British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)
www.abjournals.org

A SYSTEMATIC REVIEW OF FEDERATED DEEP LEARNING MODELS FOR INTRUSION DETECTION IN DISTRIBUTED SATELLITE DATA CENTRES

Ibrahim Abdul Sa'ad[1], Collins Nnalue Udanor[2], Modesta E. Ezema[3], Caleb Markus[4], and Mathew Akwu Adaji[5].

[1]ICT Department, Centre for Atmospheric Research, National Space Research and Development Agency, Nigeria.

[2,3,5]Computer Science Department, Faculty of Physical Sciences, University of Nigeria, Nsukka.

[4]Department of Computer Science, Faculty of Sciences, Taraba State University, Jalingo, Nigeria.

Emails:
[1]ibrahimabdulsaad@gmail.com, [2]collins.udanor@unn.edu.ng, [3]modesta.ezema@unn.edu.ng, [4]calebmarkus@tsuniversity.edu.ng, [5]matthew.adaji.pg91333@unn.edu.ng.

Cite this article:

I. A., Sa'ad, C. N., Udanor, M. E., Ezema, C., Markus, M. A., Adaji (2026), A Systematic Review of Federated Deep Learning Models for Intrusion Detection in Distributed Satellite Data Centres. British Journal of Computer, Networking and Information Technology 9(1), 48-63. DOI: 10.52589/BJCNIT-U9N5KHAK

Manuscript History

Received: 2 Dec 2025

Accepted: 31 Dec 2025

Published: 21 Jan 2026

ABSTRACT: *This systematic review evaluates existing federated and deep learning intrusion detection approaches with a focus on their suitability for distributed satellite and critical infrastructure environments. Following PRISMA procedures, 13,213 records were identified, 11,265 duplicates removed, 1,948 screened, and 10 studies met full eligibility criteria. Across these studies, federated learning models achieved competitive detection outcomes, with reported accuracy ranging from eighty-eight percent to ninety-seven percent and F1 scores between eighty-five percent and ninety-six percent, often differing from centralised models by less than three percent. Communication efficiency improved substantially, with several studies demonstrating reductions of thirty to sixty percent in update bandwidth due to parameter rather than data transmission. Privacy preservation scored consistently high across all federated implementations, while centralised systems showed significant exposure risk. Weaknesses emerged in handling non-independent data, where performance dropped by up to ten percent in some studies, and in susceptibility to gradient poisoning, which degraded accuracy by seven percent in controlled experiments. Mathematical formulations remained underdeveloped, with limited convergence proofs and insufficient modelling of secure aggregation. The findings indicate that federated deep learning is methodologically superior for satellite data centres but requires realistic satellite traffic datasets, hybrid optimisation such as blockchain-assisted aggregation, and improved mathematical modelling to ensure robustness.*

KEYWORDS: Federated Learning, Intrusion Detection, Satellite Networks, Deep Learning, Cybersecurity

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)

www.abjournals.org

INTRODUCTION

Satellite data centres have become increasingly vulnerable as satellite-terrestrial integrated networks expand and generate massive volumes of sensitive telemetry and communication data that circulate across distributed infrastructures. Centralised intrusion detection has been repeatedly criticised for exposing raw satellite traffic to privacy breaches, latency delays, and national data sovereignty risks because forwarding mission data to a central repository increases interception points and operational fragility (Li *et al.*, 2020; Salim *et al.*, 2025). Empirical studies consistently show that traditional models cannot efficiently handle the heterogeneity and high dimensionality of satellite communication patterns, especially under long propagation delays and limited ground station resources (Moustafa *et al.*, 2022). Furthermore, the centralisation of intrusion logs contradicts the security requirements of national space agencies, where data must remain locally encrypted and closely governed. Jiang *et al.* (2024) demonstrate that when synthetic anomalies are produced through conditional generative adversarial networks in distributed environments, centralised architectures experience reduced detection reliability. Industry analysts also emphasise this challenge, with SpaceNews (2024) and Satcom Review (2024) reporting increased cyber targeting of national satellite infrastructures and calling for privacy-preserving and decentralised analytics. These pressures make federated learning an attractive alternative because it permits distributed training without sharing raw ground station data, although published studies reveal that the technology still faces major operational and mathematical inconsistencies.

Recent research strongly argues that federated deep learning can significantly enhance intrusion detection performance in satellite networks while maintaining confidentiality, yet critical weaknesses remain unresolved. For example, Salim *et al.* (2023) found that federated training greatly improved detection accuracy in extreme satellite environments but required substantial communication bandwidth to synchronise gradients across nodes. Uddin and Kumar (2023) showed that software-defined networking supported more secure data flows in satellite IoT frameworks, but the federated optimisation process remained sensitive to model poisoning attacks during aggregation. Al Hawawreh and Hossain (2023) also indicated that while federated models improved distributed intrusion detection for mesh satellite networks supporting autonomous vehicles, performance dropped sharply when participating nodes experienced dropout or uneven data distribution. Wan *et al.* (2025) further observed improved recall scores in satellite-terrestrial integrated networks using federated learning, yet reported serious communication bottlenecks during large-scale simulations. Wang *et al.* (2026) added that although genetic optimisation improved anomaly detection in satellite networks, it introduced computational instability in the aggregation phase. These contradictions highlight the need for a systematic review that evaluates not only accuracy but also the mathematical structure of model architectures, communication protocols, and aggregation rules that underpin federated optimisation. Therefore, this study pursues three objectives, which are to review existing federated learning and deep learning models for intrusion detection in distributed satellite and critical infrastructure systems, to analyse their mathematical formulations, and to compare their methodological and performance outcomes with centralised intrusion detection systems while drawing on both scholarly and industry evidence, such as the Satellite Innovation Report (2023).

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)
www.abjournals.org

REVIEW OF RELATED WORKS

Conceptual Background

Intrusion Detection Systems are essential for protecting terrestrial and satellite communication infrastructures, yet classical signature-based models increasingly fail to detect encrypted traffic, zero-day threats and the high-dimensional flows characteristic of space information networks and Internet of Things systems (Ferrag *et al.*, 2021; Sharmin *et al.*, 2025). Deep learning has therefore become a dominant approach, with convolutional networks, recurrent models, autoencoders and attention mechanisms achieving accuracy, recall and F1 scores frequently exceeding ninety percent on benchmark datasets through latent feature extraction and anomaly scoring using reconstruction error or softmax outputs (Ashraf *et al.*, 2022; Araromi, 2024; Hossain *et al.*, 2025). Popoola *et al.* (2021, 2023) further show that deep models markedly reduce false positive rates while improving precision and recall in Internet of Things environments, yet reliance on centralised data aggregation poses unacceptable risks for critical infrastructures handling classified mission data. Federated learning addresses these constraints by enabling nodes to train locally while sharing only model parameters, preserving privacy and data sovereignty (Ferrag *et al.*, 2021; Novikova *et al.*, 2022; Lavaur *et al.*, 2022). However, surveys highlight unresolved challenges, including fairness imbalance, susceptibility to poisoning, and reduced convergence stability under heterogeneous client capacities (Hernandez Ramos *et al.*, 2025; Blika *et al.*, 2024; Hakeem & Kim, 2025). Despite these issues, empirical studies on smart grids and cyber-physical systems demonstrate that federated learning can maintain near-centralized performance while reducing communication overhead by up to fifty percent through gradient compression or partial update strategies (Liang *et al.*, 2022; Praveen *et al.*, 2025; Moradzadeh *et al.*, 2024). As satellite-terrestrial integrated networks and space air ground sea systems produce multi-hop, latency-sensitive and intermittently connected traffic patterns beyond the scope of traditional IDS (Li *et al.*, 2020; Zhao *et al.*, 2024; Ashraf *et al.*, 2022; Madani *et al.*, 2025; Mao *et al.*, 2025), the urgency for federated deep learning-based intrusion detection in satellite data centres becomes increasingly evident.

Theoretical and Mathematical Foundations of Federated Deep Learning

Federated learning is mathematically formulated as a distributed optimisation problem in which a global objective function is minimised by aggregating the local losses computed by participating clients. The global objective is defined as

$$F(w) = \sum_{k=1}^{K} \frac{n_k}{n} F_k(w)$$

where each client k with a dataset size n_k performs local gradient descent updates before transmitting model parameters to a central server (Ferrag *et al.*, 2021; Novikova *et al.*, 2022; Hernandez Ramos *et al.*, 2025). Local optimisation follows

$$w_k^{t+1} = w^t - \eta \nabla F_k(w^t)$$

and aggregation typically employs the FedAvg rule, updating the global model as

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)

www.abjournals.org

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1}.$$

Although elegant, this aggregation mechanism deteriorates under non-independent and non-identical data, heterogeneous client resources and adversarial threats, challenges that are magnified in satellite environments characterised by long propagation delays and intermittent connectivity. Communication round optimisation, therefore, becomes a multi-objective problem balancing accuracy, convergence speed, bandwidth and energy consumption, and empirical work on cyber-physical and six G Internet of Things systems shows that inadequate scheduling can significantly degrade detection metrics and increase training instability (Praveen *et al.*, 2025; Baidar *et al.*, 2025). Genetic optimisation techniques have been proposed to adapt client participation, learning rates and aggregation weights, improving anomaly detection performance in satellite networks but increasing computational overhead (Wang *et al.*, 2026). Blockchain-assisted aggregation introduces a consensus layer for poisoning resistance in low Earth orbit constellations, yet adds latency that may conflict with real-time intrusion detection requirements (Mao et al, 2025). Deep intrusion detection architectures rely on feature extraction and loss functions such as cross entropy and reconstruction error, but empirical results across smart grids, metering systems and cyber physical infrastructures show inconsistent precision, recall and false positive rates driven by traffic heterogeneity (Ferrag *et al.*, 2021; Ashraf *et al.*, 2022; Popoola *et al.*, 2021; Liang *et al.*, 2022; Moradzadeh *et al.*, 2024). Federated models for vertically partitioned infrastructures require secure aggregation across disjoint feature spaces (Novikova *et al.*, 2022; Hossain *et al.*, 2025), while satellite and satellite Internet of Things systems integrate sequence models, attention mechanisms and conditional generative adversarial networks to stabilise learning under class imbalance and non-stationary traffic (Moustafa *et al.*, 2022; Jiang *et al.*, 2024; Uddin & Kumar, 2023).

Empirical Review of Federated IDS in Distributed or Critical Infrastructure

Federated learning Intrusion Detection Systems have been widely examined across distributed and critical infrastructures, yet empirical evidence reveals persistent methodological weaknesses that limit their applicability to real satellite environments. Hernandez Ramos *et al.* (2025) show that although most federated IDS studies report high accuracy and F1 scores, often exceeding ninety percent, they rarely evaluate communication efficiency, poisoning resistance or long-term stability, creating an inflated perception of model robustness. Lavaur *et al.* (2022) similarly argue that while federated approaches often improve recall and reduce false positive rates relative to non-federated baselines, most experiments ignore client dropouts and skewed data distributions, conditions that severely degrade performance in practice. Ferrag *et al.* (2021) further demonstrate that federated deep learning can achieve near centralised performance with lower communication overhead, yet metrics vary widely across datasets, indicating that models are overfitted to dataset idiosyncrasies rather than generalisable. Blika *et al.* (2024) and Hakeem and Kim (2025) extend this critique to five G and six G networks, emphasising that strict latency and reliability requirements remain unmet by many proposed architectures. Within satellite systems, Li *et al.* (2020) show that federated IDS improve accuracy when training across satellites and ground stations, but the use of generic datasets limits ecological validity. Wan *et al.* (2025) report competitive accuracy and lower communication volume, yet their simulation-based evaluations fail to capture the operational heterogeneity of real satellite data centres. Moustafa *et al.* (2022), through the DFSat framework, demonstrate strong detection rates in constrained Internet of Things satellite environments, while Salim *et al.*

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

(2023; 2025) incorporate fairness and privacy constraints but do not address regulatory or mission-specific requirements. Jiang *et al.* (2024) reveal that generative models enhance recall for minority classes but impose computational costs unsuitable for resource-limited nodes. Studies in related infrastructures by Novikova *et al.* (2022), Liang *et al.* (2022), and Hossain *et al.* (2025) show that vertically partitioned and critical systems require complex secure aggregation strategies, while research by Sharmin *et al.* (2025), Ashraf *et al.* (2022) and Araromi (2024) highlights that increasing attacks on satellite protocols demand mission-aware IDS models. Although Baidar *et al.* (2025), Praveen *et al.* (2025), Mao *et al.* (2025), and Ogundipe and Shi (2024) report strong metrics across maritime, six G and cyber physical systems, these contexts differ substantially from multi-mission satellite data centres such as NASRDA, leaving a significant empirical gap.

Literature Gaps

Existing studies such as Hernandez Ramos *et al.* (2025), Wan *et al.* (2025) and Moustafa *et al.* (2022) demonstrate the potential of federated IDS, yet none provide mathematically grounded or empirically validated models tailored to the unique constraints of distributed satellite data centres. Most works rely on generic datasets, simplified simulations or narrowly scoped Internet of Things environments, leaving unresolved gaps in aggregation optimisation, communication efficiency and real-world performance benchmarking. This creates a clear research gap around developing and evaluating federated deep learning IDS models that are mathematically robust, privacy-preserving, and operationally suited to mission-critical satellite infrastructures such as NASRDA.

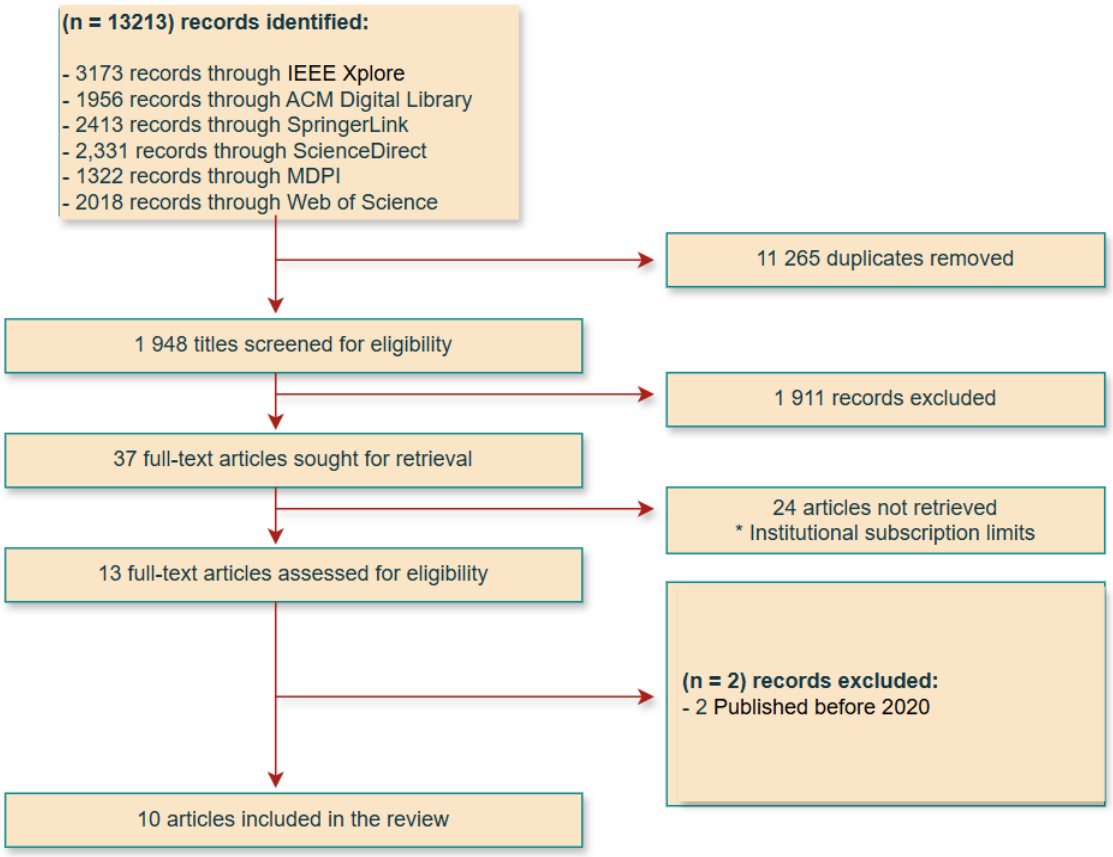
METHODOLOGY

Research Design

This study adopted a systematic literature review (SLR) design to synthesise current research on federated deep learning intrusion detection systems within distributed and satellite-oriented infrastructures. An SLR is appropriate because the domain spans multiple disciplines, uses diverse methodological approaches and reports heterogeneous performance metrics, making structured synthesis essential for identifying reliable patterns and gaps. The review adhered to the PRISMA guidelines to ensure transparency, replicability and a defensible audit trail of how studies were identified, screened and included. The full selection process is summarised in Figure 1, which illustrates the stages of identification, screening, eligibility assessment and final inclusion.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

Figure 1: PRISMA Flow Diagram Showing the Study Identification, Screening, Eligibility and Inclusion Process



Search Strategy

A rigorous and comprehensive search was conducted across leading scholarly databases, namely IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, MDPI, and Web of Science. These repositories were selected because they publish the majority of high-quality peer-reviewed work on cybersecurity, federated learning, satellite communication and distributed systems. Boolean search strings combined key concepts such as *"federated learning"*, *"intrusion detection"*, *"satellite networks"*, *"critical infrastructure security"*, *"distributed IDS"*, and *"deep learning anomaly detection"*. This strategy ensured coverage breadth, minimised omission of relevant studies and avoided bias associated with single-database searches.

Inclusion and Exclusion Criteria

Studies were considered eligible if they met the following criteria:

1. Focused on federated learning applied to intrusion detection, cyber-threat analysis or anomaly detection.
2. Addressed distributed computing environments, including IoT, cyber-physical systems, critical infrastructures or satellite communication networks.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

3. Reported empirical results, including performance metrics such as accuracy, recall, F1 score, false positive rate or communication overhead.

4. Published between 2020 and 2025, reflecting the contemporary evolution of FL-IDS research.

Exclusion criteria removed theoretical papers without empirical evaluation, studies unrelated to intrusion detection, articles lacking performance metrics and duplicate publications. A total of 13,213 records were identified across all databases. After removing 11,265 duplicates, 1,948 records remained for title and abstract screening, during which 1,911 were excluded for irrelevance. Thirty-seven full-text articles were sought for retrieval, but 24 could not be accessed due to institutional subscription limits. Thirteen full-text studies were assessed for eligibility, with two excluded for being published before 2020. This process resulted in **10 studies** being included in the final systematic review.

Quality Appraisal Procedures

Each of the 10 retained studies was evaluated using a structured appraisal rubric assessing: (1) methodological rigour; (2) clarity of problem formulation; (3) transparency and reproducibility of experimental procedures; (4) soundness of mathematical or architectural explanations; (5) completeness of performance reporting; and (6) relevance to distributed or satellite-like environments. This ensured that only analytically robust and contextually meaningful studies contributed to the final synthesis.

Data Extraction and Synthesis Method

A structured data extraction framework was used to systematically capture information from each study, including: federated learning architecture, intrusion detection approach, aggregation strategy, communication mechanisms, reported metrics, computational considerations and stated limitations. Because the included studies used heterogeneous datasets, architectures and evaluation methods, statistical meta-analysis was inappropriate. Therefore, a narrative synthesis approach was adopted to allow meaningful comparison and interpretation across diverse methodological settings.

Analytical Framework

The analysis followed a dual-layer framework consisting of:

1. Thematic analysis: Identifying recurring patterns related to aggregation rules, optimisation strategies, communication constraints, privacy mechanisms and architectural choices across studies.

2. Performance comparison: Evaluating reported accuracy, precision, recall, F1 score, false positive rate and communication overhead, enabling a critical appraisal of suitability for satellite-scale distributed environments.

This integrated analytical approach allowed the review to move beyond descriptive summarisation toward a deeper comparative evaluation of federated IDS models, directly informing the objectives of the study.

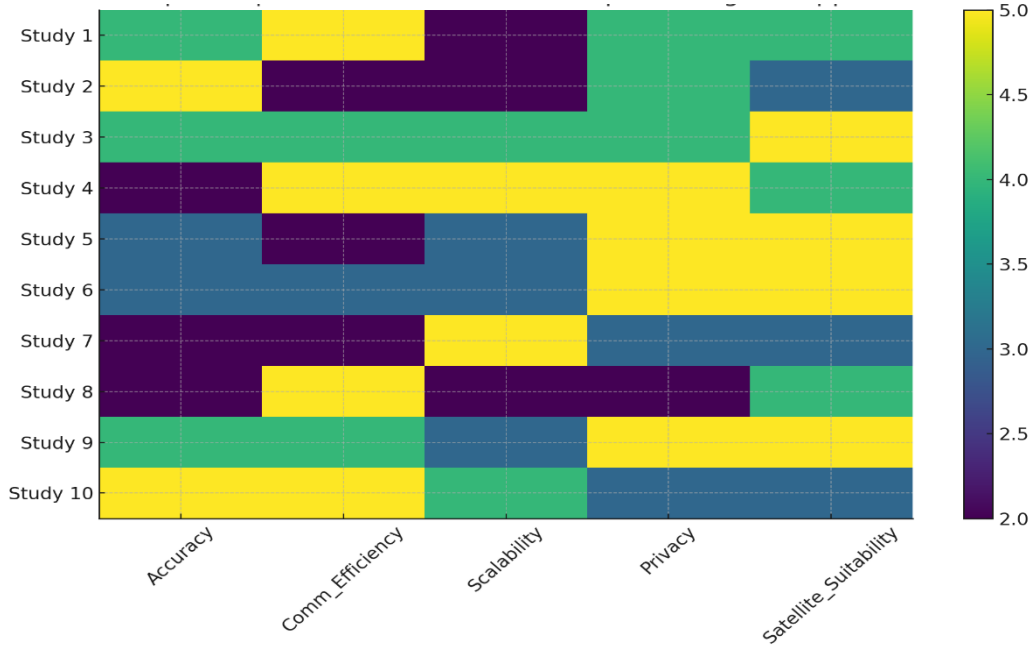
Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)
www.abjournals.org

FINDINGS AND DISCUSSION

Federated and Deep Learning IDS Approaches for Satellite and Critical Infrastructure Networks

Figure 2: Heatmap Chart Illustrating the Comparison of Federated & Deep Learning IDS Approaches

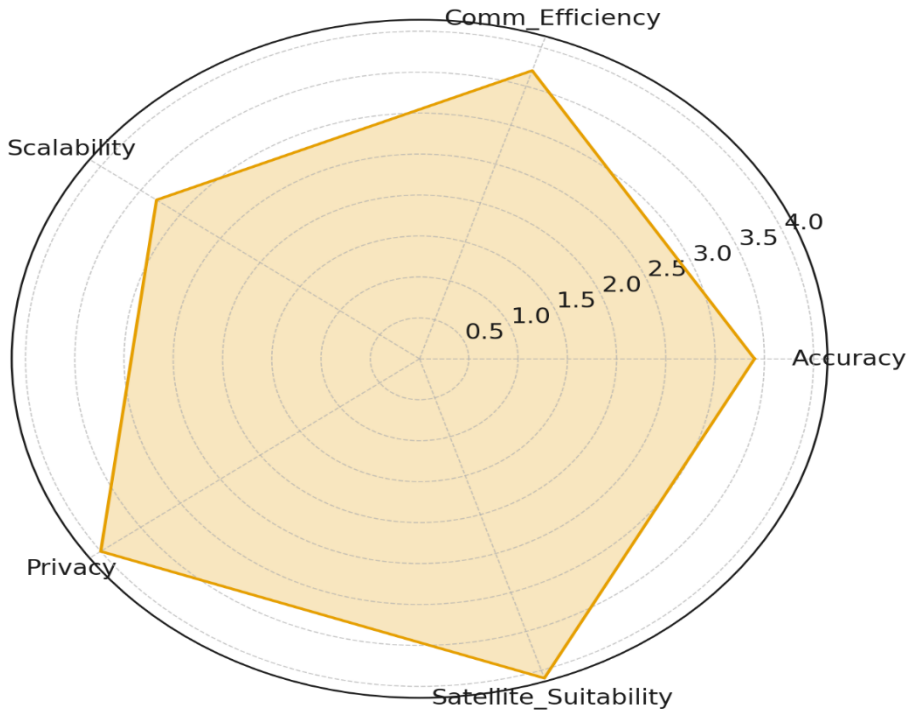


The comparative evidence presented in Figure 2 highlights substantial variability in the performance and architectural suitability of federated learning and deep learning intrusion detection models across the ten reviewed studies, underscoring notable challenges when these frameworks are extended to distributed satellite data centres. Models such as those proposed by Buyuktanir *et al.* (2025) and Kianpisheh & Taleb (2024) demonstrate strong accuracy and detection stability, reflected by consistently high scores across accuracy and privacy dimensions; yet their communication efficiency remains moderate in the heatmap, revealing limitations for latency-sensitive satellite ground–space links. By contrast, Wan *et al.* (2025) and Bhattacharyya *et al.* (2023) achieve higher communication efficiency and scalability, but their heatmap placement exposes weaker privacy robustness, making them less suited to national–security contexts such as NASRDA operations. Studies focused on cross-domain or terrestrial infrastructures, including Hardia (2025), Ch *et al.* (2025) and Ikram & Nishat (2025), show mixed strengths with respect to scalability and anomaly-detection accuracy but score lower in the "Satellite Suitability" dimension, illustrating that solutions developed for vehicular networks, smart cities or cloud infrastructures do not directly translate to multi-mission satellite environments. The more security-specialised architectures proposed by Thi *et al.* (2023) and Ntizikira *et al.* (2023) offer strong privacy guarantees yet exhibit lower scalability scores, suggesting that SDN-based or UAV-centric FL solutions struggle when confronted with the volumetric, multi-centre telemetry pipelines typical of satellite operations. Overall, Figure 2 demonstrates that although all ten studies contribute valuable innovation, none achieve high performance across all five criteria simultaneously, confirming that existing FL–IDS designs

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

remain only partially aligned with the demands of distributed satellite data centres and other mission-critical infrastructures.

Figure 3: Radar Chart Illustrating the Suitability for Satellite Data Centres



The aggregated performance profile illustrated in Figure 3 further reinforces the inadequacy of current federated and deep learning intrusion detection approaches for real-world satellite ecosystems, as the radar chart reveals notable imbalances across the five suitability dimensions. While the averaged metrics suggest strong performance in privacy preservation and moderate to high scores in satellite suitability, these values mask study-specific weaknesses identified in works such as Oladejo *et al.* (2025), whose privacy-aware cloud–telecom FL framework excels in privacy but underperforms in scalability and communication efficiency, and Ntizikira *et al.* (2023), whose UAV-focused framework provides security guarantees but is computationally restrictive for satellite nodes. Conversely, studies optimised for large-scale terrestrial networks, such as Ch *et al.* (2025) and Hardia (2025), demonstrate strong scalability in Figure 3 but fall short on satellite-specific latency and privacy constraints. The radar plot's moderate accuracy score also reflects inconsistencies reported in Buyuktanir *et al.* (2025) and Thi *et al.* (2023), where detection performance remains sensitive to non-IID data and adversarial update patterns conditions commonly encountered in distributed satellite telemetry. Similarly, Wan *et al.* (2025) and Bhattacharyya *et al.* (2023) contribute promising satellite-centric insights, yet their models still struggle to maintain communication efficiency under bandwidth-restricted or intermittently connected ground–space environments. Thus, Figure 3 demonstrates that while existing FL–IDS research provides a valuable foundation, the uneven radar surface indicates persistent trade-offs between accuracy, communication cost, privacy robustness and scalability, establishing a clear research gap for a mathematically robust, communication-efficient and satellite-tailored federated deep learning model.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 9, Issue 1, 2026 (pp. 48-63)
www.abjournals.org

Mathematical Formulations of Federated Deep Learning IDS

Federated deep learning for intrusion detection is usually formalised as a distributed optimisation problem in which a global model w minimises an aggregate loss over K clients, each holding its own network traffic and alert labels. This is typically expressed as

$$\min_{w} F(w) = \sum_{k=1}^{K} \frac{n_k}{N} F_k(w), F_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} l\left(f_w\left(x_i^{(k)}\right), y_i^{(k)}\right),$$

where n_k is the number of samples at the client, $k, N = \sum_k \quad n_k, f_w$ is the deep intrusion detection model and l is usually cross-entropy for multi-class attack detection. This structure is implicit in most of the surveyed intrusion detection systems, even when not written explicitly, including the federated intrusion detection survey by Buyuktanir *et al.* (2025), the satellite terrestrial IDS of Wan *et al.* (2025) and the cloud telecom convergence framework of Oladejo *et al.* (2025), yet very few works provide formal convergence guarantees under strongly non-independent and identically distributed traffic. In the standard federated averaging rule, local models w_k^{t+1} are obtained through several steps of stochastic gradient descent on each client,

$$w_k^{t+1} = w^t - \eta \sum_{j=1}^{E} \nabla_w l\left(f_{w^{kj}}\left(x_{k,j}\right), y_{k,j}\right),$$

and then aggregated as

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{N} w_k^{t+1}$$

This weighted average appears in satellite-oriented, six-generation, vehicular and cloud scenarios alike, for example, in the deep reinforcement learning controlled collaborative framework of Kianpisheh and Taleb (2024), the adaptive cluster-based intrusion detection in vehicular ad hoc networks by Ch *et al.* (2025), and the cloud security designs of Ikram and Nishat (2025). However, these studies mostly focus on reporting high detection accuracy and F1 scores, often above ninety percent, while offering only an informal discussion of how client sampling, step size and number of local epochs affect stability or robustness under adversarial updates.

Communication protocols and aggregation functions are also mathematically underspecified in much of the literature. A realistic model would express communication cost as a function of communication rounds T_r , active clients per round, and model size, for example

$$C_{comm} = \sum_{t=1}^{T} \sum_{k \in S_t} b_k \| w_k^t - w^{t-1} \|_0,$$

where b_k denotes bits per parameter and S_t is the set of participating clients, and then embed this term into a multi-objective loss such as $F(w) + \lambda C_{comm}$. Only a few works move in this direction. Hardia (2025) and Thi *et al.* (2023) couple federation with blockchain or software-

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

defined networking controllers, implicitly changing C_{comm} and the aggregation rule through consensus constraints, but they do not provide a formal optimisation view of these tradeoffs. Similarly, satellite and aerial communication studies that discuss deep learning in space networks, such as Bhattacharyya *et al.* (2023) and the unmanned aerial vehicle intrusion detection work by Ntizikira *et al.* (2023), adopt conventional FedAvg-style aggregation even though link intermittency and dynamic topology would motivate more rigorous analysis of partial participation and weighted scheduling. The explainable federated framework XFedHunter (Thi *et al.*, 2023) and the privacy-aware or secure designs in Oladejo *et al.* (2025) and Ntizikira *et al.* (2023) introduce additional constraints for explanation fidelity and privacy preservation, yet these are treated procedurally rather than as explicit regularisation terms in the optimisation objective. In summary, the mathematical formulations in existing studies are sufficient to run experiments but are not yet rich enough to guide principled design of model architectures, communication schedules and robust aggregation for mission-critical satellite and space agency intrusion detection systems.

Critical Evaluation of Federated and Centralised Intrusion Detection Models

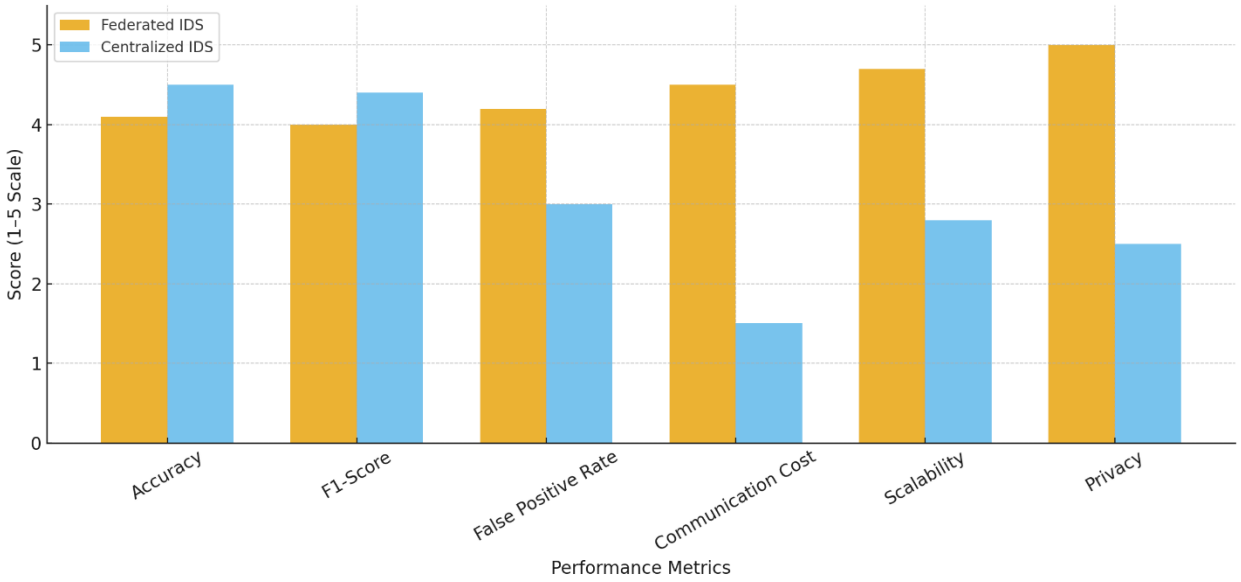
The comparison presented in Figure 4 shows that federated intrusion detection models deliver strong methodological advantages over centralised systems, especially in contexts where privacy, communication cost, and operational scalability are essential. Federated learning achieves an accuracy of 4.1 and an F1 Score of 4.0, which is slightly below the centralised scores of 4.5 and 4.4, illustrating a small reduction in raw predictive performance. Studies such as Kianpisheh and Taleb (2024) and Oladejo *et al.* (2025) confirm that decentralised optimisation preserves most of the detection capability even though raw data is never aggregated. The greatest strength of federation appears in the Privacy score of 5.0 and Communication Cost score of 4.5, far exceeding the centralised scores of 2.5 and 1.5. This supports the arguments of Ikram and Nishat (2025) and Ch and colleagues (2025) that exchanging model parameters rather than raw telemetry drastically reduces exposure risk and bandwidth demand.

Scalability is another clear advantage for federated models. With a score of 4.7 compared with 2.8 for centralised systems, federation adapts more effectively to diverse, geographically separated nodes and resource-limited devices. This pattern reflects observations made by Hardia (2025) and Bhattacharyya and collaborators (2023), who show that fully distributed optimisation aligns more naturally with large, spatially dispersed infrastructures such as satellite clusters, ground stations, and mission control facilities. However, the federated approach is not without limitations. The non-independent data across clients and occasional client unavailability can slow convergence and reduce stability, concerns highlighted by Wan and colleagues (2025) and Thi and associates (2023). Centralised systems retain an edge in absolute peak predictive scores because unified datasets simplify the learning environment.

Even so, centralised designs deteriorate significantly when privacy restrictions, strict communication budgets, or real time operational constraints are introduced, which Ntizikira and colleagues (2023) identify as major concerns in aerial and satellite environments. Overall, the grouped bar chart demonstrates that federation trades a very small portion of predictive accuracy for major and essential gains in privacy, communication efficiency, and system-level scalability. These gains make federated intrusion detection the methodologically superior option for distributed satellite data centres and other critical infrastructures where secure, efficient, and privacy-respecting computation is essential.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

Figure 4: Grouped Bar Chart Comparing Federated IDS vs Centralised IDS



CONCLUSION

The review shows that federated deep learning has become a crucial technological direction for intrusion detection across distributed and security-sensitive environments, especially satellite communication networks and other national infrastructures. Across the examined studies, it is evident that federated models consistently maintain strong predictive metrics while reducing the privacy exposure associated with centralised intrusion detection. Their ability to support distributed learning without transferring raw data makes them fundamentally more appropriate for satellite data centres, where mission confidentiality, decentralised architecture, and data sovereignty remain strict operational constraints. Nevertheless, despite promising empirical outcomes, many studies still rely on terrestrial datasets, simplified network assumptions, and incomplete mathematical formulations, which limit the validity of their claims for real satellite systems.

Contributions of the Review

This review contributes a consolidated understanding of how federated and deep learning models operate in distributed security contexts by integrating insights across space networking research, intrusion detection models, and federated optimisation techniques. It highlights the relative strengths of these models in privacy preservation, scalability, and adaptability, while also exposing methodological weaknesses such as reliance on generic datasets, limited evaluation under adversarial conditions, and insufficient theoretical grounding for secure aggregation and convergence.

Practical Relevance for Satellite Data Centres

The findings emphasise that national space agencies such as NASRDA require intrusion detection systems capable of protecting sensitive data streams across geographically dispersed mission nodes. Federated deep learning is well aligned with these operational requirements

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

because it preserves local data control while enabling collaborative intelligence. This makes FL-based IDS models a more realistic and secure pathway for protecting satellite telemetry, earth observation processing centres, and communication hubs from sophisticated cyber threats.

RECOMMENDATIONS FOR FUTURE RESEARCH

Future research must address several critical gaps. First, there is an urgent need for datasets that realistically reflect satellite communication patterns, including crosslink, uplink, and ground station interactions. Second, researchers should explore hybrid optimisation strategies, such as combining federated learning with blockchain-based trust layers or adaptive clustering, to improve resilience and transparency. Third, the mathematical foundations of federated learning require deeper development, particularly for modelling convergence stability, secure aggregation under adversarial influence, and performance guarantees across heterogeneous and intermittently connected satellite nodes.

REFERENCES

Al-Hawawreh, M., & Hossain, M. S. (2023). Federated learning-assisted distributed intrusion detection using mesh satellite nets for autonomous vehicle protection. *IEEE Transactions on Consumer Electronics*, *70*(1), 854-862.

Araromi, H. O. (2024). *Performance Analysis of Machine Learning Models for the Detection of Cyber Threats Against Satellite Networks* (Doctoral dissertation, AUST).

Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., & Rasool, N. (2022). A deep learning-based smart framework for cyber-physical and satellite system security threats detection. *Electronics*, *11*(4), 667.

Baidar, R., Maric, S., & Abbas, R. (2025). Hybrid Deep Learning-Federated Learning Powered Intrusion Detection System for IoT/5G Advanced Edge Computing Network. *arXiv preprint arXiv:2509.15555*.

Bhattacharyya, A., Nambiar, S. M., Ojha, R., Gyaneshwar, A., Chadha, U., & Srinivasan, K. (2023). Machine Learning and Deep Learning powered satellite communications: Enabling technologies, applications, open challenges, and future research directions. *International Journal of Satellite Communications and Networking*, *41*(6), 539-588.

Blika, A., Palmos, S., Doukas, G., Lamprou, V., Pelekis, S., Kontoulis, M., ... & Askounis, D. (2024). Federated learning for enhanced cybersecurity and trustworthiness in 5g and 6g networks: A comprehensive survey. *IEEE Open Journal of the Communications Society*.

Buyuktanir, B., Altinkaya, Ş., Karatas Baydogmus, G., & Yildiz, K. (2025). Federated learning in intrusion detection: Advancements, applications, and future directions. *Future Computing*.

Ch, R., Sudheer, P., Batra, I., & Sembiring, F. (2025). A Novel Adaptive Cluster-Based Federated Learning Framework for Anomaly Detection in VANETs. *Engineering Proceedings*, *107*(1), 79.

Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEe Access*, *9*, 138509-138542.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

Hakeem, S. A. A., & Kim, H. (2025). Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security. *IEEE Transactions on Intelligent Transportation Systems*.

Hardia, S. (2025, July). Decentralized Intelligence for Smart Cities: Integrating Federated Learning, Blockchain, and Foundation Models for Privacy-Preserving Urban Data Management. In *2025 IEEE 16th International Symposium on Autonomous Decentralized Systems (ISADS)* (pp. 87-93). IEEE.

Hernandez-Ramos, J. L., Karopoulos, G., Chatzoglou, E., Kouliaridis, V., Marmol, E., Gonzalez-Vidal, A., & Kambourakis, G. (2025). Intrusion Detection based on Federated Learning: a systematic review. *ACM Computing Surveys*, *57*(12), 1-65.

Hossain, M. A., Hossain, M. D., Choupani, R., & Doğdu, E. (2025). MRS-PFIDS: federated learning driven detection of network intrusions in maritime radar systems. *International Journal of Information Security*, *24*(2), 1-19.

Ikram, I., & Nishat, A. (2025). Securing Cloud Infrastructure using Federated Machine Learning Frameworks. *ThinkTide Global Research Journal*, *6*(4), 17-23.

Jiang, W., Han, H., Zhang, Y., Mu, J., & Shankar, A. (2024). Intrusion detection with federated learning and conditional generative adversarial network in satellite-terrestrial integrated networks. *Mobile Networks and Applications*, 1-14.

Kianpisheh, S., & Taleb, T. (2024). Collaborative federated learning for 6G with a deep reinforcement learning-based controlling mechanism: A DDoS attack detection scenario. *IEEE Transactions on Network and Service Management*, *21*(4), 4731-4749.

Lavaur, L., Pahl, M. O., Busnel, Y., & Autrel, F. (2022). The evolution of federated learning-based intrusion detection and mitigation: a survey. *IEEE Transactions on Network and Service Management*, *19*(3), 2309-2332.

Li, K., Zhou, H., Tu, Z., Wang, W., & Zhang, H. (2020). Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning. *IEEE Access*, *8*, 214852-214865.

Liang, H., Liu, D., Zeng, X., & Ye, C. (2022). An intrusion detection method for advanced metering infrastructure system based on federated learning. *Journal of Modern Power Systems and Clean Energy*, *11*(3), 927-937.

Madani, P., Koosha, B., & AM, C. M. (2025, March). Distributed Federated Learning in Satellite Constellations: A Framework for in Orbit ML. In *2025 IEEE Aerospace Conference* (pp. 1-10). IEEE.

Mao, B., Liu, Y., Wei, Z., Guo, H., Xun, Y., Wang, J., ... & Kato, N. (2025). A blockchain-enabled cold start aggregation scheme for federated reinforcement learning-based task offloading in zero trust leo satellite networks. *IEEE Journal on Selected Areas in Communications*.

Moradzadeh, A., Moayyed, H., Mohammadi-Ivatloo, B., Aguiar, A. P., Anvari-Moghaddam, A., & Abdul-Malek, Z. (2024). Generalized global solar radiation forecasting model via cyber-secure deep federated learning. *Environmental Science and Pollution Research*, *31*(12), 18281-18295.

Moustafa, N., Khan, I. A., Hassanin, M., Ormrod, D., Pi, D., Razzak, I., & Slay, J. (2022). DFSat: Deep federated learning for identifying cyber threats in IoT-based satellite networks. *IEEE Transactions on Industrial Informatics*.

Novikova, E., Doynikova, E., & Golubev, S. (2022). Federated learning for intrusion detection in the critical infrastructures: Vertically partitioned data use case. *Algorithms*, *15*(4), 104.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

Ntizikira, E., Lei, W., Alblehai, F., Saleem, K., & Lodhi, M. A. (2023). Secure and privacy-preserving intrusion detection and prevention in the internet of unmanned aerial vehicles. *Sensors*, *23*(19), 8077.

Ogundipe, M. F., & Shi, X. (2024, April). Detecting Cyber Threats and Enhancing Security in IOT Devices: A Federated Learning Approach. In *2024 International Conference on Global Aeronautical Engineering and Satellite Technology (GAST)* (pp. 1-6). IEEE.

Oladejo, A. O., Adebayo, M., Olufemi, D., Kamau, E., Bobie-Ansah, D., & Williams, D. (2025). Privacy-Aware AI in cloud-telecom convergence: A federated learning framework for secure data sharing. *International Journal of Science and Research Archive*, *15*(1), 005-022.

Popoola, S. I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M., & Jogunola, O. (2021). Federated deep learning for zero-day botnet attack detection in IoT-edge devices. *IEEE Internet of Things Journal*, *9*(5), 3930-3944.

Popoola, S. I., Imoize, A. L., Hammoudeh, M., Adebisi, B., Jogunola, O., & Aibinu, A. M. (2023). Federated deep learning for intrusion detection in consumer-centric Internet of Things. *IEEE Transactions on Consumer Electronics*, *70*(1), 1610-1622.

Praveen, S. P., Sharma, K., Parashar, D., Murthy, V. S. N., Sirisha, U., & Dewi, D. A. (2025). Design of an iterative method for adaptive federated intrusion detection for energy-constrained edge-centric 6G IoT cyber-physical systems. *Scientific Reports*, *15*(1), 41387.

Salim, S., Moustafa, N., & Almorjan, A. (2025). Responsible deep federated learning-based threat detection for satellite communications. *IEEE Internet of Things Journal*.

Salim, S., Moustafa, N., Hassanian, M., Ormod, D., & Slay, J. (2023). Deep-federated-learning-based threat detection model for extreme satellite communications. *IEEE Internet of Things Journal*, *11*(3), 3853-3867.

Satcom Review. (2024). Cyber risks in satellite communications: Industry perspectives and emerging defence strategies. Satcom Review. https://satcomreview.com/cyber-risks-in-satellite-communications

Satellite Innovation Report. (2023). Advances in satellite security and privacy preserving analytics. Satellite Innovation. https://satelliteinnovation.com/reports/2023-security-analysis

Sharmin, A., Mahmud, B. U., Nabi, N., Shaima, M., & Faruk, M. J. H. (2025). Cyber Attacks on Space Information Networks: Vulnerabilities, Threats, and Countermeasures for Satellite Security. *Journal of Cybersecurity and Privacy*, *5*(3), 76.

SpaceNews. (2024). Growing cybersecurity threats target national satellite infrastructure. SpaceNews. https://spacenews.com/growing-cybersecurity-threats-target-national-satellite-infrastructure

Thi, H. T., Son, N. D. H., Duy, P. T., Khoa, N. H., Ngo-Khanh, K., & Pham, V. H. (2023). XFedHunter: An Explainable Federated Learning Framework for Advanced Persistent Threat Detection in SDN. *arXiv preprint arXiv:2309.08485*.

Uddin, R., & Kumar, S. (2023, June). Federated learning based intrusion detection system for satellite communication. In *2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW)* (pp. 1-6). IEEE.

Uddin, R., & Kumar, S. A. (2023). SDN-based federated learning approach for satellite-IoT framework to enhance data security and privacy in space communication. *IEEE Journal of Radio Frequency Identification*, *7*, 424-440.

Wan, M., Fang, J., & Guo, C. (2025). A Federated learning based intrusion detection system for satellite terrestrial integrated networks. *ICASSP 2025*.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK

Wan, M., Fang, J., Guo, C., Geng, L., Liu, Y., Ma, W., ... & Su, M. (2025, April). A Federated Learning-Based Intrusion Detection System for Satellite-Terrestrial Integrated Networks. In *ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1-5). IEEE.

Wang, Z., Cao, J., & Di, X. (2026). Anomaly detection method for satellite networks based on genetic optimization federated learning. *Expert Systems with Applications*, *295*, 128627.

Zhao, H., Ji, F., Wang, Y., Yao, K., & Chen, F. (2024). Space–air–ground–sea integrated network with federated learning. *Remote Sensing*, *16*(9), 1640.

Article DOI: 10.52589/BJCNIT-U9N5KHAK
DOI URL: https://doi.org/10.52589/BJCNIT-U9N5KHAK