World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Assessing Machine Learning Enabled Anomaly Detection Models for Real Time Cyberattack Mitigation in Optical Fiber Communication Systems.

Emmanuel Selorm Gabla [1], Amina Catherine Peter-Anyebe [2,*] and Onuh Matthew Ijiga [3]

[1] *Department of Information and Telecommunication, Scripps College of Communication, Ohio University, Athens, USA.*
[2] *Department of International Relations and Diplomacy, Federal University of Lafia, Nasarawa State, Nigeria.*
[3] *Department of Physics, Joseph Sarwaan Tarkaa University, Makurdi, Benue State, Nigeria.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(02), 001–017

Publication history: Received on 16 September 2025; revised on 30 October 2025; accepted on 01 November 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1454

Abstract

The increasing complexity and data throughput of optical fiber communication systems have made them critical yet vulnerable components of modern digital infrastructure. With the rapid growth of high-speed networks, ensuring cybersecurity in these systems requires intelligent, adaptive, and real-time mitigation strategies. This review examines the application of machine learning (ML)-enabled anomaly detection models for identifying and mitigating cyberattacks in optical fiber communication environments. It highlights how supervised, unsupervised, and reinforcement learning algorithms—such as Support Vector Machines (SVM), Random Forests, Deep Neural Networks (DNN), and Autoencoders—enable real-time detection of network anomalies, signal disruptions, and malicious intrusions. Furthermore, the paper explores the integration of hybrid ML frameworks combining statistical signal processing with deep learning for enhanced detection accuracy and low false alarm rates. Special emphasis is placed on the challenges of model interpretability, scalability, and latency in large-scale fiber networks, alongside the role of edge computing and federated learning in decentralized security monitoring. The study also evaluates emerging trends such as graph-based anomaly detection, explainable AI (XAI), and transfer learning approaches for resilient optical network protection. By synthesizing current methodologies, datasets, and performance metrics, this review provides a comprehensive perspective on the state-of-the-art in ML-driven anomaly detection and outlines research directions for achieving secure, autonomous, and self-healing optical communication systems.

Keywords: Machine Learning; Anomaly Detection; Cyberattack Mitigation; Optical Fiber Communication; Real-Time Security.

1. Introduction

1.1. Background and Motivation

Optical fiber communication systems form the backbone of modern digital infrastructure, offering unparalleled bandwidth, low latency, and high reliability. However, their increasing integration with software-defined networking (SDN) and Internet of Things (IoT) components has exposed them to sophisticated cyber threats capable of disrupting large-scale data transmission (Prakash, & Kasthuri, 2024). The emergence of machine learning (ML)-enabled anomaly detection has revolutionized how network vulnerabilities are identified and mitigated in real time. Advanced architectures such as convolutional autoencoders and hybrid recurrent models allow optical systems to detect deviations in light intensity patterns, polarization shifts, and transmission anomalies long before service disruption occurs (Brian, & Alexander, 2023). These models not only enhance the accuracy of anomaly detection but also reduce

* Corresponding author: Amina Catherine Peter-Anyebe.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Lscense 4.0.

false alarm rates critical for ensuring continuity in latency-sensitive applications such as financial transactions, telemedicine, and military communications.

The motivation for this review arises from the growing convergence of AI-driven security and fiber-optic infrastructure management. Research has demonstrated that applying machine learning frameworks for anomaly detection in optical networks significantly improves early threat mitigation by learning from traffic patterns and environmental noise fluctuations (Amebleh & Igba, 2024). Moreover, with increasing cyberattack sophistication including distributed denial-of-service (DDoS) and side-channel attacks quantum-resistant cryptographic protocols and predictive analytics frameworks have become essential (Idika, 2023). The integration of explainable AI and real-time data analytics ensures not only rapid detection but also actionable interpretability, creating resilient and adaptive optical network environments capable of sustaining secure global communications.

1.2. Importance of Cybersecurity in Optical Fiber Communication Systems

Cybersecurity in optical fiber communication systems is fundamental to preserving data confidentiality, availability, and integrity across critical infrastructures. Given their extensive use in financial institutions, healthcare networks, and government operations, any breach in fiber communication can lead to catastrophic service disruptions and national security risks (Singh, et al., 2025). With transmission capacities reaching terabits per second, optical systems are susceptible to sophisticated attacks such as eavesdropping, physical tapping, jamming, and signal injection, which exploit vulnerabilities in optical amplifiers and wavelength-division multiplexing (WDM) components. Advanced AI-based security mechanisms now enable the real-time classification of intrusions by analyzing optical power variations, phase shifts, and anomalous signal noise distributions (Kumar, & Altalbe, 2024). These approaches ensure proactive threat mitigation while maintaining low-latency communication for cloud data centers and high-frequency trading platforms where even millisecond delays can cause significant losses.

The integration of intelligent cybersecurity frameworks in optical networks has evolved from static rule-based systems to dynamic, self-adaptive architectures capable of contextual learning and decision-making (James, et al, 2023). Deep reinforcement learning models, for example, enable proactive response strategies that adjust to evolving attack patterns by continuously refining their defensive policies through feedback loops. Moreover, AI-enhanced encryption and key distribution mechanisms, such as quantum-resistant cryptography and adaptive secure modulation schemes, further strengthen resilience against both classical and quantum-level threats (Oyekan, et al, 2023). The growing convergence of these intelligent systems highlights the vital role of cybersecurity in safeguarding the reliability, scalability, and operational continuity of modern optical fiber communication infrastructures.

1.3. Research Scope and Objectives

This review focuses on evaluating the integration of machine learning (ML) models in enhancing real-time anomaly detection for mitigating cyberattacks in optical fiber communication systems. The scope encompasses supervised, unsupervised, and deep learning techniques applied to detect, classify, and respond to network anomalies that threaten optical data integrity. It investigates how data-driven models, including convolutional neural networks (CNNs), autoencoders, and reinforcement learning algorithms, improve detection precision, adaptability, and scalability within dense optical transport networks. Furthermore, the review covers hybrid and federated learning frameworks designed to enable decentralized intrusion monitoring and real-time defense orchestration across geographically distributed fiber infrastructure.

The primary objective is to synthesize current methodologies, benchmark their performance in intrusion detection and response latency, and identify the technological gaps limiting full automation in optical network security. This study aims to (1) examine the evolution of ML-driven cybersecurity tools tailored for optical systems, (2) assess their efficacy in detecting both known and zero-day attacks, and (3) propose a future roadmap integrating explainable AI and predictive analytics for autonomous network defense. By consolidating existing advancements and challenges, the review aspires to guide the development of next-generation secure, adaptive, and self-healing optical communication environments.

1.4. Structure of the Paper

The structure of this paper is organized to provide a logical and systematic review of the role of machine learning-enabled anomaly detection models in enhancing cybersecurity within optical fiber communication systems. Section 1 introduces the study, outlining its background, motivation, and objectives. Section 2 presents an overview of optical fiber communication systems and the evolving cybersecurity landscape, identifying key vulnerabilities and risk factors. Section 3 discusses various machine learning models, including supervised, unsupervised, and deep learning

approaches, highlighting their application in anomaly detection. Section 4 focuses on model implementation and performance evaluation, detailing datasets, metrics, and benchmarking frameworks. Section 5 explores emerging trends, including the use of edge computing, explainable AI, and federated learning for scalable and interpretable security solutions. Finally, Section 6 concludes the review by summarizing key insights and proposing future research directions for developing autonomous, intelligent, and resilient optical communication networks capable of mitigating cyber threats in real time.

2. Optical fiber communication systems and cybersecurity landscape

2.1. Architecture and Components of Optical Fiber Networks

Optical fiber networks form the core of global high-speed communication systems, providing scalable and low-latency data transmission capabilities that underpin the modern digital economy. These networks typically consist of three main architectural layers: the core, metro, and access networks, each designed to optimize data routing and transmission efficiency as shown in Figure 1 (Zhang, et al., 2021). Core networks employ Dense Wavelength Division Multiplexing (DWDM) and Optical Transport Network (OTN) protocols to aggregate high-capacity traffic, while metro networks bridge regional nodes through dynamic bandwidth allocation. The access layer, incorporating Passive Optical Networks (PONs) and Fiber-to-the-Home (FTTH) systems, ensures end-user connectivity with minimal signal loss. The fundamental components—transmitters, receivers, amplifiers, multiplexers, and optical switches—work in concert to achieve terabit-per-second throughput. Modern architectures increasingly integrate software-defined optical networking (SDON), allowing for adaptive control and resource optimization through centralized network intelligence (Sejan, et al, 2022).

The evolution of intelligent optical systems has been accelerated by artificial intelligence and machine learning applications, which facilitate fault prediction, energy-efficient routing, and anomaly detection. AI-driven modulation optimization and power balancing enhance signal-to-noise ratios and minimize nonlinear distortions that typically degrade performance (Amebleh & Omachi, 2023). Moreover, the adoption of hybrid optical-electrical control planes enables real-time reconfiguration in response to network congestion or cyber threats. These adaptive frameworks not only improve resilience but also enhance operational efficiency by enabling self-optimization and self-healing capabilities. As optical networks expand to support data-intensive services like cloud computing and 5G backhaul, intelligent architectural designs that combine flexibility, scalability, and security have become indispensable for ensuring the reliability of next-generation communication infrastructures (Fagbohungbe, et al., 2025).

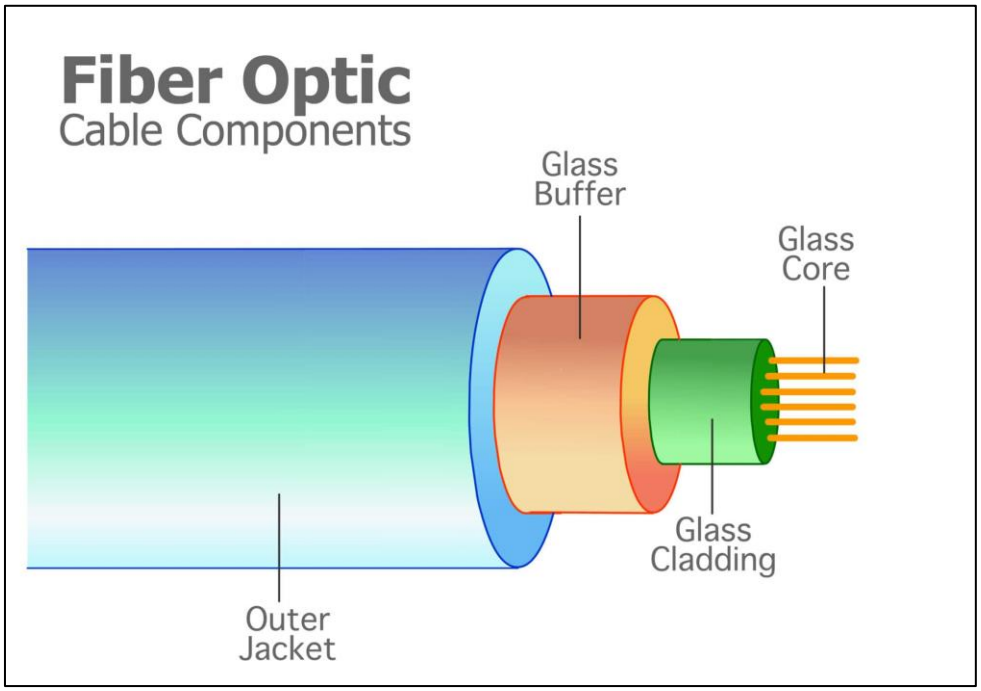

Figure 1 A picture Showing Structural Composition of a Fiber Optic Cable in Optical Network Architecture (Blog, 2024).

Figure 1 shows the main components of a fiber optic cable: the glass core, glass cladding, glass buffer, and outer jacket. The glass core carries light signals, while the cladding ensures total internal reflection for efficient transmission. The buffer layer protects the fiber from stress and microbending, and the outer jacket shields it from moisture and damage. These components form the foundation of optical network architecture, ensuring high-speed, low-loss, and reliable data transfer across core, metro, and access layers. Their precision enables advanced technologies like DWDM and SDON to support intelligent, scalable, and resilient communication systems.

2.2. Common Cyber Threats and Vulnerabilities in Optical Communication

Optical communication systems, though inherently secure due to light-based transmission, face an increasing array of cyber threats as they become more software-defined and interconnected. Common attack vectors include eavesdropping, jamming, denial-of-service (DoS), and physical layer tapping, which exploit vulnerabilities in optical amplifiers, transceivers, and control-plane protocols (Pedro, et al, 2022). Eavesdropping attacks typically occur when adversaries intercept light signals through microbending or evanescent coupling, leading to unauthorized data extraction without significant signal degradation. Similarly, jamming attacks disrupt communication by injecting high-intensity optical signals that overwhelm legitimate data channels, degrading signal-to-noise ratios and causing service outages. The transition toward Software-Defined Optical Networks (SDONs) has further expanded the attack surface, exposing control layers to malware and configuration manipulation, particularly in multi-domain infrastructures.

Machine learning-based intrusion detection frameworks are increasingly employed to counteract these vulnerabilities, providing adaptive anomaly recognition and mitigation capabilities. Recent studies have demonstrated how hybrid deep neural architectures can classify real-time signal distortions linked to cyber intrusions with higher precision than traditional threshold-based methods (Oyekan, et al, 2024). Additionally, optical-layer threat intelligence systems leverage predictive analytics to forecast jamming attempts and unauthorized spectrum access, thereby enhancing network resilience (Idika & Salami, 2024). However, the complexity of optical-layer attacks, coupled with the challenge of differentiating between environmental noise and intentional disruptions, necessitates continuous innovation in adaptive defense algorithms as presented in Table 1. The integration of intelligent monitoring tools within control and data planes remains critical to mitigating these evolving threats in high-capacity optical communication environments.

Table 1 Summary of Common Cyber Threats and Vulnerabilities in Optical Communication

Type of Threat	**Attack Mechanism**	**Impact on Optical Network**	**Mitigation / Defense Strategy**
Eavesdropping	Interception of light signals via microbending or evanescent coupling to extract data without noticeable signal loss.	Breach of data confidentiality; unauthorized access to sensitive transmitted information.	Use of advanced encryption, optical-layer monitoring, and secure channel modulation.
Jamming Attack	Injection of high-intensity optical signals to overwhelm legitimate channels.	Signal degradation, reduced signal-to-noise ratio (SNR), and potential service outage.	Machine-learning-based detection of abnormal optical power patterns and adaptive wavelength rerouting.
Denial-of-Service (DoS)	Saturation of optical control or data planes through excessive requests or malicious traffic bursts.	Network congestion, latency spikes, and temporary loss of service availability.	AI-driven traffic filtering and predictive anomaly detection models for early mitigation.
Physical Layer Tapping & Malware Injection in SDON	Unauthorized physical access or exploitation of software-defined controllers to alter configurations.	Data manipulation, configuration corruption, and expanded attack surface in multi-domain systems.	Integration of intelligent monitoring tools, control-plane authentication, and predictive analytics frameworks.

2.3. Security Requirements and Risk Assessment Frameworks

Ensuring robust security in optical fiber communication systems requires a multidimensional approach encompassing confidentiality, integrity, availability, and authenticity (Maqousi, & Basu, 2025). Unlike traditional IP networks, optical

systems operate at physical and photonic layers where attacks can compromise data transmission without triggering higher-level alarms. Therefore, risk assessment frameworks must integrate both physical-layer monitoring and software-defined control-layer analytics. The zero-trust model has emerged as a viable approach in modern optical infrastructures, requiring continuous verification and segmentation to prevent lateral movement of threats (Dong, et al., 2021). This model emphasizes continuous authentication of devices, optical amplifiers, and controllers through anomaly-based verification mechanisms that minimize the likelihood of insider and advanced persistent threats. Systematic risk analysis methods, such as failure mode and effect analysis (FMEA) combined with probabilistic risk assessment (PRA), are also employed to evaluate vulnerabilities and their potential network-wide impacts.

Recent frameworks have incorporated artificial intelligence to enhance the predictive accuracy of risk modeling and automate incident response. For example, Bayesian inference models integrated with adversarial learning have been used to predict optical signal corruption and routing-based intrusions before service degradation occurs (Ijiga, et al, 2024). Similarly, cyber risk quantification methods developed for adaptive wavelength-routed networks now leverage reinforcement learning to dynamically estimate attack probabilities and allocate mitigation resources in real time. These AI-driven methodologies ensure a proactive security posture, reducing detection latency and false positives while maintaining operational efficiency. Collectively, such hybrid approaches advance optical network protection by aligning real-time threat intelligence with compliance-driven cybersecurity governance, forming the foundation of resilient and trustworthy optical communication ecosystems (James, 2022).

3. Machine learning models for anomaly detection

3.1. Supervised learning techniques (svm, random forest, decision trees)

Supervised learning techniques form the cornerstone of machine learning-driven anomaly detection in optical communication systems. Algorithms such as Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF) have demonstrated exceptional efficiency in detecting and classifying cyber threats based on labeled datasets derived from optical signal patterns and network telemetry (Dixit, et al, 2021). SVMs are particularly effective for high-dimensional feature spaces, enabling precise boundary separation between normal and anomalous optical behaviors through kernel optimization. In contrast, Decision Trees provide interpretability and transparency, allowing security analysts to trace decision paths for specific anomalies such as signal jamming or packet injection. Ensemble-based methods like Random Forests improve robustness by combining multiple tree outputs, reducing overfitting while maintaining high detection accuracy across fluctuating optical noise environments as shown in Figure 2 (Brian, & Alexander, 2023). These algorithms are integral to systems where minimal latency and maximum classification precision are paramount for real-time cyberattack mitigation.

Recent research highlights that integrating adaptive supervised learning frameworks enhances the scalability and responsiveness of optical anomaly detection systems. For instance, reinforcement-assisted Decision Tree hybrids have been used to dynamically adjust classification thresholds in response to evolving attack patterns (Amebleh & Omachi, 2022). Similarly, multi-layer Random Forest models embedded with temporal feature selection modules have improved detection accuracy in Wavelength Division Multiplexing (WDM) networks where signal distortion and polarization mode dispersion introduce non-linear data variability. These advanced models are further optimized using real-time feedback mechanisms that continuously update training datasets, enabling adaptive learning without compromising inference speed. Consequently, supervised learning techniques continue to be foundational in developing intelligent, high-performance security frameworks for next-generation optical communication infrastructures (Ijiga, et al, 2025).

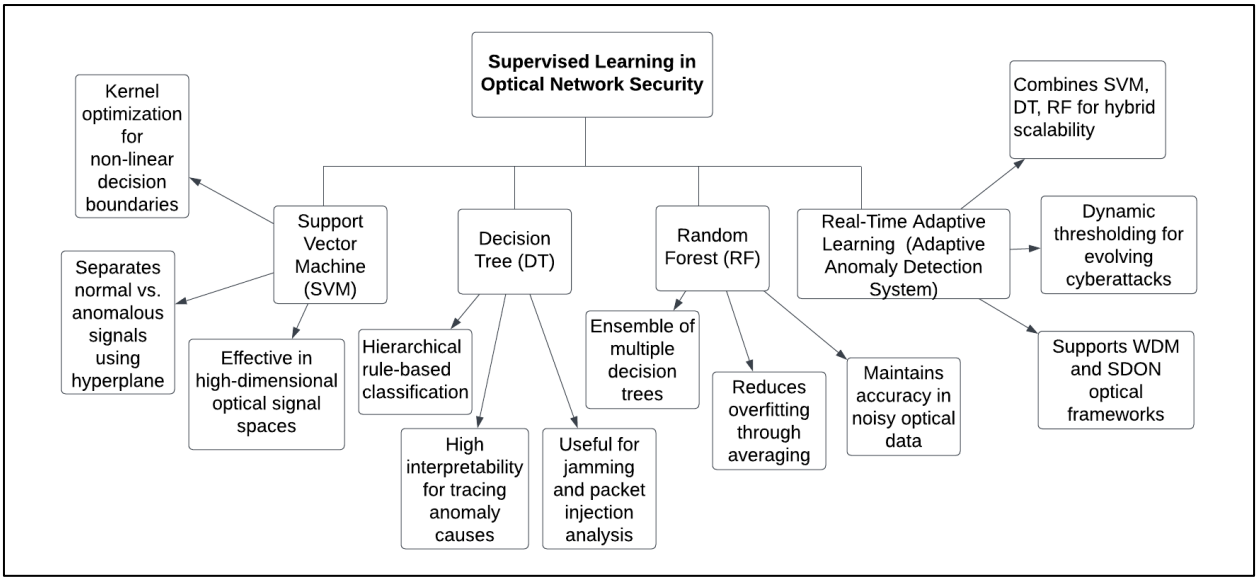

Figure 2 A Block Diagram Showing Supervised Learning Framework for Optical Network Anomaly Detection.

Figure 2 illustrates how supervised learning algorithms—Support Vector Machines (SVM), Decision Trees (DT), and Random Forests (RF)—contribute to intelligent anomaly detection in optical communication systems. The central node represents supervised learning as the foundation for identifying cyber threats using labeled datasets derived from optical signal telemetry. The SVM branch emphasizes optimal boundary separation between normal and anomalous behaviors in high-dimensional data spaces, while the Decision Tree branch highlights interpretable rule-based classification for tracing specific attacks such as jamming or packet injection. The Random Forest branch demonstrates how ensemble learning enhances robustness and accuracy by aggregating multiple tree decisions. These algorithms collectively feed into an adaptive anomaly detection system that dynamically updates models, supports real-time analysis, and mitigates evolving threats within Wavelength Division Multiplexing (WDM) and Software-Defined Optical Network (SDON) infrastructures, ensuring high reliability and minimal latency in cybersecurity operations.

3.2. Unsupervised and Semi-Supervised Learning Models (K-Means, Autoencoders, Isolation Forest)

Unsupervised and semi-supervised learning models have become indispensable in identifying anomalies within optical communication systems, particularly when labeled datasets are scarce or incomplete. Techniques such as K-Means clustering, Autoencoders, and Isolation Forests enable systems to discover latent structures and detect irregular behaviors without explicit supervision (Prakash, & Kasthuri, 2024). K-Means partitions multidimensional optical telemetry data—such as signal strength variations, phase noise, and bit error rates—into clusters, allowing deviations from normal operational patterns to be detected as outliers. This clustering capability is especially beneficial in multi-channel Wavelength Division Multiplexing (WDM) networks, where distinguishing between benign fluctuations and malicious distortions is complex. Autoencoders, on the other hand, learn compact latent representations of network states, reconstructing inputs and flagging deviations with high reconstruction error as anomalies. Their deep architectures enable nuanced feature extraction from raw optical data streams, improving accuracy in detecting low-intensity intrusions that evade traditional monitoring systems (Oyekan, et al, 2025).

Semi-supervised approaches extend these models by leveraging limited labeled samples to refine anomaly classification boundaries. Isolation Forests, which rely on recursive partitioning of feature spaces, are particularly effective for detecting rare cyber events, such as covert channel exploitation or power-level manipulation in optical amplifiers (Amebleh & Okoh, 2023). The hybridization of K-Means and Isolation Forests facilitates both clustering-based pre-screening and probabilistic isolation of anomalous points, optimizing detection precision while reducing false positives. In optical transport networks, where real-time security monitoring is critical, these hybrid unsupervised models outperform signature-based systems by adapting to evolving attack vectors and data drift as presented in Table 2. Furthermore, combining autoencoders with dynamic threshold tuning enables continuous learning from operational feedback, ensuring adaptive resilience against novel intrusion patterns. Collectively, these unsupervised and semi-supervised models establish the foundation for autonomous anomaly detection frameworks that safeguard high-capacity optical communication infrastructures with minimal human intervention (Gayawan, & Fagbohungbe, 2023).

Table 2 Summary of Unsupervised and Semi-Supervised Learning Models (K-Means, Autoencoders, Isolation Forest).

Model / Technique	Core Functionality	Application in Optical Communication Systems	Advantages / Key Outcomes
K-Means Clustering	Groups data into clusters based on similarity, identifying outliers that deviate from cluster centroids.	Used to detect abnormal variations in optical telemetry data such as power levels, phase noise, and bit error rates in WDM networks.	Simplifies anomaly visualization, detects subtle deviations, and efficiently handles large-scale optical datasets.
Autoencoders	Employ neural networks to learn compressed latent representations and reconstruct input data, flagging high reconstruction errors as anomalies.	Capture hidden optical signal behaviors and detect low-intensity intrusions that evade threshold-based methods.	Enhance detection sensitivity, extract complex patterns, and support continuous learning from raw data streams.
Isolation Forest	Utilizes recursive partitioning to isolate anomalous data points based on path length within decision trees.	Identifies rare cyber incidents such as covert wavelength manipulation and power-level tampering in amplifiers.	Effective for sparse anomalies, reduces false positives, and adapts to data drift in real-time environments.
Hybrid Models (K-Means + Isolation Forest + Autoencoders)	Combines clustering, reconstruction, and probabilistic isolation for multi-level detection.	Provides pre-screening, refined classification, and adaptive learning in optical transport networks.	Improves accuracy, resilience, and real-time anomaly detection with minimal human oversight.

3.3. Deep Learning and Reinforcement Learning Approaches for Real-Time Detection

Deep learning and reinforcement learning techniques have transformed real-time anomaly detection in optical fiber communication systems by introducing adaptive intelligence and contextual awareness into cybersecurity frameworks. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, for instance, have proven highly effective in modeling the temporal and spectral dependencies inherent in optical signal transmission (Behera, et al, 2023). CNNs excel in feature extraction from raw optical intensity and wavelength datasets, while LSTMs capture time-based correlations that indicate progressive intrusion behaviors such as packet injection or power modulation anomalies. Hybrid CNN-LSTM fusion models offer superior performance by combining spatial feature encoding with temporal prediction, enabling early identification of complex multi-stage attacks within milliseconds (James, et al, 2025). Deep learning approaches also enhance false alarm discrimination by learning nonlinear mappings between signal distortions and network state transitions, improving detection precision in highly dynamic communication environments.

Reinforcement learning extends this capability by introducing autonomous decision-making mechanisms for real-time mitigation. Deep Q-Networks (DQNs) and Actor–Critic models, for example, dynamically adapt intrusion response strategies based on reward optimization and environmental feedback (Hwang, et al., 2020). These algorithms learn optimal countermeasures—such as channel reassignment, wavelength rerouting, or power attenuation—to restore service integrity during cyber incidents. Furthermore, reinforcement learning-based intrusion response systems support the concept of *self-healing networks*, where intelligent agents continuously reconfigure optical paths in response to detected threats (Idika & James, 2024). The integration of deep and reinforcement learning not only reduces latency in anomaly recognition but also enables proactive defense mechanisms capable of adapting to unknown or evolving attack vectors. As optical networks scale toward autonomous operation, these AI-driven architectures provide a resilient and intelligent framework for safeguarding global communication infrastructures against real-time cyber threats.

4. Model implementation and performance evaluation

4.1. Dataset Characteristics and Preprocessing for Optical Network Security

The reliability of machine learning-enabled optical network security models depends heavily on the quality, diversity, and representativeness of datasets used during training and evaluation. Optical network datasets often consist of traffic flow records, signal transmission logs, and physical-layer parameters such as optical power, bit error rate (BER), chromatic dispersion, and phase noise. However, due to the complexity of optical environments, datasets are typically high-dimensional, imbalanced, and non-stationary, making preprocessing a critical step before model training (Moustafa, 2021). Data normalization techniques such as Z-score scaling and min–max normalization are commonly applied to reduce variance caused by disparate signal magnitudes, ensuring that learning algorithms effectively capture relevant anomalies without overfitting to noise. Furthermore, synthetic data generation using Generative Adversarial Networks (GANs) and signal augmentation techniques helps compensate for insufficient attack samples, particularly for rare intrusion types like coherent channel hijacking or wavelength spoofing (Khan, et al., 2022).

Recent advancements emphasize preprocessing frameworks specifically designed for the physical-layer characteristics of optical systems. For instance, signal filtering and denoising algorithms—such as Savitzky–Golay smoothing and Fast Fourier Transform (FFT)-based noise reduction—are integrated into data pipelines to enhance the clarity of optical intensity and polarization signatures before feature extraction (Ijiga, et al, 2024). Feature selection and dimensionality reduction methods, including Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE), have also been instrumental in improving computational efficiency while retaining discriminative signal attributes (Adedayo, et al, 2025). Moreover, handling data imbalance through techniques like Synthetic Minority Oversampling Technique (SMOTE) ensures equitable representation of normal and anomalous classes during supervised learning. These preprocessing strategies are vital for building resilient models that generalize across diverse network conditions and can maintain high detection accuracy under fluctuating optical transmission scenarios. By optimizing dataset preparation, machine learning frameworks can more accurately model the dynamic and nonlinear characteristics of real-world optical communication environments (Idika et al, 2023).

Table 3 Summary of Dataset Characteristics and Preprocessing for Optical Network Security

Aspect	Description	Techniques / Methods Used	Outcome / Significance
Dataset Composition	Optical network datasets include traffic flow logs, optical signal power, BER, phase noise, and chromatic dispersion parameters.	Data collected from core, metro, and access layers across multiple network nodes.	Provides a diverse, high-dimensional basis for model training and anomaly detection.
Challenges in Data Quality	Datasets are often high-dimensional, imbalanced, and non-stationary due to variable transmission conditions and rare intrusion events.	Data balancing using SMOTE; synthetic data generation via GANs for rare attack classes.	Reduces bias, enhances detection of low-frequency cyber threats, and supports robust model learning.
Preprocessing Techniques	Applied to clean, normalize, and denoise raw optical data to improve signal integrity and learning stability.	Z-score and min–max normalization; Savitzky–Golay filtering; FFT-based noise reduction.	Ensures consistent data scaling, minimizes optical noise interference, and enhances feature clarity.
Feature Selection and Dimensionality Reduction	Focuses on selecting relevant optical signal features and reducing redundancy in datasets.	Principal Component Analysis (PCA), Recursive Feature Elimination (RFE).	Improves computational efficiency, model interpretability, and detection accuracy in real-time anomaly detection.

4.2. Evaluation Metrics (Accuracy, Precision, Recall, F1-Score, ROC)

Evaluating the performance of machine learning models for anomaly detection in optical network security requires a rigorous, multidimensional framework. The most widely used evaluation metrics—Accuracy, Precision, Recall, F1-

Score, and Receiver Operating Characteristic (ROC)—quantify different aspects of predictive reliability. Accuracy measures the overall correctness of classification but can be misleading in highly imbalanced datasets typical of optical intrusion detection scenarios, where attack instances are rare compared to normal traffic as shown in Figure 3 (Imtiaz, et al, 2025). Precision, defined as the ratio of true positives to the sum of true and false positives, is particularly critical for assessing how well models minimize false alarms, which can otherwise disrupt legitimate optical channel reconfigurations. Recall, the proportion of correctly identified attacks among all actual intrusions, reflects the model's sensitivity and is essential for ensuring early detection of cyber threats such as jamming or wavelength spoofing. The F1-Score provides a harmonic balance between Precision and Recall, making it especially useful when prioritizing trade-offs between false negatives and false positives in real-time detection systems.

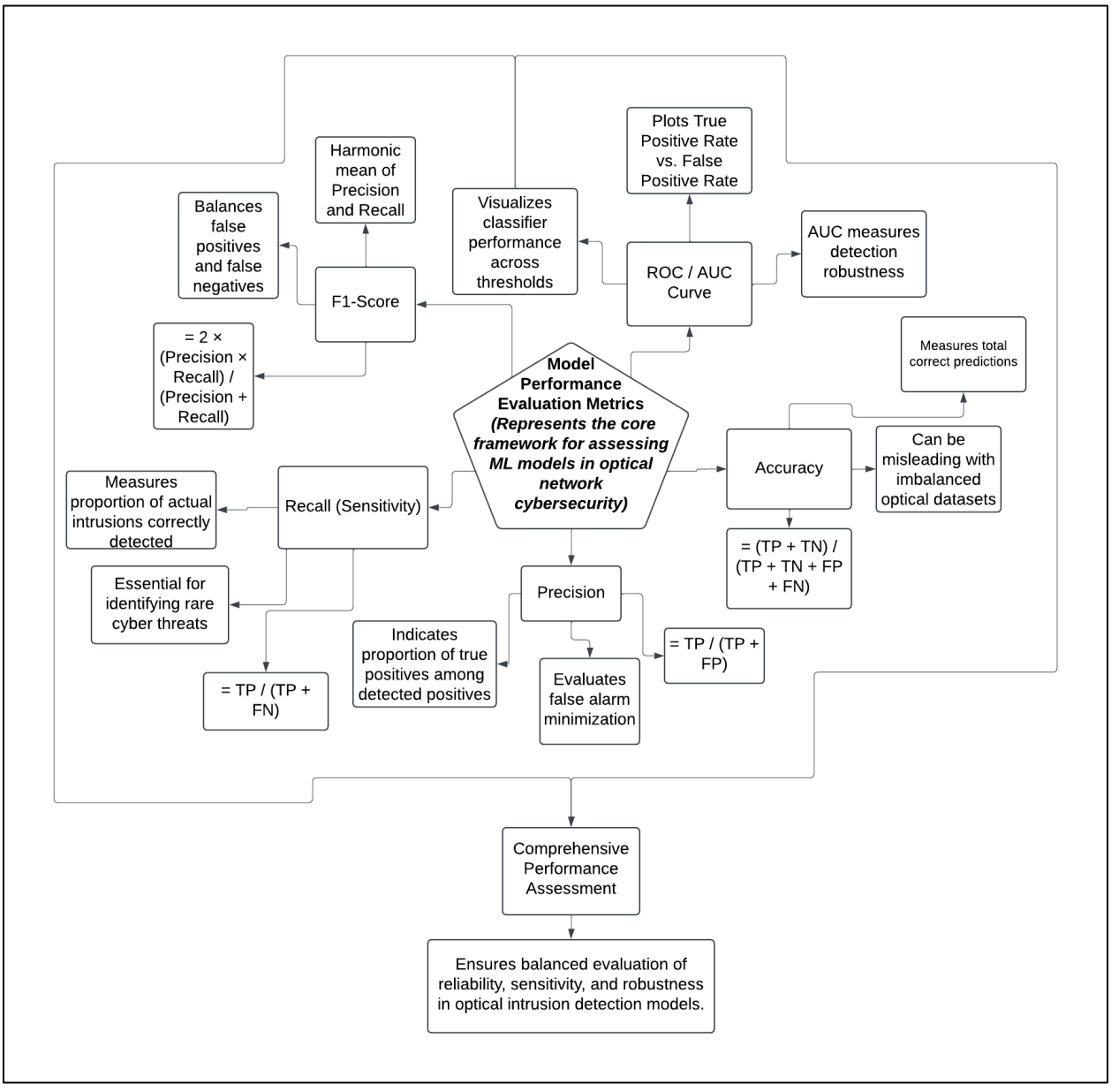

Figure 3 A Block Diagram Showing Comprehensive Evaluation Metrics Framework for Machine Learning-Based Optical Network Security.

Recent research has emphasized the importance of composite and dynamic evaluation frameworks for optical networks. For example, the ROC curve, which plots the True Positive Rate (TPR) against the False Positive Rate (FPR), offers a visual understanding of classifier discrimination performance across varying thresholds (Amebleh, et al, 2021). Advanced models now incorporate Area Under the ROC Curve (AUC) as a standard measure of overall detection robustness. Additionally, weighted F1-scores and macro-averaged metrics are applied to evaluate models across multiple classes of attacks, improving interpretability in multi-modal anomaly detection systems. To enhance reliability,

precision-oriented metrics such as Cohen's Kappa and Matthews Correlation Coefficient (MCC) are increasingly integrated into evaluation protocols for optical systems with complex noise environments (Okereke, et al, 2025). These multi-criteria evaluation frameworks ensure that ML-driven anomaly detection models not only achieve statistical accuracy but also maintain operational reliability under dynamic and high-throughput optical network conditions.

Figure 3 illustrates the core evaluation metrics used to measure the effectiveness of machine learning models in detecting anomalies within optical network security systems. At the center is Model Performance Evaluation, branching into five key metrics Accuracy, Precision, Recall, F1-Score, and ROC/AUC Curve each capturing a different aspect of model reliability. Accuracy, calculated as (TP + TN) / (TP + TN + FP + FN), measures the proportion of correct predictions among all classifications, where TP (True Positives) and TN (True Negatives) represent correctly identified instances, while FP (False Positives) and FN (False Negatives) indicate errors. Precision evaluates how well the model minimizes false alarms, while Recall measures the system's ability to detect actual cyberattacks. The F1-Score harmonizes Precision and Recall to balance false positives and negatives, ensuring fairness in performance assessment. Finally, the ROC/AUC Curve visualizes the relationship between true and false positive rates across thresholds, highlighting the model's discrimination power. Collectively, these metrics provide a comprehensive framework for evaluating detection accuracy, sensitivity, and robustness in optical communication cybersecurity applications.

4.3. Benchmarking and Comparative Analysis of ML Algorithms

Benchmarking machine learning (ML) algorithms for optical network security involves systematically comparing models based on accuracy, computational efficiency, adaptability, and robustness against diverse attack scenarios. Traditional models such as Support Vector Machines (SVM), Random Forests (RF), and Decision Trees (DT) remain foundational benchmarks due to their interpretability and low computational cost, yet they often underperform in detecting complex temporal anomalies inherent in high-speed optical transmission (Arshad, et al, 2022). Deep learning architectures—such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks—outperform classical algorithms by capturing spatial and temporal dependencies in optical signal streams, enabling the detection of subtle cyber intrusions like wavelength drift manipulation or power fluctuation attacks. Furthermore, ensemble methods combining multiple algorithms, such as Random Forest with Gradient Boosting, have achieved improved detection precision, particularly in multi-modal optical datasets with high noise variance (Idika, et al, 2024). The benchmarking process frequently relies on cross-validation techniques and standardized datasets to ensure fair model comparison, emphasizing scalability and generalization across real-world optical environments.

Recent studies have highlighted the growing importance of hybrid deep learning models and adaptive learning frameworks in achieving superior performance across varying optical network conditions. CNN-LSTM hybrids, for instance, have demonstrated a significant reduction in false alarm rates while maintaining high recall values for real-time anomaly detection (Ijiga, et al, 2024). Similarly, comparative evaluations indicate that unsupervised models, such as Autoencoders and Isolation Forests, offer complementary benefits by identifying zero-day attacks that supervised models fail to capture. Benchmarking also extends beyond static performance metrics to include energy consumption, latency tolerance, and adaptability under fluctuating optical load conditions (Amebleh & Onoja, 2025). This comprehensive comparative analysis reveals that no single algorithm dominates all performance dimensions; rather, integrating heterogeneous ML models through hybrid and ensemble learning provides the most reliable and scalable defense architecture for real-time cybersecurity in optical communication systems.

5. Emerging trends and challenges in ml-driven anomaly detection

5.1. Integration of Edge Computing and Federated Learning for Distributed Security

The integration of edge computing and federated learning (FL) has revolutionized the design of secure and distributed architectures in optical fiber communication systems. Edge computing enables data processing close to the network source, reducing latency and minimizing the need to transmit sensitive data to centralized servers—a critical advantage for real-time anomaly detection in optical infrastructures (Li, et al, 2020). Federated learning complements this by allowing multiple edge nodes to collaboratively train shared machine learning models without directly exchanging raw data, thus preserving data privacy and reducing vulnerability to interception. In optical networks, this decentralized intelligence enables intrusion detection models to learn from geographically distributed data centers while maintaining compliance with privacy and bandwidth constraints (Ijiga, et al, 2024). For example, in dense wavelength division multiplexing (DWDM) systems, local edge devices can independently detect anomalies in channel intensity or polarization variations and synchronize updates to a global model through federated aggregation protocols.

Recent studies emphasize that combining edge intelligence with federated learning significantly enhances both scalability and resilience in cybersecurity frameworks for optical transport networks. Hybrid edge–federated architectures can dynamically adapt to traffic fluctuations, identifying distributed denial-of-service (DDoS) and wavelength jamming attacks with minimal communication overhead (Amebleh, et al, 2025). Moreover, edge-assisted learning models employ gradient compression and differential privacy mechanisms to safeguard sensitive optical telemetry data during model synchronization. This ensures that global model convergence occurs efficiently even under constrained bandwidth environments. Reinforcement-based scheduling techniques are also used to optimize computational load distribution among edge nodes, enhancing fault tolerance and reducing detection latency (James, et al, 2024). By integrating edge computing with federated learning, optical communication systems can achieve real-time, privacy-preserving, and distributed anomaly detection—paving the way for autonomous, intelligent, and self-healing network defense architectures.

5.2. Explainable Artificial Intelligence (XAI) and Model Interpretability

The increasing reliance on deep learning and complex ensemble models in optical communication security has elevated the demand for Explainable Artificial Intelligence (XAI) to ensure transparency, accountability, and trust in automated decision systems. Traditional machine learning algorithms, though highly accurate, often operate as "black boxes," offering limited insight into how specific predictions or anomaly classifications are derived. XAI addresses this limitation by providing interpretable representations of model reasoning processes, enabling network administrators to understand the underlying causes of detected threats as shown in Figure 4(Mankodiya, et al, 2021). In optical fiber networks, where decisions directly affect signal integrity and data routing, model interpretability becomes critical for diagnosing misclassifications and false positives. Techniques such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) are increasingly applied to visualize feature importance across optical telemetry parameters, such as wavelength deviation, phase modulation, and power variation (Mehra, 2020). These tools allow engineers to validate whether model outputs correspond to real optical behaviors or spurious signal noise, strengthening operational confidence in automated security frameworks.

Recent advancements in XAI research within optical communication emphasize the development of interpretable deep learning architectures that integrate visual and symbolic reasoning components. Hybrid models combining convolutional layers with attention mechanisms enable contextual interpretation of temporal signal patterns and anomaly features (Abiola, et al, 2025). Additionally, interpretable graph neural networks (GNNs) have been deployed to model the topological dependencies between optical nodes, allowing clear visualization of attack propagation pathways. Reinforcement-driven XAI frameworks further enhance decision transparency by correlating network responses with specific environmental conditions or adversarial inputs. By bridging the gap between predictive accuracy and human interpretability, XAI-driven cybersecurity solutions ensure that AI-based anomaly detection systems in optical networks remain not only precise but also auditable and trustworthy (Idika, et al, 2024). This paradigm shift toward transparent AI governance fosters sustainable human–machine collaboration for resilient optical communication infrastructures.

Figure 4 A Picture Showing Intersection of Ethical and Explainable AI Principles in Optical Network Security (Hamida, et al., 2024).

Figure 4 illustrates the intersection between ethical and explainable principles of Artificial Intelligence, emphasizing the foundational attributes necessary for trustworthy and transparent AI systems. In the context of optical communication network security, Explainable AI (XAI) integrates these principles to ensure that automated anomaly detection models are both technically interpretable and socially responsible. The ethical dimension encompasses inclusiveness, fairness, and accountability, ensuring that AI-driven security systems do not introduce bias or compromise user trust. Meanwhile, the explainable dimension emphasizes transparency, privacy, and security, vital for

understanding how deep learning algorithms classify threats or respond to anomalies in optical signals. At the center of this intersection lies reliability and safety, which are essential in preventing misclassifications that could disrupt optical data transmission or compromise network integrity. Thus, the diagram effectively captures the dual objective of XAI in optical cybersecurity: achieving model interpretability while maintaining ethical governance.

5.3. Limitations, Scalability Issues, and Real-Time Adaptation Challenges

Despite the rapid progress in machine learning (ML)-enabled optical network security, several limitations and scalability challenges persist in achieving fully autonomous and real-time cyber defense. One primary constraint is the high computational complexity of deep neural models, which require extensive processing power and memory—difficult to sustain in distributed optical environments with limited edge resources (Furdek, et al, 2020). Additionally, latency-sensitive applications such as 5G backhaul and cloud interconnects demand sub-millisecond anomaly response times, a requirement often unmet by traditional centralized ML architectures. Scalability also becomes an issue as optical networks grow in node density and wavelength diversity, leading to exponential increases in data dimensionality and communication overhead (Bhide, et al., 2025). Moreover, the heterogeneity of network topologies and equipment vendors complicates the standardization of training data formats and model deployment protocols. In dynamic transmission conditions, optical impairments—such as polarization mode dispersion and nonlinear phase noise—further distort telemetry signals, making real-time inference models prone to misclassification and reduced detection accuracy.

Recent studies highlight that most adaptive ML frameworks lack the elasticity to handle rapidly evolving cyber threats and environmental drift without extensive retraining. Continuous retraining is resource-intensive, risking model degradation and overfitting when datasets are unbalanced or lack temporal variability. Furthermore, federated and distributed learning architectures introduce synchronization delays during parameter aggregation, hindering real-time adaptability across multi-domain optical infrastructures (Igwe, et al, 2025). Data privacy regulations further constrain the sharing of optical telemetry, limiting the development of globally synchronized threat intelligence models. To mitigate these challenges, emerging research advocates lightweight neural architectures, model compression techniques, and edge-based retraining strategies to balance computational cost with detection responsiveness as presented in Table 4. However, achieving scalability without compromising performance remains a complex problem, Highlighting the need for continuous innovation in distributed learning and adaptive control mechanisms for next-generation optical cybersecurity systems (Fagbohungbe, et al., 2020).

Table 4 Summary of Limitations, Scalability Issues, and Real-Time Adaptation Challenges

Challenge Category	Description	Underlying Causes / Technical Constraints	Proposed Solutions / Research Directions
Computational Complexity and Resource Demand	Deep neural networks require significant processing power and memory, which strain distributed and edge-based optical environments.	High model dimensionality, limited GPU/CPU resources at network edges, and continuous data streams from multiple optical nodes.	Use lightweight neural architectures, model pruning, and compression to optimize inference speed and reduce hardware dependency.
Latency and Real-Time Adaptation Constraints	Centralized ML models fail to deliver sub-millisecond responses required in latency-sensitive optical systems such as 5G and cloud backhaul.	Centralized data processing, high communication overhead, and synchronization delays in federated learning setups.	Deploy edge-based and distributed intelligence to support local, low-latency decision-making with adaptive retraining strategies.
Scalability and Data Heterogeneity	Increasing wavelength diversity and node density in optical networks lead to exponential data growth and integration issues.	Non-standardized telemetry formats, multi-vendor equipment heterogeneity, and bandwidth saturation in large infrastructures.	Develop standardized data protocols, hierarchical model training, and adaptive learning pipelines for large-scale environments.
Model Maintenance and Privacy Limitations	Continuous retraining of ML models is costly and restricted by data-sharing regulations, reducing	Resource-intensive retraining, unbalanced datasets, and privacy	Implement federated learning with privacy-preserving techniques and incremental model updates

	adaptability to evolving threats.	constraints on telemetry data exchange.	to maintain resilience and compliance.

6. Conclusion and future research directions

6.1. Summary of Key Findings

This study has demonstrated that integrating machine learning into optical fiber communication systems significantly enhances anomaly detection and cyberattack mitigation through adaptive, data-driven intelligence. Supervised learning algorithms, including Support Vector Machines and Random Forests, have proven effective for structured intrusion detection, while unsupervised models such as Autoencoders and Isolation Forests excel at uncovering zero-day attacks in complex, unlabeled datasets. Deep learning frameworks—particularly CNN-LSTM hybrids—enable spatiotemporal modeling of optical signal behaviors, achieving high precision in identifying subtle transmission anomalies like wavelength spoofing and optical jamming. Furthermore, reinforcement learning introduces autonomous decision-making that dynamically adjusts mitigation responses based on real-time environmental feedback. Edge computing and federated learning architectures further optimize performance by decentralizing model training, reducing latency, and preserving data privacy. Explainable AI (XAI) enhances transparency by clarifying model decisions, thereby improving operator trust and system accountability. Collectively, these advancements establish that multi-model hybridization, combined with distributed intelligence, provides the most resilient and scalable defense architecture for modern optical communication systems.

6.2. Research Gaps and Opportunities for Innovation

Despite notable progress, critical research gaps persist in achieving seamless real-time adaptability and standardization of ML-enabled optical security frameworks. Current systems still face latency and synchronization constraints when scaling to multi-domain optical backbones, particularly under high-traffic conditions. There remains a lack of universal datasets that accurately represent cross-layer interactions between optical, physical, and control planes, hindering generalization of anomaly detection models. Additionally, the interpretability of deep neural architectures continues to pose a challenge; while XAI frameworks have improved visibility, they often struggle to contextualize non-linear optical impairments. Opportunities for innovation lie in developing lightweight, adaptive neural networks capable of incremental learning with minimal retraining overhead. Integrating quantum-safe cryptographic mechanisms and neuromorphic processors could enhance both security and energy efficiency. Moreover, cross-layer intelligence—where optical, transport, and application layers collaborate dynamically—can lead to predictive defense systems that preemptively respond to emerging threats. These research directions highlight the potential for designing intelligent, interoperable, and evolution-ready optical network defense ecosystems.

6.3. Toward Autonomous and Self-Healing Optical Network Security Systems

The future of optical network cybersecurity lies in the realization of autonomous, self-healing architectures capable of proactive threat detection and autonomous recovery. Such systems will leverage continuous learning loops driven by reinforcement learning agents, enabling real-time reconfiguration of optical channels in response to detected intrusions or transmission faults. Embedded AI modules will dynamically optimize routing, modulation formats, and power distribution without human intervention, ensuring uninterrupted communication even under coordinated cyberattacks. Self-healing networks will employ digital twin environments to simulate potential network disruptions and test recovery strategies, reducing downtime through predictive maintenance and automated fault correction. By integrating federated edge intelligence, these systems will coordinate anomaly insights across distributed nodes, ensuring synchronized defense without centralized control bottlenecks. Future optical infrastructures will thus evolve into cognitive ecosystems capable of understanding, reasoning, and adapting to adversarial conditions. This paradigm will redefine cybersecurity from a reactive posture to an anticipatory one—where optical communication systems are not only secure but resilient, self-optimizing, and continuously evolving to meet the demands of global digital interconnectivity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abiola, O. B. & Ijiga, M. O. (2025), Implementing Dynamic Confidential Computing for Continuous Cloud Security Posture Monitoring to Develop a Zero Trust-Based Threat Mitigation Model. International Journal of Innovative Science and Research Technology (IJISRT) IJISRT25MAY587, 69-83. DOI: 10.38124/ijisrt/25may587.https://www.ijisrt.com/implementing-dynamic-confidential-computing-for-continuous-cloud-security-posture-monitoring-to-develop-a-zero-trustbased-threat-mitigation-model

[2] Adedayo I. S., Jinadu, S. O., Alaka, E., Abiodun, K. D., Peter-Anyebe, A. C. (2025). Leading the development of AI-Drive AML and Compliance Infrastructure to Modernize U.S Financial Crime Prevention System Across Digital and Traditional Platforms. *International Journal for Multidisciplinary Research (IJFMR),* Volume 7, Issue 4, July-August 2025.

[3] Amebleh, J., & Igba, E. (2024). Causal uplift for rewards aggregators: Doubly-robust heterogeneous treatment-effect modeling with SQL/Python pipelines and real-time inference. International Journal of Scientific Research and Modern Technology, 2(5), 39–55. https://doi.org/10.38124/ijsrmt.v3i5.819

[4] Amebleh, J. & Omachi, A. (2022). Data Observability for High-Throughput Payments Pipelines: SLA Design, Anomaly Budgets, and Sequential Probability Ratio Tests for Early Incident Detection *International Journal of Scientific Research in Science, Engineering and Technology Volume* 9, Issue 4 576-591 DOI: https://doi.org/10.32628/IJSRSET221658

[5] Amebleh, J. & Onoja, D. A. (2025). PRIVACY-PRESERVING CONSUMER-BEHAVIOR ANALYTICS ACROSS MULTISTATE TELEMEDICINE: DIFFERENTIAL PRIVACY, K-ANONYMITY, AND FEDERATED GRADIENT AGGREGATION *Acta Scientifica Malaysia (ASM)* Zibeline publishing DOI: http://doi.org/10.26480/asm.02.2025.43.53

[6] Amebleh, J., & Okoh, O. F. (2023). Explainable Risk Controls for Digital Health Payments: SHAP-Constrained Gradient Boosting with Policy-Based Access, Audit Trails, and Chargeback Mitigation. *International Journal of Scientific Research and Modern Technology*, *2*(4), 13–28. https://doi.org/10.38124/ijsrmt.v2i4.746

[7] Amebleh, J., & Omachi, A. (2023). Integrating Financial Planning and Payments Data Fusion for Essbase SAP BW Cohort Profitability LTV CAC Variance Analysis. *International Journal of Scientific Research and Modern Technology*, *2*(4), 1–12. https://doi.org/10.38124/ijsrmt.v2i4.752

[8] Amebleh, J., Bamigwojo, O. V. & Enyejo, J. O. (2025). Automated UAT for Regulated Payment Systems: Property-Based Testing, Synthetic Data Generation, and IFRS/GAAP Revenue-Recognition Validation Gates *International Journal of Innovative Science and Research Technology* Volume 10, Issue 9, https://doi.org/10.38124/ijisrt/25sep331

[9] Amebleh, J., Igba, E. & Ijiga, O. M. (2021). Graph-Based Fraud Detection in Open-Loop Gift Cards: Heterogeneous GNNs, Streaming Feature Stores, and Near-Zero-Lag Anomaly Alerts *International Journal of Scientific Research in Science, Engineering and Technology* Volume 8, Issue 6 DOI: https://doi.org/10.32628/IJSRSET214418

[10] Arshad, K., Ali, R. F., Muneer, A., Aziz, I. A., Naseer, S., Khan, N. S., & Taib, S. M. (2022). Deep reinforcement learning for anomaly detection: A systematic review. Ieee Access, 10, 124017-124035.

[11] Behera, S., Panayiotou, T., & Ellinas, G. (2023, July). Machine learning for real-time anomaly detection in optical networks. In 2023 23rd International Conference on Transparent Optical Networks (ICTON) (pp. 1-4). IEEE.

[12] Bhide, P., Shetty, D., & Mikkili, S. (2025). Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain. IET Quantum Communication, 6(1), e12114.

[13] Blog, (2024). What is a Fiber Optic Network? A Comprehensive Guide on Components. Retrieved from: https://www.zayo.com/resources/fiber-optic-networks-a-comprehensive-guide.

[14] Brian, J., & Alexander, D. (2023). AI-Powered Intrusion Detection Systems for Next-Gen Cloud Networks.

[15] Dixit, P., Kohli, R., Acevedo-Duque, A., Gonzalez-Diaz, R. R., & Jhaveri, R. H. (2021). Comparing and analyzing applications of intelligent techniques in cyberattack detection. Security and Communication Networks, 2021(1), 5561816.

[16] Dong, Y., Sun, B., & Wang, G. (2021). Research on modeling method of power system network security risk assessment based on object-oriented Bayesian network. Energy Reports, 7, 289-295.

[17] Fagbohungbe, T., Gayawan, E. & Akeboi, O. S. (2020). Spatial prediction of childhood malnutrition across space in Nigeria based on point-referenced data: an SPDE approach Journal of Public Health Policy 41(3) DOI: 10.1057/s41271-020-00246-x

[18] Fagbohungbe, T., Zhang, L. & Cao, X. (2025). Sparse inverse covariance selection with mass-nonlocal priors Statistics & Probability Letters 219(2):110348 DOI: 10.1016/j.spl.2024.110348

[19] Furdek, M., Natalino, C., Lipp, F., Hock, D., Giglio, A. D., & Schiano, M. (2020). Machine learning for optical network security monitoring: A practical perspective. Journal of Lightwave Technology, 38(11), 2860-2871.

[20] Gayawan, E. & Fagbohungbe, T. (2023). Continuous Spatial Mapping of the Use of Modern Family Planning Methods in Nigeria Global Social Welfare 10(2):1-11 DOI: 10.1007/s40609-023-00264-z

[21] Hamida, S. U., Chowdhury, M. J. M., Chakraborty, N. R., Biswas, K., & Sami, S. K. (2024). Exploring the Landscape of Explainable Artificial Intelligence (XAI): A Systematic Review of Techniques and Applications. Big Data and Cognitive Computing, 8(11), 149. https://doi.org/10.3390/bdcc8110149

[22] Hwang, R. H., Peng, M. C., Huang, C. W., Lin, P. C., & Nguyen, V. L. (2020). An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access, 8, 30387-30399.

[23] Idika, C. N. (2023). Quantum resistant cryptographic protocols for securing autonomous vehicle-to-vehicle (V2V) communication networks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(1), 1–10. https://doi.org/10.32628/CSEIT2391547

[24] Idika, C. N., & James, I. S. (2024). Optical-layer cybersecurity: Adaptive threat intelligence for mitigating intrusion and jamming attacks in wavelength-routed networks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 54–69. https://doi.org/10.32628/CSEIT2411623

[25] Idika, C. N. & Ijiga, O. M. (2025). Blockchain-Based Intrusion Detection Techniques for Securing Decentralized Healthcare Information Exchange Networks. *Information Management and Computer Science*, Zibeline International Publishing 8(2): 25-36. DOI: http://doi.org/10.26480/imcs.02.2025.25.36

[26] Idika, C. N., & Salami, E. O. (2024). Federated Learning Approaches for Privacy-Preserving Threat Detection in Smart Home IoT Environments *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 10, Issue (1125 -1131) doi :https://doi.org/10.32628/CSEIT24113369

[27] Idika, C. N., James, U. U., Ijiga, O. M., Okika, N. & Enyejo, L. A, (2024). Secure Routing Algorithms Integrating Zero Trust Edge Computing for Unmanned Aerial Vehicle Networks in Disaster Response Operations *International Journal of Scientific Research and Modern Technology, (IJSRMT)* Volume 3, Issue 6, https://doi.org/10.38124/ijsrmt.v3i6.635

[28] Idika, C. N., James, U.U, Ijiga, O. M., Enyejo, L. A. (2023). Digital Twin-Enabled Vulnerability Assessment with Zero Trust Policy Enforcement in Smart Manufacturing Cyber-Physical System *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 9, Issue 6 DOI: https://doi.org/10.32628/CSEIT23906189

[29] Igwe, E. U., Peter-Anyebe, A. C. & Onoja, A. D. (2025). Integrating Trauma-Informed Pastoral Counseling into Correctional Behavioral Health: A Review of Evidence-Based Practices and Spiritual Care Models. Journal of Healthcare in Developing Countries (JHCDC) 5(2) (2025) 50-60. DOI: http://doi.org/10.26480/jhcdc.02.2025.50.60

[30] Ijiga, A. C., Aboi, E. J., Idoko, P. I., Enyejo, L. A., & Odeyemi, M. O. (2024). Collaborative innovations in Artificial Intelligence (AI): Partnering with leading U.S. tech firms to combat human trafficking. *Global Journal of Engineering and Technology Advances, 2024,18(03), 106-123.* https://gjeta.com/sites/default/files/GJETA-2024-0046.pdf

[31] Ijiga, A. C., Abutu E. P., Idoko, P. I., Ezebuka, C. I., Harry, K. D., Ukatu, I. E., & Agbo, D. O. (2024). Technological innovations in mitigating winter health challenges in New York City, USA. *International Journal of Science and Research Archive*, 2024, 11(01), 535–551. https://ijsra.net/sites/default/files/IJSRA-2024-0078.pdf

[32] Ijiga, A. C., Abutu, E. P., Idoko, P. I., Agbo, D. O., Harry, K. D., Ezebuka, C. I., & Umama, E. E. (2024). Ethical considerations in implementing generative AI for healthcare supply chain optimization: A cross-country analysis across India, the United Kingdom, and the United States of America. *International Journal of Biological and Pharmaceutical Sciences Archive*, 2024, 07(01), 048–063. https://ijbpsa.com/sites/default/files/IJBPSA-2024-0015.pdf

[33] Ijiga, A. C., Enyejo, L. A., Odeyemi, M. O., Olatunde, T. I., Olajide, F. I & Daniel, D. O. (2024). Integrating community-based partnerships for enhanced health outcomes: A collaborative model with healthcare providers, clinics, and

pharmacies across the USA. *Open Access Research Journal of Biology and Pharmacy,* 2024, 10(02), 081–104. https://oarjbp.com/content/integrating-community-based-partnerships-enhanced-health-outcomes-collaborative-model

[34] Ijiga, A. C., Olola, T. M., Enyejo, L. A., Akpa, F. A., Olatunde, T. I., & Olajide, F. I. (2024). Advanced surveillance and detection systems using deep learning to combat human trafficking. *Magna Scientia Advanced Research and Reviews, 2024*, 11(01), 267–286. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0091.pdf.

[35] Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B. & Okolo, J. N. (2025). Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches. International Journal of Scientific Research and Modern Technology, 4(3), 1–15. https://doi.org/10.38124/ijsrmt.v4i3.376

[36] Imtiaz, N., Wahid, A., Ul Abideen, S. Z., Muhammad Kamal, M., Sehito, N., Khan, S., ... & Alibakhshikenari, M. (2025, January). A deep learning-based approach for the detection of various internet of things intrusion attacks through optical networks. In Photonics (Vol. 12, No. 1, p. 35). MDPI.

[37] James, U. U. (2022). Federated Identity Management Using Secure Enclaves for Cross-Domain Access Control in 5G Edge Networks International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET) Vol. 9, No. 6 doi : https://doi.org/10.32628/IJSRSET25122271

[38] James, U. U., Idika, C. N., & Enyejo, L. A. (2023). Zero Trust Architecture Leveraging AI-Driven Behavior Analytics for Industrial Control Systems in Energy Distribution Networks, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* Volume 9, Issue 4 doi : https://doi.org/10.32628/CSEIT23564522

[39] James, U. U., Idika, C. N., Enyejo, L. A., Abiodun, K., & Enyejo, J. O. (2024). Adversarial Attack Detection Using Explainable AI and Generative Models in Real-Time Financial Fraud Monitoring Systems. *International Journal of Scientific Research and Modern Technology,* 3(12), 142–157. https://doi.org/10.38124/ijsrmt.v3i12.64 4

[40] James, U.U., Olarinoye, H.S., Uchenna, I.R., Idika, C.N., Ngene, O.J., Ijiga, O.M. & Itemuagbor, K. (2025) Combating Deepfake Threats Using X-FACTS Explainable CNN Framework for Enhanced Detection and Cybersecurity Resilience. *Advances in Artificial Intelligence and Robotics Research,* 1, 41-64.https://www.scirp.org/journal/airr

[41] Khan, L. Z., Pedro, J., Costa, N., De Marinis, L., Napoli, A., & Sambo, N. (2022). Data augmentation to improve performance of neural networks for failure management in optical networks. Journal of Optical Communications and Networking, 15(1), 57-67.

[42] Kumar, G., & Altalbe, A. (2024). Artificial intelligence (AI) advancements for transportation security: in-depth insights into electric and aerial vehicle systems. Environment, Development and Sustainability, 1-51.

[43] Li, Z., Zhao, Y., Li, Y., Liu, M., Zeng, Z., Xin, X., ... & Zhang, J. (2020). Self-optimizing optical network with cloud-edge collaboration: architecture and application. IEEE Open Journal of the Computer Society, 1, 220-229.

[44] Mankodiya, H., Obaidat, M. S., Gupta, R., & Tanwar, S. (2021, October). XAI-AV: Explainable artificial intelligence for trust management in autonomous vehicles. In 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI) (pp. 1-5). IEEE.

[45] Maqousi, A., & Basu, K. (2025). IoT Security in Smart Cities: Balancing Connectivity and Resilience. In Complexities and Challenges for Securing Digital Assets and Infrastructure (pp. 95-114). IGI Global Scientific Publishing.

[46] Mehra, A. D. (2020). Unifying adversarial robustness and interpretability in deep neural networks: A comprehensive framework for explainable and secure machine learning models. International Research Journal of Modernization in Engineering Technology and Science, 2(9), 1829-1838.

[47] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. Sustainable Cities and Society, 72, 102994.

[48] Oyekan, M., Igba, E. & Jinadu, S. O.. (2024). Building Resilient Renewable Infrastructure in an Era of Climate and Market Volatility *International Journal of Scientific Research in Humanities and Social Sciences* Volume 1, Issue 1 https://doi.org/10.32628/IJSRSSH243563

[49] Oyekan, M., Jinadu, S. O. & Enyejo, J. O. (2023). Harnessing Data Analytics to Maximize Renewable Energy Asset Performance. International Journal of Scientific Research and Modern Technology, 2(8), 64–80. https://doi.org/10.38124/ijsrmt.v2i8.850

[50] Oyekan, M., Jinadu, S. O. & Enyejo, J. O. (2025). The Role of Strategic Asset Management in Accelerating the Energy Transition, Volume 10, Issue 9, DOI : https://doi.org/10.38124/ijisrt/25sep792

[51] Okereke, O. B., Abejoye, A., Ekhorutomwen, P. A. & Peter-Anyebe, A. C. (2025). Application of SAR-Driven Flood Detection Systems in Wetland Ecosystems and its Implications for Migratory Bird Habitat Management. *International Journal of Innovative Science and Research Technology*. Volume 10, Issue 4, April – 2025 https://doi.org/10.38124/ijisrt/25apr1627

[52] Pedro, J., Costa, N., & Sanders, S. (2022). Cost-effective strategies to scale the capacity of regional optical transport networks. Journal of Optical Communications and Networking, 14(2), A154-A165.

[53] Prakash, P., & Kasthuri, P. (2024, August). Machine Learning Based Denoising Anomaly Detection and Localisation Using BiGRU in Optical Fiber Monitoring. In 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP) (pp. 1-5). IEEE.

[54] Sejan, M. A. S., Rahman, M. H., Shin, B. S., Oh, J. H., You, Y. H., & Song, H. K. (2022). Machine learning for intelligent-reflecting-surface-based wireless communication towards 6G: A review. Sensors, 22(14), 5405.

[55] Singh, S. K., Kumar, S., Chhabra, A., Sharma, A., Arya, V., Srinivasan, M., & Gupta, B. B. (2025). Advancements in secure quantum communication and robust key distribution techniques for cybersecurity applications. Cyber Security and Applications, 100089.

[56] Zhang, X., Feng, C., Gong, X., Zhang, Q., Zong, Y., Hou, W., & Guo, L. (2021). On throughput optimization in software-defined multi-dimensional space division multiplexing optical networks. Journal of Lightwave Technology, 39(9), 2635-2651.