computing*, while externally it links to *NDVI*, *GIS*, *cybersecurity*, and *remote sensing*. The strong link structure around *GPS* and *indoor localization* highlights the importance of improving security in indoor localization leveraging on GPS technologies in NTN assisted LoRAWAN based IoT as well as the significance of RSSI-based finger print localization leveraging on machine learning technologies.

Edge computing is a promising approach for delivering real-time services and addressing location-privacy challenges by deploying differentially private location-based services directly on edge nodes [32]. Overall, this cluster underscores how edge intelligence contributes to location privacy in NTN-assisted LoRaWAN IoT and smart-city systems, particularly as diverse positioning technologies and privacy-aware computation increasingly converge.

7 Blockchain-Enabled IoD Security for Aerial Image Classification and IDS for Internet of Drones and Service Quality

The Blockchain-Enabled IoD Security domain consists of 12 keywords, as presented according to their keyword distribution and connectivity in Fig. 11. These keywords include: *5g network, blockchain, channel allocation, clustering, communication, image classification, internet of drones (iod), intrusion detection system (ids), lidar, power control, quality of service (qos), technology*. Blockchain technology has been studied for intrusion detection systems as well as Internet of Drones applications. Similarly, quality of service is one of the main concerns and metrics considered in 5G, as shown in the visualization due to the connection between both keywords. Fig. 12 shows the top 10 connected keywords in this cluster and their connected keywords within the same cluster.

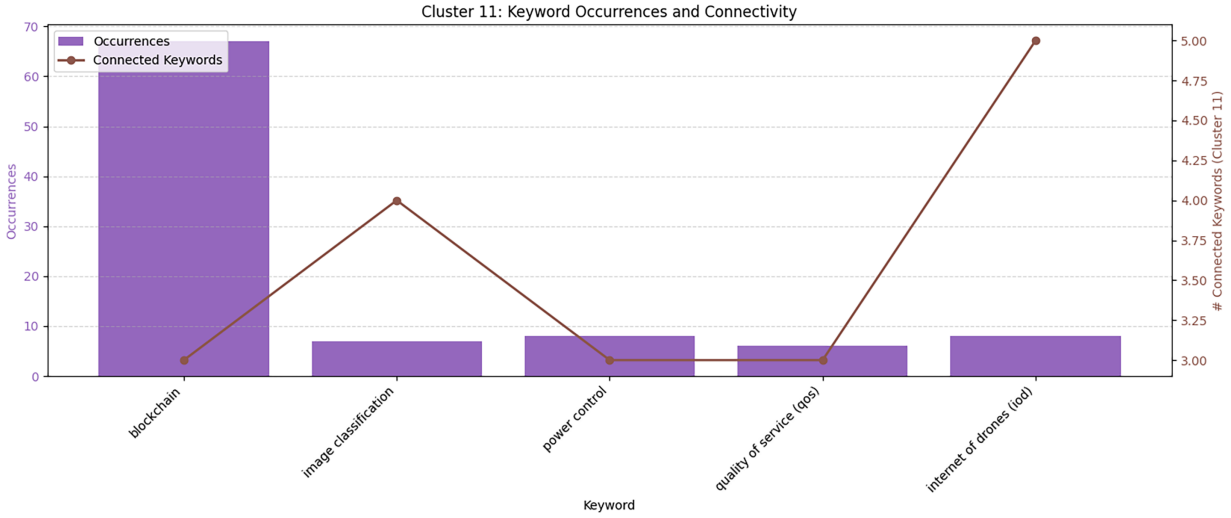

Figure 11: Keyword Statistics for Blockchain-Enabled IoD Security Keywords.

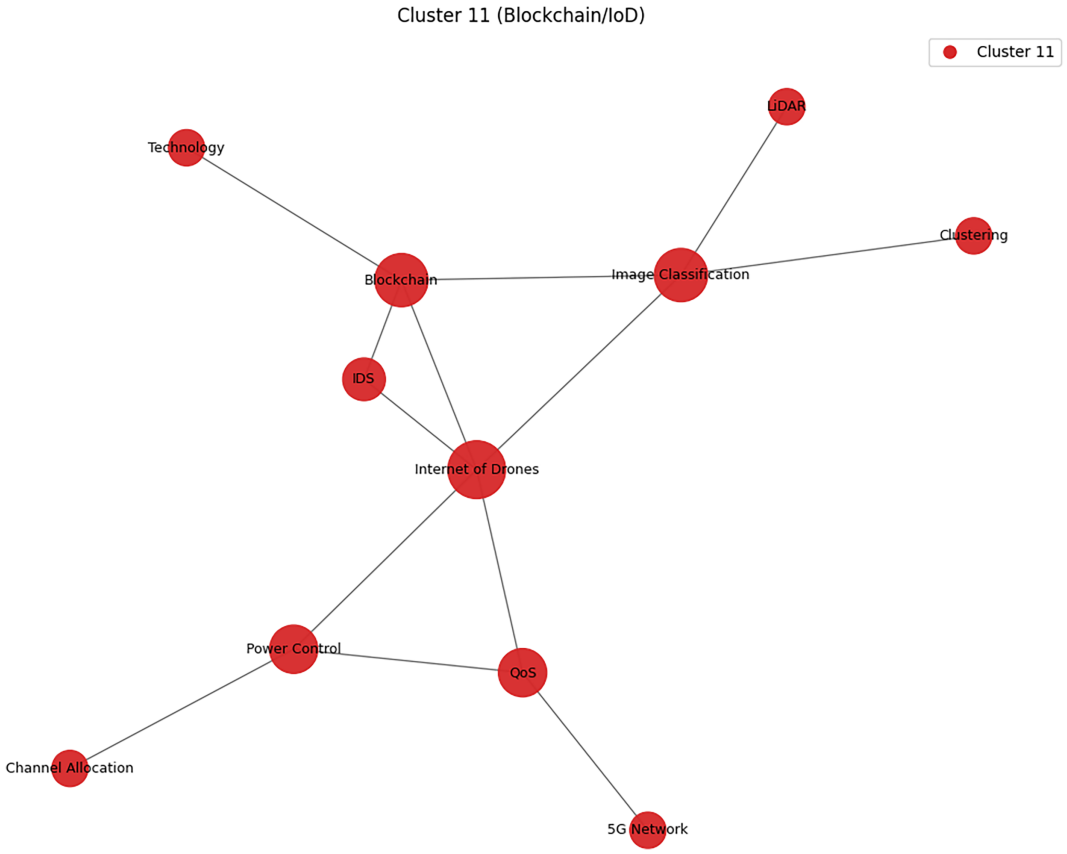

Figure 12: Network-based mapping of the top ten most connected keywords in Blockchain-Enabled IoD Security (Blockchain, Internet of Drones, and QoS), illustrating their intra-cluster relationships.

In addition, channel allocation is often studied with power control. The clustering technique appears with blockchain and image classification, showing the importance of clustering using ML algorithms for image classification in NTN-assisted IoT applications, as well as the integration of blockchain within this architecture. Similarly, QoS is not only studied for 5G but also in the context of power control and the Internet of Drones. The use of ML for image classification is vital in NTN-assisted IoT, with techniques such as clustering and technologies such as lidar, blockchain, and the internet of drones framework, as observed from the relationship between these keywords. Moreover, blockchain is used both within the IoD and IDS frameworks. As for the Internet of Drones, this relates to intrusion detection systems, quality of service, power control, and image classification, showing some of its applications, requirements, and the role of machine learning in its applications (image classification).

Based on these statistics, it is evident that Image classification and Internet of Drones are fundamental keywords within this domain. The high link strength of blockchain is mainly due to the large number of keywords it is connected to within other clusters.

7.1 Internet of Drones

Internet of Drones (IoD) is linked to Intrusion detection systems, QoS, power control, blockchain, and image classification within the same cluster. Particularly, the keywords connected to Internet of Drones are indicative of the need for security mechanisms, interference control in IoD scenarios, as well as achieving the quality of service expectations. The link between internet of drones and image classification also shows

the research interest in the intersection between both keywords. Internet of Drones (IoD) is also linked to Computation offloading, Energy harvesting, energy consumption, fog computing, security, and smart cities in other clusters. This indicates paradigms such as computation offloading (in edge computing), security, energy harvesting, security are all major research directions in IoD applications. Similarly, smart cities are one of the most prominent internet of drones applications. Intrusion detection system (IDS) is linked to the Internet of Drones, and Blockchain within the same cluster, all indicating the importance of IDS in Internet of Drones applications.

7.2 Image Classification

Image classification is linked to Internet of Drones, Lidar, clustering, and blockchain in the same cluster, and Remote sensing in a different cluster. These links show that Lidar and image classification play a vital role in NTN-assisted IoT applications. LIDAR is linked to Image classification and big data within the same cluster. In addition, clustering is vital in image classification for NTN-assisted IoT applications. Similarly, blockchain can play a vital role in supporting image classification as well as Internet of Drones technology, as Blockchain is linked to IDS, IoD, and Technology within the same cluster. Clustering is linked to Blockchain, and image classification within the same cluster. Clustering is also linked to Security, task offloading, data collection, AoI, and NOMA all in other clusters.

7.3 Blockchain and Applications

Blockchain is one of the most linked keywords in the literature on NTN-assisted IoT from the research dataset studied in this paper. Its link with other clusters is versatile as it is also linked to Augmented reality, robot, virtual reality, COVID-19, data analytics, cloud computing, big data, healthcare, automation, environmental monitoring, industry 4.0, crop monitoring, agriculture, resource optimization, smart farming, precision farming, remote sensing, cloud, smart city, smart cities, IoT sensors, cybersecurity, robotics, energy, edge computing, LoRa, reliability, SDN, random access, network slicing, digital twin, 5G, MEC, wireless communication, 5G network, mobile edge computing, energy efficiency, NOMA, RIS, differential privacy, resource allocation, computation offloading, MEC, game theory, satellite network, intrusion detection, IDS, image classification, and monitoring in other clusters.

Notably, all these indicate several applications of Blockchain in NTN-assisted IoT such as Crop monitoring, smart farming, precision farming, environmental monitoring, smart city, smart cities, intrusion detection (IDS), image classification. Also, some of the technologies where Blockchain has also been deployed such as Augmented reality, virtual reality, cloud computing, edge computing, mobile edge computing (MEC), 5G, 5G network, wireless communication, IoT sensors, LoRa, robotics, robot, satellite network, digital twin. In addition, Blockchain is linked to concepts, techniques and approaches Automation, data analytics, big data, resource optimization, resource allocation, computation offloading, reliability, random access, network slicing, differential privacy, game theory, NOMA, RIS, SDN, energy efficiency. In addition, technical research objectives studied in blockchain-enabled architecture can also be observed.

7.4 Communication, Related Aspects and Technologies

Communication is linked to 5G Network, and Technology within the same cluster. On the other hand, Technology is linked to Communication, and Blockchain in the same cluster as well as Cybersecurity, Covid-19, Big Data Analytics, and Big Data in other clusters. Similarly, communication is linked to MEC, Task offloading, path planning, wireless communication, 5G, Autonomous navigation, security, cybersecurity, monitoring, and smart farming in other clusters. 5G is linked QoS, and communication within the same cluster. Channel allocation is linked to Power control within the same cluster. Power control is connected

to Channel allocation, QoS, and Internet of Drones within the same cluster. Power control is also linked to Fog Computing, energy harvesting, computation offloading, trajectory design, and fairness in other clusters. QoS (Quality of Service) is linked to 5G Network, power control, and Internet of Drones within the same cluster. Quality of service is also linked to Fog computing, Energy harvesting, and Computation offloading in other clusters.

8 Highlights of Research Linked to Selected Keywords

Based on the thematic clusters identified in the preceding section, the existing body of research on ML-based NTN-assisted IoT proves to be a diverse yet interconnected field that spans multiple subdomains. Each cluster represents a focal area of research, with evolving research patterns. As such, examining the literature through these thematic groupings provides a mapping of research priorities and the level of integration between different areas and technologies.

8.1 Machine Learning-Based Security Approaches for IoT-Assisted UAV Networks

Numerous studies have explored ML and DL approaches to enhance security across IoT-assisted UAV networks and related IoT systems. AI-enabled cybersecurity models have also been developed for satellite systems, such as the satellite-protection framework proposed by Thach [33]. A significant body of work focuses on combining DL or DRL with meta-heuristic optimization to strengthen UAV-IoT security. For example, Babu et al. [34] developed a DRL-based security model enhanced by a modified marine predators algorithm, while Alotaibi et al. [35] integrated deep learning with an adaptive mongoose optimization strategy to further improve UAV network resilience.

Machine learning is also applied to access control in IoD environments. Perumalla et al. [36] modeled access control using oppositional aquila optimization and ML, whereas Aftab et al. [19] proposed a hybrid access-control system that supports secure vehicular localization in IoT- and 5G-enabled settings. In IoD communication security, Al-Wesabi et al. [37] introduced an oppositional poor-and-rich optimization technique combined with DL to ensure secure drone communications.

Intrusion detection remains a central theme in securing UAV-IoT networks. Al-Fuwaiers et al. [38] analyzed ML-based intrusion-detection systems for drone-IoT architectures, while Uhongora et al. [39] proposed a DL-based IDS for SDN-enabled space systems. Wu et al. [40] demonstrated a lightweight ML IDS suitable for UAVs with strict resource constraints, and Alissa et al. [41] developed a deep autoencoder-based IDS using crystal instruction optimization for secure IoD environments.

Beyond standalone ML methods, there is growing interest in integrating ML with distributed and trust-enhancing technologies such as blockchain, while Islam et al. [42] introduced a blockchain-integrated federated learning framework to secure drone-IoT data aggregation.

Despite these advancements, deploying ML models on UAV and IoT hardware poses challenges related to energy consumption, memory limits, and privacy, motivating a shift toward edge-based and lightweight security solutions [24]. RF fingerprinting can also support identity verification, although inherent channel variability makes secure implementation difficult. Overall, security requirements for UAV-IoT systems, spanning intrusion detection, access control, identity management, and encrypted communication, are increasingly addressed through ML, optimized path planning, and cryptographic techniques, reinforcing the importance of robust security within modern NTN-assisted UAV communication frameworks [5].

8.2 Edge Computing, Localization, and Privacy

Several studies have explored the integration of AI, IoT, and UAVs to enhance security in various systems, including those focused on cyber threats, illegal activities, and network optimization.

Security plays a critical role in edge-computing-assisted localization and communication in smart-city UAV-IoT systems. In computation offloading, Wei et al. [43] demonstrated that privacy-aware DRL techniques can support efficient UAV-assisted edge processing while mitigating preference leakage. AI-based security mechanisms have also been widely explored to protect UAV and IoT systems from cyber-physical attacks, including GPS spoofing and network intrusions [44,45]. Privacy-preserving security architectures for small drone networks have further been investigated within 6G-IoT cyber-physical systems [46]. AI-enabled UAV-IoT frameworks have additionally been applied to monitoring and detection applications, such as preventing unauthorized or illegal activities using intelligent sensing and aerial surveillance [47].

Privacy concerns associated with ML hardware deployment motivate a preference for local (edge-based) intelligence over centralized cloud processing [24], reinforcing the relevance of privacy-aware security solutions in smart UAV ecosystems. To this end, blockchain and federated learning have been identified as promising enablers for secure and decentralized collaboration in drone-IoT networks [42], with implications for both communication security and localization services.

Deep learning also plays an important role in UAV-assisted localization, where learning-based methods can improve positioning accuracy and energy efficiency. Several studies have explored DL-enabled localization in UAV-assisted WSNs and IoT networks [48,49], while recent work has incorporated UAVs with reconfigurable intelligent surfaces to further enhance localization performance in energy-constrained environments [50]. Fingerprinting-based approaches have been widely adopted for indoor localization in GPS-denied environments; however, they involve inherent trade-offs among accuracy, latency, complexity, and energy consumption [17]. Beyond localization, RF fingerprinting has also been applied to secure UAV-based IoT authentication and access control [19,51].

In smart-city IoT ecosystems, Drones-as-a-Service (DaaS) frameworks integrating 5G connectivity and blockchain technologies have emerged as a flexible deployment model [52]. More broadly, ML- and DL-based security frameworks have been applied across diverse domains, including smart agriculture, smart grids, surveillance systems, and fog/edge-enabled infrastructures [4,53]. Particularly, reference [53] investigates how artificial intelligence, deep learnin,g and machine learning support smart city automation. AI-driven UAV systems have also been investigated for healthcare, mobility, and disaster-response applications [20,54,55]. Particularly, reference [54] discusses the role of AI and how it will affect transportation and smart cities with attention to smart mobility and autonomous vehicles. Finally, edge AI combined with encryption and lightweight security mechanisms has been shown to enhance secure UAV communications under stringent latency and resource constraints [5].

Machine-learning-based optimization techniques further contribute to cybersecurity in UAV-assisted IoT networks [34,56]. In parallel, AI-driven predictive models have been explored to estimate optimal signal strength and connectivity conditions for drones supporting IoT services in smart cities [57].

8.3 Security and Service Quality in Aerial Image Classification and Internet of Drones

Studies have explored a broad set of communication, machine learning, and security techniques to advance UAV-assisted and satellite-based IoT networks. In the domain of communication enhancement, Meng et al. [58] demonstrated that UAVs equipped with cylindrical array antennas and deep learning-based attitude estimation can act as mobile base stations and deliver reliable mmWave communication by enabling accurate beam alignment. For satellite IoT, Liu et al. [59] and Zhao et al. [60] developed deep reinforcement

learning (DRL) methods for dynamic and energy-efficient channel allocation, significantly reducing latency and energy usage in LEO satellite networks. Xu et al. [61] incorporated UAVs and reconfigurable intelligent surfaces (RIS) to mitigate wireless channel blockages in industrial IoT, proposing deep learning-based centralized and distributed algorithms that optimize transmit power, channel allocation, and RIS coefficients for green communication. Addressing real-world application needs, Othman and Aydin [62] designed a UAV-assisted social distancing monitoring system that uses computer vision and IoT technologies for real-time public health enforcement.

Security and privacy have also been central themes in UAV-IoT and satellite-IoT research. Uddin and Kumar [63] introduced SDN-based federated learning frameworks to protect satellite IoT communication from cyberattacks, incorporating traffic regulation and privacy-preserving learning. Building on secure data aggregation, Islam et al. [42] proposed a blockchain-integrated federated learning scheme with multi-stage authentication and differential privacy for drone-based IoT, while Tong et al. [64] developed a blockchain-assisted hierarchical federated learning framework to ensure trustworthy model aggregation and efficient UAV-assisted IoT operation. Beyond data privacy, blockchain-enabled resource and task management systems have emerged: Seid et al. [65] used a multi-agent DRL model and Stackelberg game formulation to optimize UAV-assisted computation offloading and energy harvesting, whereas Abegaz et al. [66] integrated MADRL with blockchain-based dynamic pricing to support secure and efficient IIoT resource trading.

Federated learning continues to be widely adopted for resource management and system optimization. Yang et al. [67] applied federated reinforcement learning to hypergraph-based wireless resource allocation in dense UAV-IoT networks, while Gad et al. [68] and Gad et al. [69] proposed communication-efficient FL frameworks for UAV trajectory optimization and rural health monitoring using LoRa and knowledge distillation. Federated learning has also been used for power- and energy-conscious applications, such as energy maximization in solar-powered UAV networks [70].

Reinforcement learning, particularly DRL and multi-agent DRL, has been employed for joint communication and control tasks across diverse UAV and satellite IoT scenarios. Examples include trajectory and user association optimization using POMDP-MADDPG models [71], multi-step DDQN for integrated sensing and communications (ISAC) [72], blockchain-incentivized secure data collection using DRL [73], communication scheduling for UAV swarms [74], and DRL-LSTM models for adaptive satellite channel allocation [75]. Additional applications include RIS-assisted UAV communication for energy-efficient IIoT networks [76] and DL-based UAV clustering for RSSI-based target tracking [77]. Together, these studies illustrate the growing reliance on learning-driven, secure, and adaptive communication frameworks across UAV-assisted and satellite IoT environments.

9 Discussion and Research Outlook, and Case studies

This section discusses the key issues from the preceding analysis, providing context for the interrelationships among central keywords. Also, it reinforces the thematic patterns identified in the three clusters (Clusters 9, 10, and 11). This section presents practical deployment examples drawn from real-world systems where elements of these themes have been investigated or implemented. While some of these case studies do not explicitly address security, the integration of security mechanisms is clearly feasible and actionable.

9.1 Discussion and Research Outlook

In this section, further context is provided from some of the patterns identified in the previous sections for all three clusters based on research done in literature.

9.1.1 Security and Intrusion Detection in UAV and NTN-IoT Systems

Efficient simulation of IDSs is crucial for NTN-IoT, particularly in satellite-integrated networks. This is because such simulations can generate large volumes of adversarial samples, which are valuable for evaluating the robustness of various classifiers. These insights can guide engineers in selecting the most effective classifiers for ensemble IDSs. Additionally, adversarial training can enhance detection performance due to the self-learning capabilities of IDSs when exposed to adversarial attacks. However, conventional adversarial attack methods often suffer from low success rates and impose high computational and communication overheads. These challenges are exacerbated by the limited computing resources and long communication delays in satellite-terrestrial integrated networks. Therefore, it is essential to develop robust and efficient evaluation schemes that minimize interaction between satellite and terrestrial nodes while maintaining effective adversarial attack simulations. Such simulations should also be lightweight to ensure compatibility with resource-constrained ensemble IDSs [78].

IoD refers to a decentralized network framework that facilitates drone access to controlled airspace and enables inter-location navigation services. This connectivity is largely powered by the IoT, which supports communication and coordination between drones. However, due to its reliance on IoT infrastructure, the IoD is inherently vulnerable to various security and privacy threats. Ensuring the security and privacy of IoD networks is critical for the reliable execution of drone-based applications. This requires serious attention to threat mitigation through the development of effective security mechanisms. In particular, it is important to propose robust countermeasures against potential attacks, along with a comprehensive performance evaluation of these techniques to assess their effectiveness [79].

IoT offers numerous benefits for drone navigation, especially in small-drone technology driven by recent advancements. IoT enables inter-location services that enhance navigation capabilities in these drones. However, due to their design and architecture, drones remain vulnerable to privacy and security threats. Establishing a secure and reliable network is therefore crucial to ensure optimal drone performance. To address these challenges, it is essential to enhance current small-drone architectures, particularly those used in civil and defense applications, to meet growing demands for safety, privacy, and security. Achieving secure communication in IoD systems requires techniques that prevent intrusions and interceptions. This involves proposing intelligent frameworks that integrate machine learning models for threat detection and mitigation within IoT-assisted drone environments. Such approaches can significantly improve adaptability and cybersecurity, making them valuable for use in cyber-physical satellite systems and IoT-enabled aerial vehicles [80].

Satellite communication plays a critical role in modern telecommunications by enabling global connectivity and addressing the limitations of terrestrial networks. In satellite-enabled NTNs, authentication is especially important for securing communication, particularly in LEO systems. The integration of terrestrial and non-terrestrial components in vertical heterogeneous networks introduces unique security challenges. Therefore, it is essential to thoroughly examine these challenges and understand the complexities of authentication mechanisms to develop robust and sustainable security solutions for space-ground communications, as explored in [81].

UAVs are increasingly used in smart cities for tasks such as surveillance, monitoring, and data collection. While these applications are promising, they raise significant concerns related to security and privacy. To address these challenges, it is essential to develop privacy-preserving intrusion detection and prevention mechanisms for UAVs and the broader Internet of UAVs (IoUAV) ecosystem. Ensuring the confidentiality and integrity of UAV data is critical. To that end, modern machine learning and artificial intelligence techniques, such as federated learning, secure multi-party computation, and differential privacy, are being explored. Additionally, deep neural networks, including CNN-LSTM architectures, can facilitate real-time

anomaly detection for accurate threat identification. To strengthen UAV security further, real-time decision-making systems capable of triggering alerts and initiating automatic blacklisting are crucial. Multi-factor authentication (MFA) can also enhance access control within UAV-based intrusion detection systems, making them more resilient to evolving cyber threats [82].

The integration of UAVs with satellite and 5G technologies offers significant benefits, particularly in extending high-quality and stable connectivity to remote and underserved areas. However, as UAV systems grow in scale and complexity, they are increasingly becoming targets for cyberattacks, largely due to their inherently weak security infrastructure. To address these risks, it is essential to develop robust security models that leverage ML to detect vulnerabilities and cyber threats. ML algorithms can be employed for intrusion detection and deployed at both satellite and terrestrial gateways to monitor and classify network traffic. By identifying malicious packets in real time, these models can significantly enhance the security of UAV-based networks [83].

9.1.2 Localization and Privacy in IoT and UAV Networks

Location information is essential in the IoT era. While outdoor localization has seen major improvements thanks to satellite technologies, these signals are often inadequate for complex indoor environments, making indoor localization a persistent challenge. Recently, Wi-Fi fingerprinting combined with deep learning has gained attention for indoor localization in multistorey buildings due to its cost-effectiveness and reasonable accuracy. However, implementing such solutions on resource-constrained IoT devices requires efficient preprocessing techniques to reduce computational demands. This approach investigates the use of publicly available Wi-Fi fingerprinting datasets to compare different preprocessing methods combined with Convolutional Neural Networks (CNNs) for floor-level localization in an edge computing setting. Notably, the authors report over 94% floor-level localization accuracy, a 15% improvement on the UJIIndoorLoc dataset, by adjusting the received signal strength indicator (RSSI) for non-detected access points and applying min-max normalization. These results highlight the strong potential for deploying accurate and efficient indoor localization systems on low-power IoT devices, enabling advances in applications such as healthcare, industrial automation, robotics, and smart city infrastructure [84].

Outdoor LoRa gateways play a critical role in dense urban environments characterized by tall buildings, narrow streets, commercial complexes, heavy vehicle activity, and significant interference. These conditions pose unique challenges to LoRaWAN networks, particularly in non-line-of-sight (NLOS) scenarios. To ensure reliable coverage and performance, it is important to optimize key metrics such as Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR) across different spreading factors. Deploying efficient gateways with appropriate hardware specifications and antenna configurations is essential, as these factors directly influence network reliability and range. Ideally, gateways should maintain stable RSSI and minimal SNR degradation at both short and long distances. Higher antenna gain, for instance, can lead to better range performance, making the selection of gateway hardware especially critical in urban deployments. Additionally, strategic placement and proper planning are key to optimizing LoRaWAN performance in dense settings. These optimizations are particularly important in smart city and industrial automation applications, where consistent and reliable data transmission is vital [85].

Security and privacy are fundamental in today's digital world, particularly for real-time applications involving internet-connected devices such as smartphones, tablets, and laptops. These devices are often vulnerable to cyberattacks, making it easier for attackers to gain access to sensitive and confidential data belonging to individuals or organizations. As technology rapidly advances, applications like drone-based deliveries and mobile hotspot provisioning are expected to become more widespread, especially in smart city environments. However, the increasing reliance on drones and connected devices also introduces new

security risks, including threats like GPS spoofing and authentication attacks, which can lead to the leakage of sensitive information. To address these risks, smart devices increasingly rely on embedded systems-on-chip (SoCs) that are designed to manage large volumes of user data efficiently. These systems must balance the limited capabilities of edge hardware with the computational demands of advanced machine-learning models. Therefore, improving the security of edge devices at scale is crucial for the development of secure and resilient smart cities. Recent research has proposed methodologies leveraging blockchain technology and environmental sensing (e.g., temperature, light) to enhance the security of smart devices [86]. Securing edge computing systems is essential for protecting user privacy and ensuring that smart city infrastructures remain resilient against cyberattacks.

Energy efficiency and network lifetime are critical considerations in IoT localization, especially for power-constrained end nodes. Traditional localization systems such as GPS, Galileo, and GLONASS are often unsuitable for IoT applications due to their high power consumption. To address this, LoRaWAN has gained significant attention for its low power requirements and wide coverage. Conventional localization approaches typically rely on estimating the distance between end nodes and anchor nodes using a path loss model combined with the Received Signal Strength Indicator (RSSI). However, this method is vulnerable to inaccuracies caused by transmission effects such as interference, which can distort RSSI readings. To improve accuracy under these constraints, it is essential to develop novel distance estimation techniques based on robust empirical data. One such approach involves comparing the probability density functions (PDFs) of RSSI values obtained from controlled measurement campaigns with those observed in real deployments [87].

Explainable AI (XAI) plays a crucial role in enhancing transparency and trust in AI-powered UAV systems, particularly in smart city applications where safety and accountability are essential. Traditional machine learning models often function as "black boxes," making their decision-making processes difficult to interpret, especially problematic in high-stakes environments. UAV navigation systems have evolved from conventional methods like GPS and inertial navigation to more sophisticated AI- and ML-driven techniques. While monocular vision-based navigation offers a cost-effective and lightweight alternative, it suffers from limitations such as restricted fields of view and depth perception ambiguities.

Integrating XAI into these vision-based frameworks can significantly improve their interpretability and reliability. This is particularly important for critical UAV functions like obstacle detection, path planning, and collision avoidance, capabilities that are vital in dynamic urban environments with traffic congestion, infrastructure changes, and environmental monitoring needs. XAI-enhanced UAVs are also promising for decision-critical scenarios such as disaster response and urban planning, where clear reasoning behind autonomous decisions is necessary. To push the frontier further, researchers should explore the integration of vision models with Large Language Models (LLMs), which could enhance situational awareness and autonomous decision-making. Ultimately, incorporating XAI into UAV systems not only boosts performance but also ensures transparency and adaptability, essential qualities for the next generation of smart city technologies cities [88].

Real-time applications aimed at determining the exact location of sensor nodes in specific areas have gained significant attention. Developing innovative methods for efficiently localizing unknown nodes is therefore essential. In this context, FPGA-enhanced edge-computing UAVs are particularly effective, especially when their trajectory is known and represented through multiple anchor positions. Equipped with GPS systems, these UAVs gather positional data from sensor nodes as they move through the environment. To estimate the location of unknown nodes, the UAV collects hop count information, indicating the number of communication steps from each node, and inputs it into a localization algorithm. The onboard FPGA enables real-time processing of sensory data, allowing the UAV to make fast and accurate decisions in dynamic environments [89]. Furthermore, efficient localization algorithms remain critical for mobile WSNs.

9.1.3 Secure and Intelligent Frameworks for the Internet of Drones

Although the IoD is increasingly used in both civilian and military applications, critical challenges, particularly in secure communication, remain. These challenges are most evident during communication with ground control stations or when drones act as mobile aerial access points. Among these concerns, security and privacy stand out as key issues that must be effectively addressed. Blockchain technology emerges as a promising solution due to its decentralized architecture, immutability, and the traceability it provides for transactions. A blockchain-based secure framework can enhance data management within IoD systems and help resist various security threats in IoT-enabled IoD environments. Therefore, it is essential to propose frameworks that not only offer robust security and functional capabilities but also minimize communication and computation overhead [90].

IoD spans a wide range of applications that are increasingly relevant across academia, industry, and public management. Key areas of deployment include civilian and military operations, aerial photography, and smart city surveillance. In addition, IoD plays a significant role in supporting technologies such as WSNs, mobile computing, and cloud/fog computing frameworks. It also integrates with modern paradigms like blockchain, security authentication, and privacy protection, making it a central enabler of secure and intelligent systems [3].

Recent breakthroughs in the IoT and drone technology have revolutionized key domains such as remote operations, remote sensing, and automation. Drones have gained widespread popularity in IoT applications, particularly for remote monitoring and task automation. This surge in interest has given rise to a promising business model known as Drones-as-a-Service (DaaS), which offers commercial drone deployment on demand. The growing demand is largely due to drones' ease of deployment, flexibility of operation, and risk-free functioning. To capitalize on this momentum, it is essential to understand the current research landscape, considering drone capabilities, drone types, and deployment architectures. Research must also explore the integration of intelligent systems and enhancements in drone communication architectures using advanced technologies such as blockchain. Furthermore, understanding the diverse communication protocols (e.g., WiFi, LTE, 5G, and satellite) and their integration into broader systems is crucial, especially for applications in smart cities and precision agriculture. Finally, it is imperative to examine the growing number of security challenges and cyber-attacks that drones face and to evaluate the countermeasures proposed in recent literature [52].

Drones within the IoD ecosystem are increasingly vulnerable to security and privacy threats due to limitations in their current architecture and communication design. Ensuring reliable and secure communication is essential for maintaining optimal drone performance and mitigating cyberattacks. Recent studies have shown that incorporating intelligent machine learning models into the design and structure of IoT-aided drones can facilitate adaptable and secure technologies to counter cybersecurity threats [80].

With the evolution of 5G technology, use cases requiring high data rates, low latency, and scalable, flexible architectures to enhance Quality of Experience (QoE) are expected to grow significantly. Among these, the IoT stands out, with expanding applications in domains such as smart factories, smart agriculture, and smart cities. However, the limitations of terrestrial networks, particularly in terms of coverage, scalability, and infrastructure, continue to hinder seamless IoT deployment. Additionally, the IoT ecosystem comprises a wide range of solutions, short- and long-range, standardized and commercialized, built on different communication protocols and access infrastructures. This diversity presents considerable challenges for their integration into the 5G framework. To fully realize the potential of 5G-enabled IoT, it is essential to assess and align existing and emerging IoT standards with 5G infrastructure. In this context, the deployment of satellites and UAVs emerges as a promising direction for overcoming terrestrial limitations, such as incomplete coverage and the increasing density of IoT devices [91].

The rapid increase in drone applications underscores the need to address critical privacy and security challenges, including those related to flight boundary enforcement, data collection in public and private spaces, and the secure storage and dissemination of sensitive information. These challenges highlight the requirement for drones to communicate and store data securely, even over potentially untrusted or insecure channels. In response, there is a growing need to develop robust surveillance models tailored for the IoD. Such models should ensure secure and reliable communication between drones and ground stations, while mitigating a wide range of cyber and physical attacks. For instance, surveillance drones are particularly vulnerable to physical capture attacks, where attackers may gain unauthorized access to stored data or ongoing sessions. Therefore, implementing effective countermeasures against such threats is essential to ensure the security and integrity of IoD systems [92].

Although IoD applications have gained a measure of public acceptance, significant security and safety concerns, particularly those affecting human life, remain unresolved. IDSs in IoD environments face numerous challenges due to the dynamic and decentralized network architecture, particularly in achieving a balance between detection accuracy and computational efficiency. To enhance the performance of IoD networks, recent research has proposed a blockchain-based radial basis function neural network (RBFNN) model, aimed at improving data integrity and secure storage for intelligent decision-making across drone architectures. Blockchain facilitates decentralized predictive analytics and supports the distributed application of deep learning methods within the IoD ecosystem. These models present a promising solution for developing effective classifiers that operate within the resource-constrained environments typical of intrusion detection in drone networks [93].

The authors [10] present a systematic literature review of machine learning-based IDS for the IoD. Their study highlights a wide variety of ML algorithms applied to intrusion detection, with hybrid and deep learning models being the most commonly used. Additionally, meta-heuristic algorithms are often employed for feature selection and parameter tuning to enhance model interpretability, reduce overfitting, shorten training times, and improve overall performance. Below, we provide some of their findings and recommendations [10]:

- Python is the most frequently used implementation language. However, real-world testing and validation remain crucial to ensure the practical applicability of these IDS solutions. Model performance is typically evaluated using metrics such as accuracy, precision, recall, and F1-score. Despite this, many solutions fail to consider IoD-specific constraints such as limited computational capacity, energy consumption, mobility, resource constraints, and the need for real-time detection.
- Most studies rely on multi-class classification to identify specific attack types, but this approach demands significant computational resources and processing time. While binary classification offers less granularity, it is more efficient and better suited for resource-constrained drones. Striking a balance between these approaches is key to optimizing performance.
- The authors also note that commonly used datasets, such as NSL-KDD, KDDCup 99, CICIDS2017, and UNSW-NB15, are outdated, often imbalanced, and lack coverage of IoD-specific scenarios. This underscores the need to curate and deploy newer, larger, and more specialized labeled datasets.
- Key challenges in implementing ML-based IDS in IoD include high latency in real-time detection, limited onboard resources, and issues with scalability in complex and dynamic networks. Furthermore, dataset scarcity, adversarial attacks, and the lack of standardized protocols limit the adaptability and reliability of IDS across diverse IoD platforms.
- In terms of future directions, the field is moving toward the use of federated learning and edge computing to enhance privacy and enable real-time responses. There is also growing interest in robust

hybrid models for proactive intrusion prevention and the exploration of quantum computing to address complex detection tasks, offering improved resilience and adaptability to advanced threats.

Overall, the reviewed literature indicates that secure and intelligent IoD systems increasingly depend on the integration of machine learning-based security mechanisms, distributed and edge-assisted intelligence, and robust communication frameworks. As drones operate as aerial access points and support applications such as smart city surveillance, remote sensing, and mission-critical operations, the need for secure communication, data integrity, and resilience against cyber and physical threats becomes more pronounced.

The studies discussed in this subsection highlight that security challenges in IoD environments are closely linked to constraints such as limited computational capacity, energy consumption, mobility, and real-time detection requirements. Consequently, recent research trends emphasize lightweight, scalable, and privacy-aware solutions, including blockchain-based trust management, machine learning-driven intrusion detection, and the use of edge and federated learning to support real-time and privacy-preserving security operations.

Furthermore, the increasing reliance on heterogeneous communication technologies, including WiFi, LTE, 5G, and satellite links, reinforces the importance of addressing security, localization, and data protection jointly in drone-assisted IoT and smart city applications. The collective findings summarized in this subsection reveal both the progress achieved and the persistent research challenges in securing IoD systems, while underscoring the need for further investigation into adaptable ML-based security models, robust datasets, and efficient deployment strategies tailored to the dynamic and resource-constrained nature of IoD environments.

9.2 Influential Security-Related Keywords without Filtering

We conducted an additional round of analysis by feeding the dataset into the VOSviewer tool without applying keyword filtering, as was primarily done in earlier sections of this paper. The objective of this analysis is to examine how major security-related keywords, such as *security*, *blockchain*, *cybersecurity*, and *authentication*, are mapped to machine learning algorithms. In addition, we focus on *federated learning* as a privacy-preserving learning framework for multi-drone-assisted IoT systems. The key observations from this analysis are summarized below.

Fig. 13 shows that deep learning is a dominant algorithmic paradigm for enabling security in NTN-assisted IoT systems. Other aspects, including resource allocation and emerging 5G and 6G networks, are also closely linked to security, underscoring its central role in future communication infrastructures. Security is similarly associated with both cloud and edge computing, consistent with observations discussed earlier in this paper. These results further confirm that security is a fundamental consideration in Internet of Drones-enabled IoT communication networks.

Fig. 14 further highlights the role of deep learning in cybersecurity, alongside federated learning and blockchain technologies. Likewise, Fig. 15 indicates that deep learning and federated learning are strongly connected to intrusion detection. Both learning paradigms are particularly important for identifying security threats and supporting privacy preservation in UAV-assisted IoT frameworks, including those supported by satellite-based NTN architectures.

Given the prominence of federated learning, Fig. 16 presents its corresponding keyword map. The results indicate that federated learning plays a multifaceted role in NTN-assisted IoT security, particularly in cybersecurity and privacy preservation. Moreover, federated learning exhibits strong potential for integration with differential privacy, deep learning, deep reinforcement learning, blockchain, and energy-aware frameworks, as well as for applications involving resource allocation and emerging 5G and 6G networks.

Fig. 17 identifies blockchain as one of the most versatile technologies within the NTN-IoT ecosystem. Blockchain spans a broad range of application domains, including smart farming, industrial IoT, healthcare (e.g., COVID-related applications), smart grids, and digital twins. It is also closely associated with big data analytics, cloud- and edge-based computing, and immersive technologies such as augmented and virtual reality. Furthermore, blockchain is linked to enabling technologies such as software-defined networking (SDN), 5G and 6G networks, and satellite communications.

From a security perspective, blockchain is associated with key concepts such as privacy, authentication, access control, and intrusion detection systems, as well as broader security-related themes. Its linkage to machine learning, deep learning, and deep reinforcement learning further highlights its potential to support trust-based frameworks in scenarios where traditional centralized learning approaches may be insufficient. Overall, blockchain emerges as a foundational technology for enhancing security, trust, and resilience in NTN-assisted IoT systems.

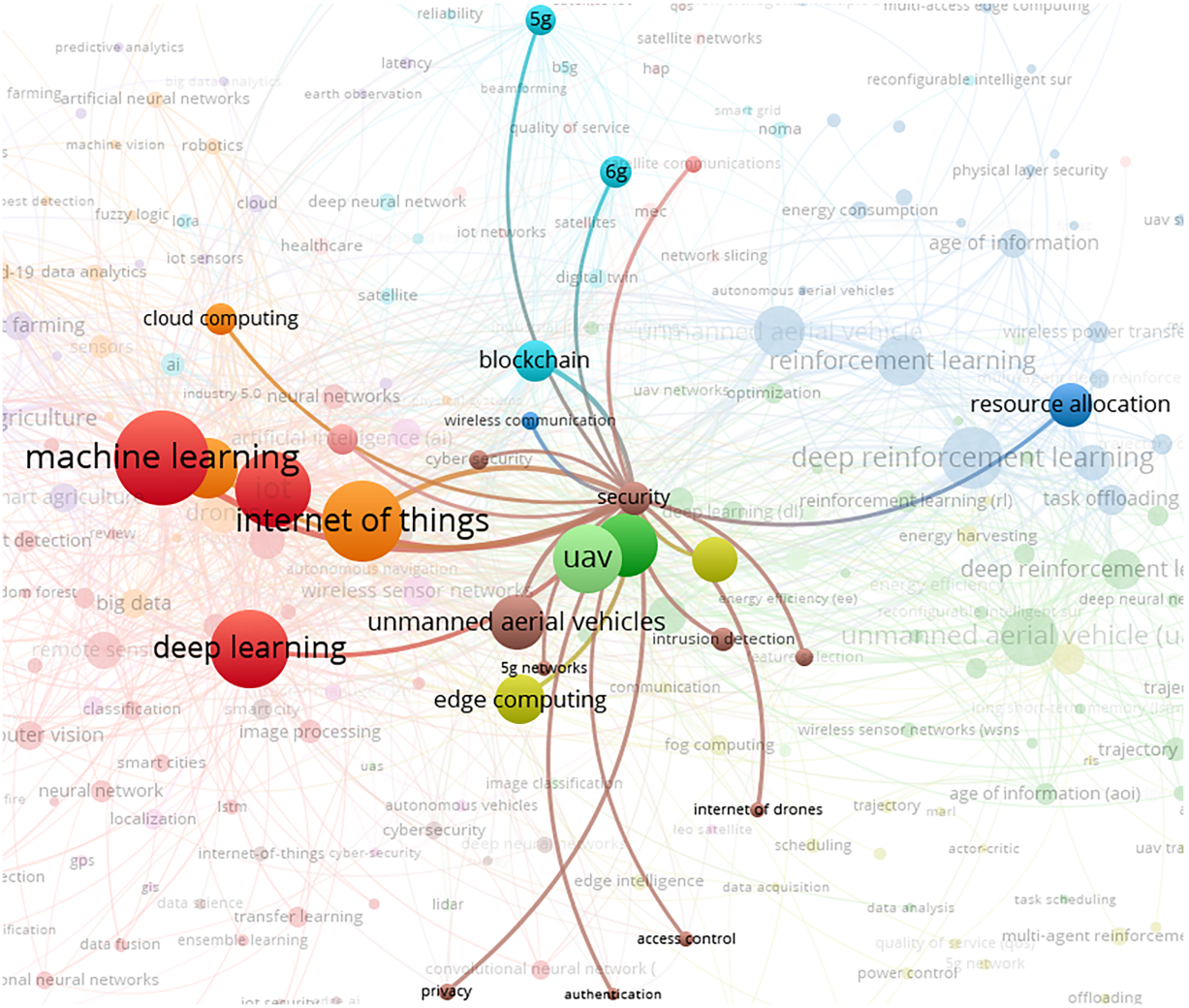

Figure 13: VosViewer map showing security and associated keywords (without filtering).

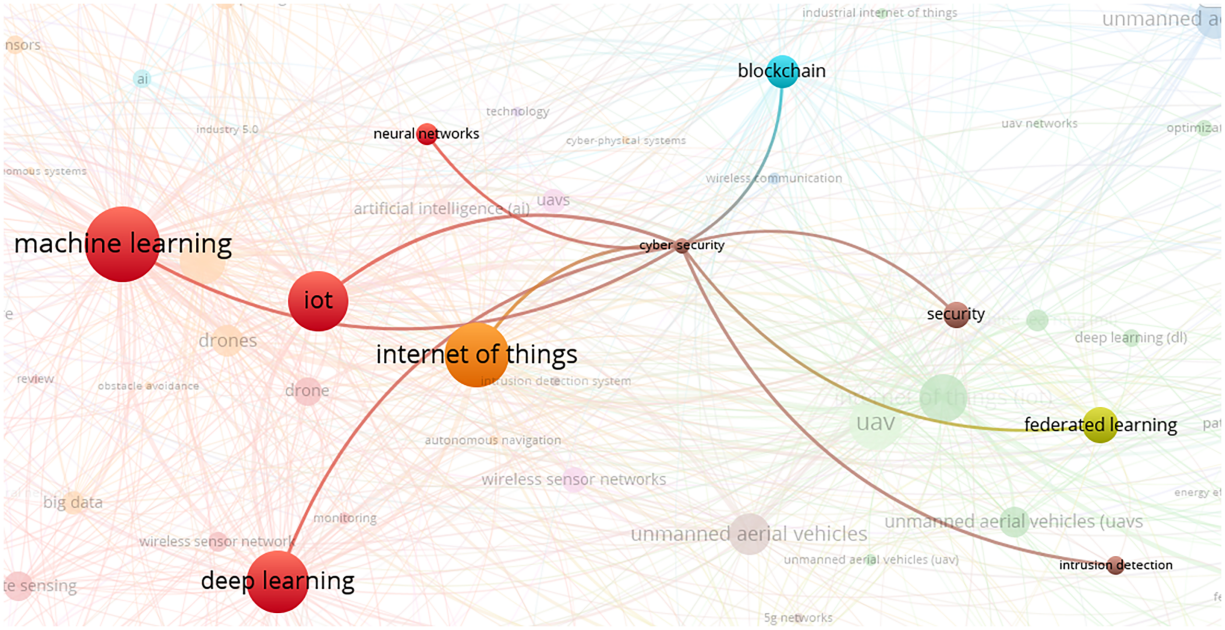

Figure 14: VoSViewer map showing cyber security and associated keywords (without filtering).

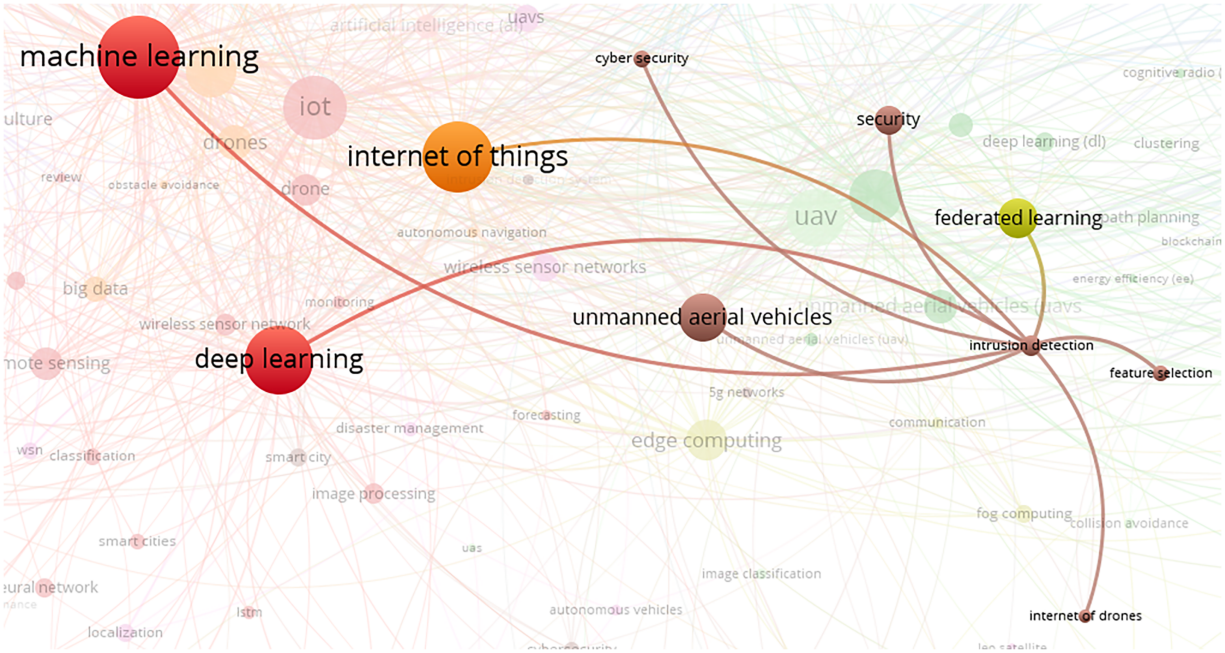

Figure 15: VoSViewer map showing intrusion detection and associated keywords (without filtering).

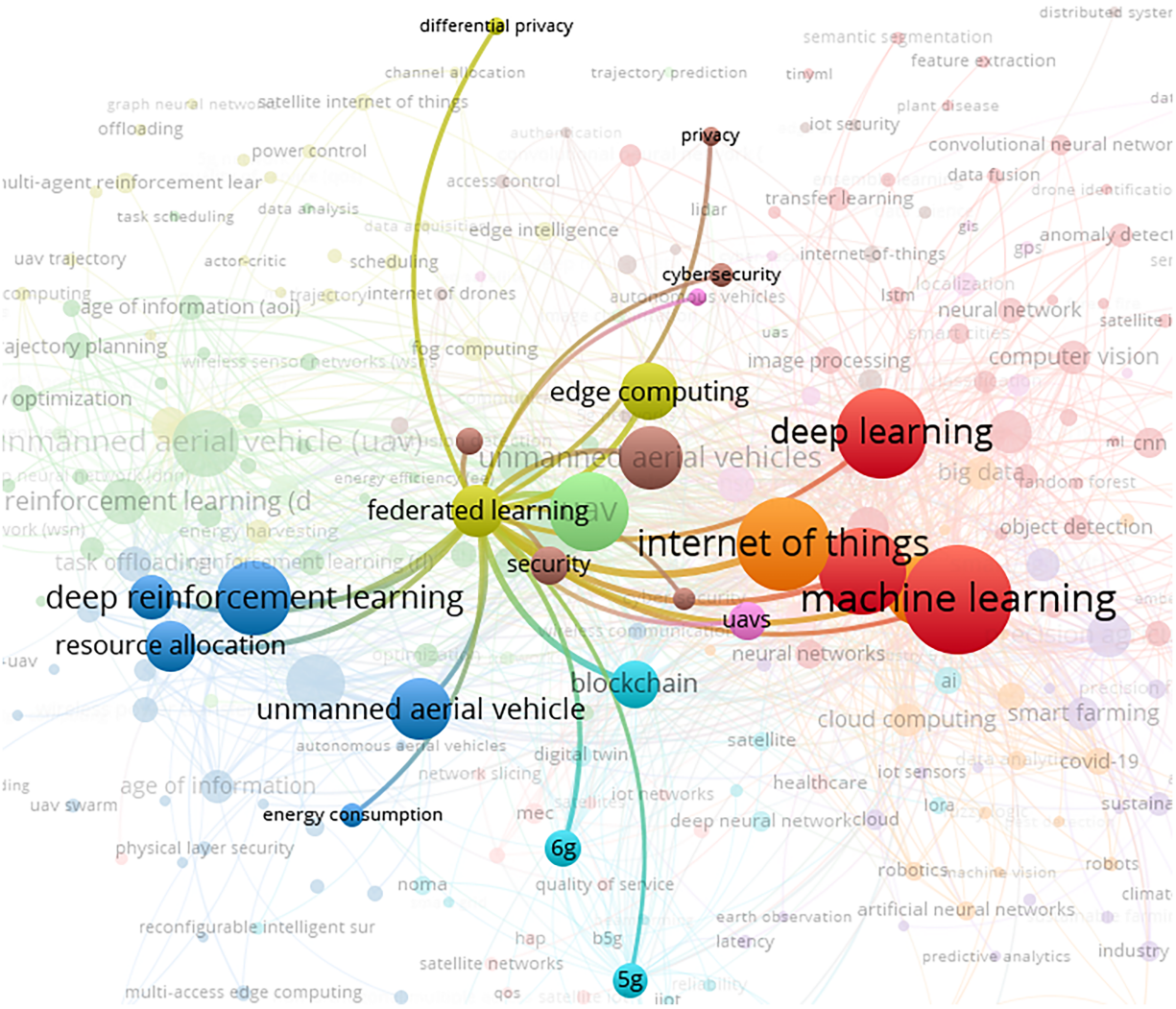

Figure 16: VoSViewer map showing federated learning and associated keywords (without filtering).

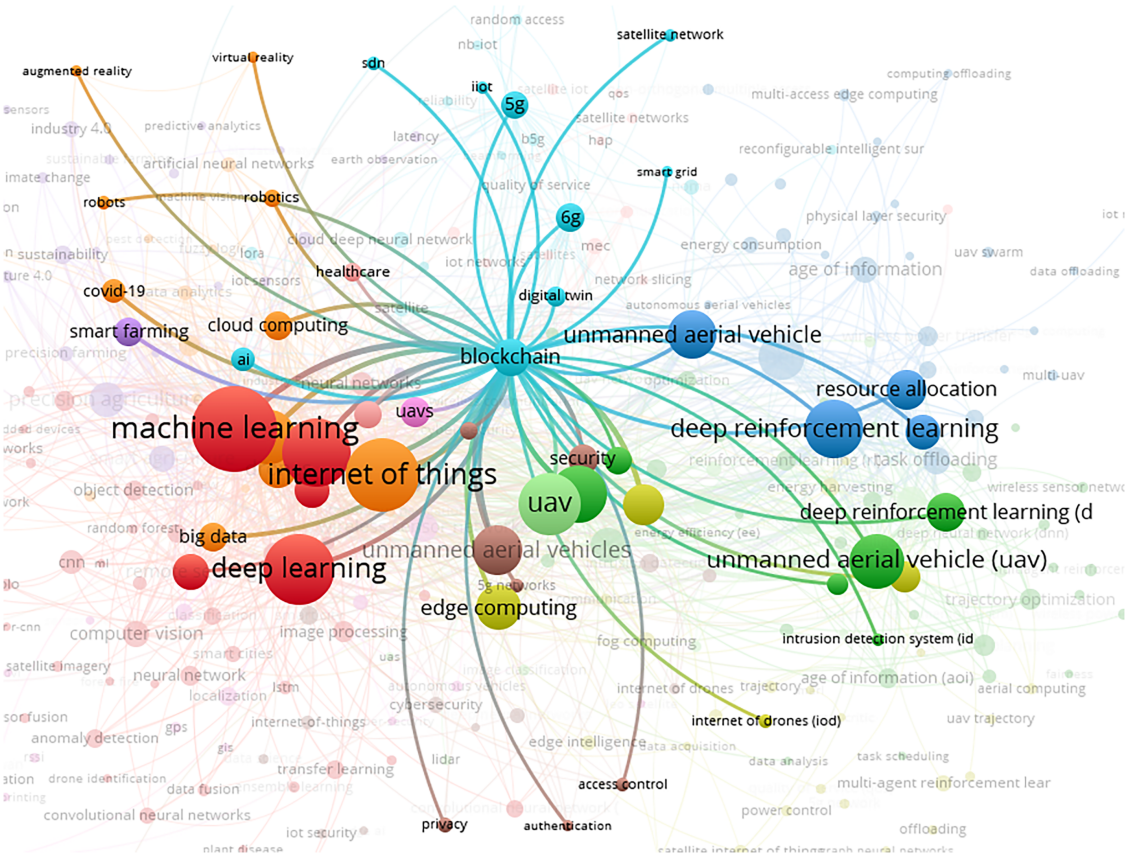

Figure 17: VoSViewer map showing blockchain and associated keywords (without filtering).

9.3 Real-World Case Studies Validating Cluster Themes

This section provides examples that illustrate how ML-driven security, privacy-preserving edge intelligence, efficient localization, and blockchain-based trust mechanisms can support mission-critical operations. These examples substantiate the three security-related research domains identified in this paper for NTN-assisted IoT.

9.3.1 UAV-Based Search and Rescue in GNSS-Denied Environments

Autonomous drones can perform search-and-rescue (SAR) missions in GNSS-denied environments such as underground mines, confined tunnels, and subterranean caverns. Although events like DARPA's Subterranean Challenge have showcased technologies for such missions, many existing systems rely on heavy and expensive sensors, particularly LiDAR, mounted on costly platforms such as heavy-lift multicopters and legged robots. These factors limit accessibility for most SAR organizations. To address this issue, the authors [94] developed a custom quadcopter built around low-cost, lightweight sensors to reduce system cost and extend flight time. They also describe the technical challenges encountered during design and testing and how they were resolved. The system is validated through autonomous flight experiments conducted underground without GNSS access. While security aspects were not addressed, the study shows how low-cost UAV platforms can support practical SAR missions in GNSS-denied environments.

Applications such as precision mapping, surveillance, search and rescue, and assisted navigation rely heavily on accurate localization. With increasing UAV automation and commercial adoption, precise

positioning becomes even more critical. Anticipating a future airspace shared by manned and unmanned aircraft, the authors [95] developed a cooperative localization prototype that enables UAVs to share information with each other and with static anchor nodes to improve positioning accuracy. Each UAV is equipped with low-cost sensors, including cameras, GPS receivers, UWB radios, and inertial units. The system is evaluated in real-world conditions, including environments with partially obstructed GNSS. Results show that the prototype achieves navigation-grade accuracy in GNSS-degraded areas, and that information sharing improves positioning performance even under ideal GNSS conditions.

These deployments illustrate the intersection between the cluster which emphasizes localization, edge sensing, and autonomous navigation in GNSS-denied environments, and that which broadly relates to resilient UAV communication. Although explicit security mechanisms are not implemented in these studies, the demonstrated reliance on cooperative sensing, low-cost platforms, and distributed information sharing highlights the practical importance of robust and resilience-aware localization support in future drone-assisted and NTN-enabled search-and-rescue applications.

9.3.2 Multi-Scale Flood Mapping Using UAVs and SAR Satellites

SAR satellites and UAVs are complementary NTN-enabled sensing tools for flood monitoring. However, SAR imagery suffers from limited resolution and difficulties capturing dynamic flood boundaries, while UAVs cannot efficiently cover very large regions. To overcome these limitations, the authors [96] propose a framework that fuses UAV imagery with multiscale SAR data, supported by a federated learning (FL) scheme and feedback loop to establish a vertical space-air sensing structure. FL handles data heterogeneity across distributed sensing platforms while avoiding the challenges of centralized aggregation. The system is tested in Moama, New South Wales, Australia, a flood-prone region. Results show substantial improvements in flood assessment accuracy, demonstrating the effectiveness, scalability, and robustness of combining SAR, UAV data, and FL.

This case study reflects an emphasis on distributed sensing, edge-assisted intelligence, and data fusion for disaster monitoring, while also aligning with the last cluster's focus on space-air integrated sensing and scalable distributed learning. The application of federated learning to combine UAV imagery and SAR satellite data demonstrates how privacy-aware and distributed intelligence can be applied in real-world, large-scale flood assessment scenarios.

9.3.3 Blockchain-Secured Internet of Drones (IoD) for Aerial Computing

IoD-enabled aerial computing can lower communication delay and energy consumption compared to traditional systems, making it valuable for disaster relief, emergency response, and battlefield communications. However, IoD environments remain vulnerable to attacks such as credential leakage, replay, impersonation, man-in-the-middle, and data modification. To mitigate these risks, the authors [97] propose a blockchain-based secure communication framework for IoD-enabled aerial computing. Blockchain's tamper-proof structure enhances data integrity and authentication. Security analysis shows that the framework resists numerous active and passive attacks, while maintaining low computational and communication overhead.

In IoD systems, multiple drones operate across different zones and exchange critical information before transmitting it to a Ground Station Server (GSS). All drones and the GSS are pre-registered with a trusted authority. Because communication occurs over open wireless channels, security and privacy vulnerabilities are inevitable. To address these vulnerabilities, the authors [98] propose a blockchain-based access control scheme that secures communication among drones and between drones and the GSS. Blockchain ensures data immutability once transactions are stored in the distributed ledger. Extensive security analysis, including

formal, informal, and simulation-based verification, shows that the proposed scheme can withstand various attacks while maintaining low computation and communication costs.

These deployments demonstrate the application of blockchain-enabled trust, authentication, and access control mechanisms in IoD-based aerial computing environments. They align with the focus on cybersecurity and secure communication identified earlier in this paper while also reflecting the emphasis on blockchain-supported coordination and resilient information exchange in distributed UAV systems.

Collectively, these real-world deployments illustrate how the cluster-derived themes identified in this study are reflected in practical UAV- and satellite-assisted IoT applications. The case studies show how security mechanisms, distributed learning, localization, edge-based intelligence, and blockchain-enabled trust are explored across different operational contexts. While these capabilities are not uniformly implemented in all deployments, the examples confirm the practical relevance of the identified clusters and demonstrate their applicability to mission-oriented scenarios such as disaster response and aerial monitoring.

10 Future Directions

In addition to the major clusters discussed earlier, this study also examined keywords with fewer than five occurrences. Though less frequent, these terms highlight emerging or niche directions in ML-driven IoT for agriculture with potential societal impact. A total of 29 clusters, of which 6 are security-related, were identified from these low-frequency keywords (Table 9). The most thematically relevant clusters were then grouped and used to outline potential future research directions.

Table 9: Clusters and their associated keywords (including those with fewer than five occurrences).

Cluster	Associated Keywords
4	4G, ConvLSTM, generative AI, industrial IoT, internet of everything, long short-term memory, mobile networks, network intrusion detection system, O-RAN, optical wireless communication, precision livestock management, search and rescue, semantics, sensing, spoofing, tactile internet, technologies, terahertz, THz communications, tracking, V2X
7	ARM, BIM, cyber forensics, data security, DL, edge device, FPGA, GPU, industrial internet of things, interoperability, kNN, MAC, real-time data, real-time systems, SVM, threat intelligence, trusted execution environment, trustworthy AI
12	Autonomous driving, autonomous robots, autonomous UAV, crowdsourcing, cruise control, imitation learning, jamming attacks, mobile robots, multimedia, obstacle detection, path planning, remotely piloted aircraft system, UAV-aided WSN, unmanned aircraft system, value of information, WSNs
14	Attack detection, cryptography, decryption, distributed deep learning, encryption, fire point detection, golden eagle optimization, interference management, next generation multiple access, performance evaluation, rate-splitting multiple access, satellite-based internet of things, satellite-terrestrial networks, secure communication, YOLOv4
15	Accuracy, crop yield, cyber-attack, data models, data visualization, deep learning, detection, Flask, geospatial data, logistic regression, low-cost sensors, multispectral imaging, network, power grid, predictive models
24	Cognitive radio network, cyberattacks, energy management, intelligent transportation, internet of flying things, network sensing, privacy preservation, software-defined radio

10.1 AI-Enhanced Security and Intelligence for Next-Generation NTN-Assisted IoT

Keywords: 4G, ConvLSTM, generative AI, industrial IoT, internet of everything, long short-term memory, mobile networks, network intrusion detection system, O-RAN, optical wireless communication, precision livestock management, search and rescue, semantics, sensing, spoofing, tactile internet, technologies, terahertz, THz communications, tracking, V2X.

Network intrusion detection and spoofing remain critical security challenges in NTN-assisted IoT, particularly as emerging technologies and high-bandwidth applications become increasingly integrated. Communication frameworks such as optical wireless communication and O-RAN provide the bandwidth necessary for data-intensive applications in industrial IoT, V2X systems, and search-and-rescue missions. THz communication similarly promises ultra-high data rates for tactile internet and real-time tracking.

The Internet of Everything and precision livestock management represent additional domains where ML-assisted IoT systems must ensure data integrity and operational security. Predictive learning models such as LSTM and ConvLSTM can help detect anomalies and forecast threats. Advances in artificial intelligence are further driving the emergence of semantic communication, where meaning rather than raw data is transmitted, enhancing efficiency and contextual awareness. Generative AI extends this potential but also introduces new security risks.

Future research should prioritize the development of secure, intelligent, and context-aware artificial intelligence frameworks tailored to the unique characteristics of non-terrestrial network (NTN)-assisted IoT systems. In particular, generative AI techniques, including Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), can be leveraged to generate high-fidelity synthetic data for training and validating intrusion detection and spoofing mitigation mechanisms across space-air-ground integrated network layers, thereby improving resilience against data scarcity, adversarial manipulation, and evolving attack surfaces. As wireless connectivity advances toward beyond-5G and 6G paradigms, the adoption of terahertz (THz) communications will be instrumental in supporting ultra-low-latency and bandwidth-intensive applications such as the tactile internet, real-time sensing, and mission-critical tracking, while simultaneously introducing new security and reliability challenges. Addressing these challenges requires decentralized and intelligent resource management and security orchestration frameworks capable of operating across heterogeneous NTN architectures to support massive machine-type communications in applications including Industry 4.0, precision agriculture, and large-scale environmental monitoring. Finally, the co-evolution of high-capacity NTN communication technologies and AI-driven security intelligence must incorporate sustainability and energy-efficiency considerations, ensuring that future NTN-IoT systems achieve scalable, secure, and resilient operation in hyper-connected environments.

This direction directly addresses the intrusion detection, spoofing, and privacy challenges identified in Cluster 9 (Security and Access Control), particularly in NTN-assisted IoT systems involving drones, satellites, and high-bandwidth applications.

10.2 AI-Driven Predictive Intelligence and Cyber Resilience in NTN-Assisted IoT Systems

Keywords: Accuracy, crop yield, cyber-attack, data models, data visualization, deep learning, detection, Flask, geospatial data, logistic regression, low-cost sensors, multispectral imaging, power grid, predictive models.

Future research should advance *AI-driven predictive intelligence* and *cyber resilience* to ensure secure and reliable data-driven decision-making across NTN-assisted applications. Data collected from sensors, drones, and IoT devices enable situational awareness for smart agriculture, remote sensing, energy systems, and

smart grids. Multispectral imaging and geospatial data help enhance predictive analytics for yield estimation and environmental monitoring.

Ensuring robust defense mechanisms throughout the data lifecycle, from acquisition to visualization, remains a central challenge. Addressing these concerns requires ML algorithms such as deep learning, logistic regression, and predictive modeling for threat detection and anomaly recognition. Visualization frameworks (e.g., Flask-driven dashboards) also improve interpretability and situational responsiveness.

Future research should prioritize the development of AI-driven predictive intelligence frameworks that tightly couple multi-source data fusion with cyber-resilient design principles for NTN-assisted IoT systems. In particular, hybrid deep learning architectures that integrate multispectral satellite imagery with high-resolution temporal data from low-cost ground-based IoT sensors can significantly enhance predictive accuracy for applications such as crop yield estimation, environmental monitoring, and infrastructure surveillance. Beyond conventional machine learning approaches, the synergistic use of convolutional neural networks (CNNs) for spatial feature extraction and recurrent models such as Long Short-Term Memory (LSTM) networks for temporal modeling enables a more comprehensive representation of complex, dynamic environments operating across distributed NTN topologies.

As NTN-assisted IoT deployments scale and become increasingly interconnected, security frameworks must evolve to address expanded attack surfaces and resource constraints. Future research should focus on lightweight, adaptive intrusion detection systems optimized for edge and aerial nodes, enabling effective detection of cyber-attacks such as distributed denial-of-service and unauthorized access while minimizing computational and energy overhead. Incorporating adversarial robustness, uncertainty-aware prediction, and continuous learning mechanisms will be essential to sustaining long-term cyber resilience in geographically dispersed IoT ecosystems. Finally, the integration of these predictive and security-enhanced models into intuitive, visualization-driven web interfaces, such as Flask-based platforms, will be critical for translating complex analytics into actionable intelligence, thereby supporting timely and secure decision-making in precision agriculture, smart energy systems, and other mission-critical NTN-enabled applications.

This addresses the edge-level security, hardware trust, and real-time processing challenges identified in this paper where secure, low-latency intelligence is critical for industrial NTN-assisted IoT deployments.

10.3 Cognitive and Secure Communication for Energy-Efficient NTN-Assisted IoT Networks

Keywords: Cognitive radio network, cyberattacks, energy management, intelligent transportation, internet of flying things, network sensing, privacy preservation, software-defined radio.

Applications relying on IoT-based communication, such as intelligent transportation systems and the Internet of Flying Things (IoFT), face stringent service demands, especially in heterogeneous communication environments where spectrum resources must be dynamically shared. Software-defined radio (SDR) and cognitive radio networks (CRNs) enable adaptive spectrum access, interference management, and efficient resource utilization.

However, ensuring privacy and cybersecurity in these networks is equally important, as attacks on a single component can have cascading effects across the system. Therefore, preventing and mitigating cyberattacks, as well as supporting intelligent network sensing, should remain key areas of focus.

Future research should prioritize the design of cognitive and secure communication frameworks that jointly optimize spectrum efficiency, cybersecurity, and energy consumption in NTN-assisted IoT networks. In particular, green cognitive radio network (CRN) architectures that integrate energy-harvesting and adaptive power management mechanisms are critical for supporting energy-constrained NTN components such as unmanned aerial vehicles and low Earth orbit (LEO) satellites operating as aerial or space-based

communication relays. These frameworks must account for the dynamic power and spectrum constraints inherent to Internet of Flying Things (IoFT) deployments and intelligent transportation systems, enabling sustained operation without compromising connectivity or service quality.

As NTN-assisted networks become increasingly autonomous and software-defined, security mechanisms must evolve beyond static encryption and rule-based defenses. Future research should investigate machine learning-driven and deep learning-enabled security architectures capable of real-time spectrum sensing, threat prediction, and adaptive mitigation of sophisticated attacks, including jamming, spoofing, and coordinated cyber-physical interference. Incorporating privacy-preserving techniques, such as location obfuscation and secure cooperative sensing protocols, will be essential to protect sensitive node information while maintaining reliable spectrum sharing. Ultimately, the convergence of cognitive communication, AI-driven security intelligence, and energy-aware design will be central to achieving resilient, efficient, and trustworthy NTN-assisted IoT networks in highly dynamic and contested environments.

This direction directly addresses the communication-level security, spectrum awareness, and efficiency challenges identified in the analyzed clusters especially for bandwidth-intensive and heterogeneous NTN-assisted IoT environments.

10.4 Trustworthy and Secure Edge Intelligence for Industrial NTN-Assisted IoT Systems

Keywords: ARM, BIM, cyber forensics, data security, deep learning (DL), edge device, FPGA, GPU, Industrial Internet of Things (IIoT), interoperability, k-nearest neighbors (kNN), medium access control (MAC), real-time data, real-time systems, support vector machine (SVM), threat intelligence, trusted execution environment (TEE), trustworthy AI.

Security at the edge is critical in NTN-assisted IoT systems, where edge devices execute computation tasks that cannot be handled by constrained IoT nodes. In real-time industrial applications, maintaining a *trusted execution environment (TEE)* and ensuring the interoperability of hardware and data processes are essential for reliable and safe operation. Future research should prioritize the development of *lightweight and trustworthy AI frameworks* that enhance data security while meeting the resource constraints of edge platforms.

Hardware-level security remains equally important. Potential vulnerabilities in *MAC protocols*, *ARM*, *FPGA*, and *GPU*-based systems must be assessed, and their secure integration across heterogeneous architectures should be investigated. In addition, advancements in *cyber forensics* are needed to trace and analyze attacks targeting industrial edge devices. Machine learning models such as SVM, kNN, and deep learning approaches can be leveraged for real-time threat intelligence, anomaly detection, and adaptive security monitoring in Industrial IoT environments.

This direction directly addresses the edge-level security, hardware trust, and real-time processing challenges identified earlier where secure, low-latency intelligence is critical for industrial NTN-assisted IoT deployments.

10.5 Autonomous, Secure, and Resilient Robotic Intelligence in NTN-Assisted IoT Systems

Keywords: Autonomous driving, autonomous robots, autonomous UAV, crowdsourcing, cruise control, imitation learning, jamming attacks, mobile robots, multimedia, obstacle detection, path planning, remotely piloted aircraft system, UAV-aided WSN, unmanned aircraft system, value of information, WSNs.

The autonomous deployment of mobile robots and UAVs plays a crucial role in enhancing IoT networks, particularly in data collection and situational awareness. As NTN-assisted IoT systems evolve toward greater autonomy and connectivity, ensuring robust security for these intelligent agents becomes increasingly

important. In particular, mitigating jamming attacks that disrupt communication or compromise mission objectives remains a significant research challenge.

Future research should focus on developing adaptive and resilient control mechanisms that enable UAVs and mobile robots to maintain functionality under adversarial or uncertain network conditions. Protecting UAVs, IoT nodes, and sensor networks from such attacks is critical in applications involving autonomous navigation and real-time data transmission. Furthermore, strengthening mobile crowdsourcing platforms and integrating *imitation learning* techniques can enhance decision-making, coordination, and resilience in UAV-assisted IoT systems.

Jamming attacks not only hinder UAV operations but can also prevent high-value information from reaching data centers, reducing the overall reliability of industrial IoT applications. Therefore, designing secure communication protocols and intelligent defense mechanisms will be key to realizing autonomous, secure, and resilient robotic intelligence in future NTN-assisted IoT environments. This direction directly addresses the autonomy, jamming resilience, and secure coordination challenges for Internet-of-Drones and UAV-assisted IoT environments.

Overall, the future directions identified in this section converge on a single insight: secure, intelligent, and energy-efficient NTN-assisted IoT systems will require a unified design approach that integrates ML-driven security, resilient distributed intelligence, privacy-preserving computation, and adaptive communication across space-air-ground layers. The anchor-keyword connectivity structures mapped in this study provide a foundational roadmap for shaping these developments.

11 Conclusion

This paper maps security-related thematic domains within the broad landscape of machine learning-driven NTN-assisted IoT systems. The analysis is based on a VOSviewer-driven keyword co-occurrence study of a comprehensive dataset comprising 2469 publications. From the resulting twelve thematic clusters, three clusters are identified as being directly related to security, reflecting the multifaceted nature of security, privacy, and resilience challenges in ML-enabled NTN-assisted IoT environments.

A core methodological contribution of this work is the introduction of a connectivity-driven cluster validation technique, which identifies anchor keywords based on intra-cluster connectivity to define core research areas. This approach provides an objective and reproducible mechanism for interpreting cluster semantics, reduces reliance on subjective validation, and enables consistent identification of dominant and emerging thematic structures within the literature. Although this paper focuses on the most highly connected keywords within each cluster during intra-cluster association analysis, these keywords provide significant insights into the state of the art, which are further validated through detailed literature discussion.

The analysis shows that cybersecurity, access control, intrusion detection, authentication, and privacy preservation are central security concerns in NTN-assisted IoT research, particularly in drone- and satellite-enabled systems. The security and privacy of UAV-based networks, especially those operating within the Internet of Drones (IoD) paradigm, remain pressing research challenges. As UAVs increasingly serve as aerial base stations and participate in mission-critical applications, the literature emphasizes the need for robust mechanisms to support secure communication, data integrity, and resilience against both cyber and physical threats. Within this context, blockchain-based approaches are frequently discussed as potential enablers of decentralized trust management, intrusion detection, and secure data sharing, particularly when combined with machine learning-based security techniques.

The bibliometric findings further indicate that several security challenges in NTN-assisted IoT research are closely interconnected with localization, edge intelligence, and distributed learning mechanisms.

The strong interaction between security-focused clusters and clusters related to edge computing and localization highlights the importance of jointly considering secure communication, privacy-preserving analytics, and resource-efficient machine learning, rather than addressing these aspects in isolation, particularly in drone-assisted IoT and smart city applications.

Despite the breadth of existing research, limitations related to computational constraints, dataset scarcity, and adaptability to IoD-specific operating conditions remain evident in the literature. These challenges point to an ongoing research emphasis on lightweight, scalable, and practically deployable security solutions. In particular, security challenges in smart city applications and those involving RSSI fingerprinting and LoRaWAN architectures highlight the need for lightweight and resource-efficient approaches. Future research should pay increased attention to federated learning, hybrid AI models, and quantum-resilient cryptographic techniques as potential approaches for improving robustness against evolving threats in IoT and NTN environments.

In addition, the analysis of low-frequency and emerging keywords reveals early-stage research themes related to semantic communication, autonomous NTN robotics, jamming-resilient distributed learning, and satellite-terrestrial coordination. Although these topics currently appear with lower frequency, their presence indicates emerging directions that may shape future research agendas in NTN-assisted IoT.

Overall, this study provides an integrated, data-driven mapping of machine learning research related to security in NTN-assisted IoT systems, highlighting co-occurrence relationships among intrusion detection, authentication, and privacy; edge computing and localization; and blockchain and intrusion detection systems. The bibliometric and thematic patterns identified in this work offer a consolidated analytical reference for understanding the current research landscape and for informing future investigations as NTN-assisted IoT systems continue to evolve through multi-orbit satellite deployments, UAV-enabled platforms, and large-scale IoT integration.

Acknowledgement: Gemini 2.0 Flash AI model was used to perform text extraction from VOSviewer “Items” panel screenshots to capture keyword lists for each cluster for subsequent analysis.

Funding Statement: Oluwatosin Ahmed Amodu and Zurina Mohd Hanapi acknowledge the support of the Ministry of Higher Education Malaysia through the Fundamental Research Grant Scheme under Grant FRGS/1/2023/ICT11/UPM/02/2/5540649.

Author Contributions: The authors confirm their contribution to the paper as follows: Study Conception and Design: Oluwatosin Ahmed Amodu; Data Collection: Oluwatosin Ahmed Amodu, Faten A. Saif, Huda Althumali, Chedia Jarray; Analysis and Interpretation of Results: Oluwatosin Ahmed Amodu; Draft Manuscript Preparation: Oluwatosin Ahmed Amodu; Review and Editing: Raja Azlina Raja Mahmood, Umar Ali Bukar; Illustrations: Oluwatosin Ahmed Amodu, Umar Ali Bukar, Mohammed Sani Adam; Supervision: Zurina Mohd Hanpi; Funding: Zurina Mohd Hanapi. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: This paper is predominantly a review that synthesizes existing methods and literature findings. This investigation utilized only data obtained from publicly accessible sources. These datasets are accessible via the sources listed in the References section of this paper.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. He P, Lei H, Wu D, Wang R, Cui Y, Zhu Y, et al. Non-terrestrial network technologies: applications and future prospects. IEEE Internet Things J. 2025;12(6):6275–99.
2. Chen K, Zhang L, Zhong J. Space-air-ground integrated network (SAGIN) in disaster management: a survey. IEEE Trans Netw Serv Manag. 2025;22(5):4021–49. doi:10.1109/tnsm.2025.3580965.
3. Abualigah L, Diabat A, Sumari P, Gandomi AH. Applications, deployments, and integration of internet of drones (IoD): a review. IEEE Sens J. 2021;21(22):25532–46. doi:10.1109/jsen.2021.3114266.
4. Ferrag MA, Shu L, Friha O, Yang X. Cyber security intrusion detection for agriculture 4.0: machine learning-based solutions, datasets, and future directions. IEEE/CAA J Autom Sin. 2022;9(3):407–36. doi:10.1109/jas.2021.1004344.
5. Sharma A, Vanjani P, Paliwal N, Basnayaka CMW, Jayakody DNK, Wang H-C, et al. Communication and networking technologies for UAVs: a survey. J Netw Comput Appl. 2020;168:102739.
6. Kou G, Ye Q, Zhang M, Wang XA, Fu W, Zhou Q, et al. Intelligent UAV swarm key agreement survey: systematic taxonomy, cryptographic automaton and quantum resistance. Internet Things. 2025;34:101720.
7. Alladi T, Chamola V, Sahu N, Guizani M. Applications of blockchain in unmanned aerial vehicles: a review. Veh Commun. 2020;23(2):100249. doi:10.1016/j.vehcom.2020.100249.
8. Mehta P, Gupta R, Tanwar S. Blockchain envisioned UAV networks: challenges, solutions, and comparisons. Comput Commun. 2020;151(14):518–38. doi:10.1016/j.comcom.2020.01.023.
9. Wang Z, Zhang F, Yu Q, Qin T. Blockchain-envisioned unmanned aerial vehicle communications in space-air-ground integrated network: a review. Intell Converg Netw. 2021;2(4):277–94. doi:10.23919/icn.2021.0018.
10. Ogab M, Zaidi S, Bourouis A, Calafate CT. Machine learning-based intrusion detection systems for the internet of drones: a systematic literature review. IEEE Access. 2025;13(13):96681–714. doi:10.1109/access.2025.3575236.
11. Ye Y, Min X, Liu X, Chen X, Cao K, Howlader SMRK, et al. Secure and intelligent low-altitude infrastructures: synergistic integration of IoT networks, AI decision-making and blockchain trust mechanisms. Sensors. 2025;25(21):6751.
12. Stojnic T, Kayes ASM, Rahayu W, Chowdhury MJM. A comprehensive literature review of cyber threats and vulnerabilities in IoT-driven satellite networks: research challenges and future directions. Comput Netw. 2025;272(2):111678. doi:10.1016/j.comnet.2025.111678.
13. He Y, Wu J, Zhu L, Huang F, Wang B, Yang D, et al. A review of physical layer security in aerial-terrestrial integrated internet of things: emerging techniques, potential applications, and future trends. Drones. 2025;9(4):312. doi:10.3390/drones9040312.
14. Li B, Fei Z, Zhou C, Zhang Y. Physical-layer security in space information networks: a survey. IEEE Internet Things J. 2019;7(1):33–52. doi:10.1109/jiot.2019.2943900.
15. Abdelsalam N, Al-Kuwari SM, Erbad AM. Physical layer security in satellite communication: state-of-the-art and open problems. IET Commun. 2025;19(1):e12830. doi:10.1049/cmu2.12830.
16. Massimi F, Ferrara P, Benedetto F. Deep learning methods for space situational awareness in mega-constellations satellite-based internet of things networks. Sensors. 2022;23(1):124. doi:10.3390/s23010124.
17. Zhu X, Qu W, Qiu T, Zhao L, Atiquzzaman M, Wu DO. Indoor intelligent fingerprint-based localization: principles, approaches and challenges. IEEE Commun Surv Tutor. 2020;22(4):2634–57. doi:10.1109/comst.2020.3014304.
18. Sheikh RA, Al-Hadi AA, Sabapathy T, Hossain TM, Mirza H, Akkaraekthalin P, et al. Review of positioning technologies and antenna designs for indoor, outdoor and wearable applications. IEEE Access. 2025;13(2):180317–43. doi:10.1109/access.2025.3614190.
19. Aftab MU, Munir Y, Oluwasanmi A, Qin Z, Aziz MH, Son NT, et al. A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles. IEEE Access. 2020;8:24196–208. doi:10.1109/access.2020.2969715.
20. Ullah Z, Al-Turjman F, Mostarda L, Gagliardi R. Applications of artificial intelligence and machine learning in smart cities. Comput Commun. 2020;154(2):313–23. doi:10.1016/j.comcom.2020.02.069.
21. Ogbodo EU, Abu-Mahfouz AM, Kurien AM. A survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: from the aspect of architecture and security. Sensors. 2022;22(16):6313. doi:10.3390/s22166313.

22. Alsamhi SH, Ma O, Ansari MS, Almalki FA. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. IEEE Access. 2019;7:128125–52.
23. Lagkas T, Argyriou V, Bibi S, Sarigiannidis P. UAV IoT framework views and challenges: towards protecting drones as "things". Sensors. 2018;18(11):4015.
24. Sze V, Chen Y-H, Emer J, Suleiman Amr, Zhang Z. Hardware for machine learning: challenges and opportunities. In: 2018 IEEE Custom Integrated Circuits Conference (CICC). Piscataway, NJ, USA: IEEE; 2018. p. 1–8.
25. Yazid Y, Ez-Zazi I, Guerrero-González A, Oualkadi AE, Arioua M. UAV-enabled mobile edge-computing for IoT based on AI: a comprehensive review. Drones. 2021;5(4):148.
26. Hussain A, Li S, Hussain T, Lin X, Ali F, AlZubi AA. Computing challenges of UAV networks: a comprehensive survey. Comput Mater Contin. 2024;81(2):1999–2051.
27. Cheng N, Wu S, Wang X, Yin Z, Li C, Chen W, et al. AI for UAV-assisted IoT applications: a comprehensive review. IEEE Internet Things J. 2023;10(16):14438–61.
28. Lutakamale AS, Myburgh HC, Freitas AD. RSSI-based fingerprint localization in LoRaWAN networks using CNNs with squeeze and excitation blocks. Ad Hoc Netw. 2024;159:103486.
29. Kamal MA, Alam MM, Sajak AAB, Su'ud MM. SNR and RSSI based an optimized machine learning based indoor localization approach: multistory round building scenario over lora network. Comput Mater Contin. 2024;80(2):1927–45.
30. Zholamanov B, Saymbetov A, Nurgaliyev M, Bolatbek A, Dosymbetova G, Kuttybay N, et al. RSSI fingerprint-based indoor localization solutions using machine learning algorithms: a comprehensive review. Smart Cities. 2025;8(5):153.
31. Zhang XJ, He FC, Gai JY, Bao J, Huang H, Du X. A differentially private federated learning model for fingerprinting indoor localization in edge computing. J Comput Res Dev. 2022;59(6):2667–88. doi:10.1007/s00521-021-06815-9.
32. Zhou L, Yu L, Du S, Zhu H, Chen C. Achieving differentially private location privacy in edge-assistant connected vehicles. IEEE Internet Things J. 2018;6(3):4472–81.
33. Vasudevan N, Thach A, Paoli C. Developing an AI-enabled cybersecurity model to protect satellite systems from cyber threats. In: Proceedings of the 74th International Astronautical Congress (IAC); 2023 Oct 2–6; Baku, Azerbaijan.
34. Anantha Babu S, Ranganath A, Goswami MM, Gnanaprakasam T, Ishak MK. Modified marine predators algorithm with deep learning-driven security solution for IoT-assisted UAV networks. IEEE Access. 2024;12:54991–8.
35. Alotaibi SS, Sayed A, Elhameed ESA, Alghushairy O, Assiri M, Ibrahim SS. Enhancing security in IoT-assisted UAV networks using adaptive mongoose optimization algorithm with deep learning. IEEE Access. 2024;12:63768–76.
36. Perumalla S, Chatterjee S, Siva Kumar AP. Modelling of oppositional aquila optimizer with machine learning enabled secure access control in internet of drones environment. Theor Comput Sci. 2023;941:39–54.
37. Al-Wesabi FN, Alrowais F, Alzahrani JS, Marzouk R, Duhayyim MA, Alkhayyat A, et al. Oppositional poor and rich optimization with deep learning enabled secure internet of drone communication system. Comput Electr Eng. 2022;104(Pt A):108368.
38. Al-Fuwaiers A, Mishra S. ML-based intrusion detection for drone IoT security. J Cybersecur Inf Manag. 2024;14(1):64– 78.
39. Uhongora U, Mulinde R, Law YW, Slay J. Deep-learning-based intrusion detection for software-defined networking space systems. Eur Conf Cyber Warfare Secur. 2023;22(1):639–47.
40. Wu Y, Yang L, Zhang L, Nie L, Zheng L. Intrusion detection for unmanned aerial vehicles security: a tiny machine learning model. IEEE Internet Things J. 2024;11(12):20970–82.
41. Alissa KA, Alotaibi SS, Alrayes FS, Aljebreen M, Alazwari S, Alshahrani H, et al. Crystal structure optimization with deep-autoencoder-based intrusion detection for secure internet of drones environment. Drones. 2022;6(10):297.
42. Islam A, Amin AA, Shin SY. FBI: a federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things. IEEE Wirel Commun Lett. 2022;11(5):972–6.
43. Wei D, Xi N, Ma J, He L. UAV-assisted privacy-preserving online computation offloading for internet of things. Remote Sens. 2021;13(23):4853.

44. Hakeem A, Sabir M, Alhebshi RM, Almakky AG, Ashraf I. Integrating artificial intelligence for improved security of IoT-drones through cyber-physical attack detection. Front Comput Sci. 2025;7:1545282.
45. Aldaej A, Ahanger TA, Atiquzzaman M, Ullah I, Yousufudin M. Smart cybersecurity framework for IoT-empowered drones: machine learning perspective. Sensors. 2022;22(7):2630.
46. Tandra N, Babu CNG, Dhanke J, Sudhakar AVV, Rao MK, Ravichandran S. Enhancing security and privacy in small drone networks using 6G-IoT driven cyber physical system. Wirel Pers Commun. 2024. doi:10.1007/s11277-024-11138-8.
47. Ramadan MN, Ali MA, Khoo SY, Alkhedher M. AI-powered IoT and UAV systems for real-time detection and prevention of illegal logging. Results Eng. 2024;24:103277.
48. Zhang H, Yan F, Li H, Ding K, Wu T, Xia W, et al. Deep learning based localization scheme for UAV aided wireless sensor networks. In: 2022 14th International Conference on Wireless Communications and Signal Processing (WCSP). Piscataway, NJ, USA: IEEE; 2022. p. 638–43.
49. Annepu V, Anbazhagan R. Implementation of an efficient extreme learning machine for node localization in unmanned aerial vehicle assisted wireless sensor networks. Int J Commun Syst. 2020;33(10):e4173.
50. Bhardwaj VK, Shukla A, Pandey OJ. Energy-efficient node localization in time-varying UAV-RIS-assisted and cluster-based IoT networks. IEEE Trans Netw Serv Manag. 2025;22(3):2897–913.
51. Lin D, Wu W. Optimization of a secure UAV-based IoT: RF-fingerprint authentication and resource allocation. IEEE Internet Things J. 2023;10(21):19208–17.
52. Garg T, Gupta S, Obaidat MS, Raj M. Drones as a service (DAAS) for 5G networks and blockchain-assisted IoT-based smart city infrastructure. Cluster Comput. 2024;27(7):8725–88.
53. Heidari A, Navimipour NJ, Unal M. Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: a systematic literature review. Sustain Cities Soc. 2022;85:104089.
54. Nikitas A, Michalakopoulou K, Njoya ET, Karampatzakis D. Artificial intelligence, transport and the smart city: definitions and dimensions of a new mobility era. Sustainability. 2020;12(7):2789.
55. Gohari A, Ahmad AB, Rahim RBA, Supa'at ASM, Abd Razak S, Gismalla MSM. Involvement of surveillance drones in smart cities: a systematic review. IEEE Access. 2022;10:56611–28.
56. Bansal P, Mewara M, Tripathi S, Gupta S, Sonwane P. Development of smart machine learning algorithm to design and develop the IoT based drone cyber physical security system. In: 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS). Piscataway, NJ, USA: IEEE; 2023. p. 1–7.
57. Alsamhi SH, Almalki FA, Ma O, Ansari MS, Lee B. Predictive estimation of optimal signal strength from drones over IoT frameworks in smart cities. IEEE Trans Mob Comput. 2023;22(1):402–16.
58. Meng S, Dai X, Xiao B, Zhou Y, Li Y, Gao C. Deep learning-based fifth-generation millimeter-wave communication channel tracking for unmanned aerial vehicle internet of things networks. Int J Distrib Sens Netw. 2019;15(8):15501477198.
59. Liu J, Zhao B, Xin Q, Liu H. Dynamic channel allocation for satellite internet of things via deep reinforcement learning. In: 2020 International Conference on Information Networking (ICOIN). Piscataway, NJ, USA: IEEE; 2020. p. 465–70.
60. Zhao B, Liu J, Wei Z, You I. A deep reinforcement learning based approach for energy-efficient channel allocation in satellite Internet of Things. IEEE Access. 2020;8:62197–206.
61. Xu Q, You Q, Gong Y, Yang X, Wang L. RIS-assisted UAV-enabled green communications for industrial IoT exploiting deep learning. IEEE Internet Things J. 2024;11(16):26595–609.
62. Othman NA, Aydin I. A new UAV-based social distance detector for covid-19 outbreaks reduction, using IoT, computer vision and deep learning technologies. Trait Signal. 2022;39(6):1951–9.
63. Uddin R, Kumar SAP. SDN-based federated learning approach for satellite-IoT framework to enhance data security and privacy in space communication. IEEE J Radio Freq Identif. 2023;7:424–40. doi:10.1109/JRFID.2023.3279329.
64. Tong Z, Wang J, Hou X, Chen J, Jiao Z, Liu J. Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks. IEEE Internet Things J. 2024;11(21):34270–82.

65. Seid AM, Lu J, Abishu HN, Ayall TA. Blockchain-enabled task offloading with energy harvesting in multi-UAV-assisted IoT networks: a multi-agent DRL approach. IEEE J Sel Areas Commun. 2022;40(12):3517–32.
66. Abegaz MS, Abishu HN, Yacob YH, Ayall TA, Erbad A, Guizani M. Blockchain-based resource trading in multi-UAV-assisted industrial IoT networks: a multi-agent DRL approach. IEEE Trans Netw Serv Manag. 2023;20(1):166–81.
67. Yang F, Zhao Z, Huang J, Liu P, Tolba A, Yu K, et al. A federated reinforcement learning approach for optimizing wireless communication in UAV-enabled IoT network with dense deployments. IEEE Internet Things J. 2024;11(20):33953–66.
68. Gad G, Farrag A, Fadlullah ZM, Fouda MM. Communication-efficient federated learning in drone-assisted IoT networks: path planning and enhanced knowledge distillation techniques. In: 2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). Piscataway, NJ, USA: IEEE; 2023. p. 1–7.
69. Gad G, Farrag A, Aboulfotouh A, Bedda K, Fadlullah ZM, Fouda MM. Joint self-organizing maps and knowledge-distillation-based communication-efficient federated learning for resource-constrained UAV-IoT systems. IEEE Internet Things J. 2024;11(9):15504–22.
70. Jabbari A, Khan H, Duraibi S, Budhiraja I, Gupta S, Omar M. Energy maximization for wireless powered communication enabled IoT devices with NOMA underlaying solar powered UAV using federated reinforcement learning for 6G networks. IEEE Trans Consum Electron. 2024;70(1):3926–39.
71. Qureshi KI, Lu B, Lu C, Lodhi MA, Wang L. Multi-agent DRL for air-to-ground communication planning in UAV-enabled IoT networks. Sensors. 2024;24(20):6535.
72. Liu X, Wu J, Zhao C, Liu Z. Integrated sensing and communications for UAV assisted internet of things based on deep reinforcement learning. IEEE Trans Veh Technol. 2025;74(6):9604–16.
73. Tang X, Lan X, Li L, Zhang Y, Han Z. Incentivizing proof-of-stake blockchain for secured data collection in UAV-assisted IoT: a multi-agent reinforcement learning approach. IEEE J Sel Areas Commun. 2022;40(12):3470–84.
74. Emami Y, Wei B, Li K, Ni W, Tovar E. Joint communication scheduling and velocity control in multi-UAV-assisted sensor networks: a deep reinforcement learning approach. IEEE Trans Veh Technol. 2021;70(10):10986–98.
75. Durga S, Rajeshwari C, Allehaibi KH, Gupta N, Albaqami NN, Bharti I, et al. Deep reinforcement learning-based long short-term memory for satellite IoT channel allocation. Intell Autom Soft Comput. 2022;33(1):1–19.
76. Nguyen KK, Masaracchia A, Vishal Sharma HP, Duong TQ. RIS-assisted UAV communications for IoT with wireless power transfer using deep reinforcement learning. IEEE J Sel Top Signal Process. 2022;16(5):1086–96.
77. Spyridis Y, Lagkas T, Sarigiannidis P, Argyriou V, Sarigiannidis A, Eleftherakis G, et al. Towards 6G IoT: tracing mobile sensor nodes with deep learning clustering in UAV networks. Sensors. 2021;21(11):3936.
78. Zhuang S, Sun J, Zhang H, Kuang X, Pang L, Liu H, et al. Stinattack: a lightweight and effective adversarial attack simulation to ensemble IDSS for satellite-terrestrial integrated network. In: 2022 IEEE Symposium on Computers and Communications (ISCC). Piscataway, NJ, USA: IEEE; 2022. p. 1–8.
79. Yahuza M, Idris MYI, Ahmedy IB, Wahab AWA, Nandy T, Noor NM, et al. Internet of drones security and privacy issues: taxonomy and open challenges. IEEE Access. 2021;9:57243–70.
80. Alturki N, Aljrees T, Umer M, Ishaq A, Alsubai S, Saidani O, et al. An intelligent framework for cyber–physical satellite system and IoT-aided aerial vehicle security threat detection. Sensors. 2023;23(16):7154.
81. Suhaimi NHS, Kamarudin NH, Khalid MNA, Tahir I, Mohamed MAA. State-of-the-art authentication measures in satellite communication networks: a comprehensive analysis. IEEE Access. 2024;12:142241–64.
82. Ntizikira E, Lei W, Alblehai F, Saleem K, Lodhi MA. Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. Sensors. 2023;23(19):8077.
83. Shrestha R, Omidkar A, Roudi SA, Abbas R, Kim S. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics. 2021;10(13):1549.
84. Neupane I, Shahrestani S, Ruan C. Indoor localization of resource-constrained IoT devices using wi-fi fingerprinting and convolutional neural network. In: ACSW '24: Proceedings of the 2024 Australasian Computer Science Week. New York, NY, USA: ACM; 2024. p. 20–5.

85. Graha RT, Setiawan RR, Fakhrurroja H, Meylani L, Pramesti D. Performance evaluation of the Dragino DLOS8N and four-faith F8L10GW LoRaWAN gateways in an urban scenario. In: 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA). Piscataway, NJ, USA: IEEE; 2024. p. 784–9.
86. Pansari N, Saiya R. Reliability and security of edge computing devices for smart cities. In: Enabling technologies for effective planning and management in sustainable smart cities. Cham, Switzerland: Springer; 2023. p. 29–52.
87. Gonzalez-Palacio M, Luna-delRisco M, Garcia-Giraldo J, Arrieta-Gonzalez C, Gonzalez-Palacio L, Roehrig C, et al. Novel RSSI-based localization in LoRaWAN using probability density estimation similarity-based techniques. Internet Things. 2025;31:101551.
88. Javaid S, Khan MA, Fahim H, He B, Saeed N. Explainable AI and monocular vision for enhanced UAV navigation in smart cities: prospects and challenges. Front Sustain Cities. 2025;7:1561404.
89. Mani R, Rios-Navarro A, Ramos JLS, Liouane N. Localizing unknown nodes with an FPGA-enhanced edge computing UAV in wireless sensor networks: implementation and evaluation. Pervasive Mob Comput. 2024;103:101961.
90. Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M. Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. IEEE Trans Veh Technol. 2020;69(8):9097–111.
91. Marchese M, Moheddine A, Patrone F. IoT and UAV integration in 5G hybrid terrestrial-satellite networks. Sensors. 2019;19(17):3704.
92. Gilani SM, Anjum A, Khan A, Syed MH, Moqurrab SA, Srivastava G. A robust internet of drones security surveillance communication network based on IOTA. Internet Things. 2024;25:101066.
93. Heidari A, Navimipour NJ, Unal M. A secure intrusion detection platform using blockchain and radial basis function neural networks for internet of drones. IEEE Internet Things J. 2023;10(10):8445–54.
94. Allan S, Barczyk M. A low-cost experimental quadcopter drone design for autonomous search-and-rescue missions in GNSS-denied environments. Drones. 2025;9(8):523.
95. Goel S, Kealy A, Lohani B. Development and experimental evaluation of a low-cost cooperative UAV localization network prototype. J Sens Actuator Netw. 2018;7(4):42.
96. Sheng Z, Li C, Qi X, Wu K, Ni W, Liu RP, et al. Beyond boundaries: synergizing SAR, UAV, and federated learning for flood mapping in Australia. IEEE Geosci Remote Sens Lett. 2026;23:4002605.
97. Wazid M, Bera B, Das AK, Garg S, Niyato D, Hossain MS. Secure communication framework for blockchain-based internet of drones-enabled aerial computing deployment. IEEE Internet Things Magaz. 2021;4(3):120–6.
98. Bera B, Chattaraj D, Das AK. Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment. Comput Commun. 2020;153:229–49.