International Journal of Multidisciplinary Research and Growth Evaluation.

AI-Powered Cybersecurity in Edge Computing: Lightweight Neural Models for Anomaly Detection

Olufunbi Babalola [1], Olaitan Miriam Olufisayo Raji [2], Jamiu Olamilekan Akande [3*], Abdullahi Olalekan Abdulkareem [4], Vincent Anyah [5], Adeladan Samson [6], Steve Folorunso [7]

[1] Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh, PA 15213 USA
[2] Western Illinois University Macomb Illinois USA
[3] School of Computing and Digital Technology Birmingham City University, Birmingham UK
[4] Lamar University, College of Business Beaumont Texas USA
[5] Department of Computer Science New Mexico Highlands University USA
[6] Centre of Excellence for Excellence for Artificial Intelligence and Data Modelling University of Hull Cottingham Rd Hull, HU6 7RX United Kingdom.
[7] University of Liverpool United Kingdom

* Corresponding Author: **Jamiu Olamilekan Akande**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 02
March-April 2024
Received: 07-03-2024
Accepted: 08-04-2024
Page No: 1130-1138

Abstract
The proliferation of edge computing has revolutionized data processing by enabling low-latency, real-time analytics at the network periphery. However, this shift has introduced novel cybersecurity challenges, particularly due to the limited computational resources and heightened vulnerability of edge devices. Traditional security mechanisms often fall short in this context, necessitating the development of lightweight and adaptive solutions. This explores the integration of Artificial Intelligence (AI) in edge-based cybersecurity, with a focus on lightweight neural models for anomaly detection. These models leverage the power of deep learning while maintaining computational efficiency suitable for edge environments. Lightweight neural networks such as MobileNets, SqueezeNet, and TinyML architectures are specifically designed to operate under resource constraints, offering an optimal trade-off between accuracy and inference speed. By embedding these models into edge nodes, systems can detect anomalies in real time, enabling rapid response to threats such as intrusion attempts, malware, and data exfiltration. The use of AI enhances detection precision by learning complex patterns and temporal behaviors that traditional rule-based systems may miss. This presents a systematic analysis of model architectures, training methodologies, and deployment strategies that support secure, scalable, and energy-efficient anomaly detection at the edge. We also address key challenges including model compression, adversarial robustness, and on-device learning. Experimental results from edge-device testbeds demonstrate the viability of our approach, achieving high detection accuracy with minimal latency and resource usage. The findings contribute to the growing body of knowledge in AI-powered edge security and pave the way for intelligent, autonomous threat detection frameworks. Ultimately, the fusion of lightweight AI models and edge computing offers a promising avenue for building resilient and responsive cybersecurity systems capable of operating in decentralized, bandwidth-sensitive environments.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.2.1130-1138

Keywords: AI-Powered, Cybersecurity, Edge Computing, Lightweight, Neural Models, Anomaly Detection

1. Introduction

Edge computing has emerged as a transformative paradigm in modern information systems, bringing data processing capabilities closer to the source of data generation (Angel *et al*., 2021; Modupe *et al*., 2024). Unlike traditional cloud-centric architectures,

edge computing distributes computational workloads across decentralized devices such as sensors, gateways, and embedded edge computing distributes computational workloads across decentralized devices such as sensors, gateways, and embedded systems. This decentralization reduces latency, conserves bandwidth, and supports real-time applications in domains like smart manufacturing, autonomous vehicles, and remote healthcare (Jain *et al*., 2021; Khalil *et al*., 2022). By enabling low-latency responses and local decision-making, edge computing addresses critical requirements in time-sensitive and mission-critical applications, making it an essential component of the next-generation digital infrastructure (Gupta *et al*., 2021; Qiu *et al*., 2022).

However, the adoption of edge computing introduces new and complex cybersecurity challenges. The distributed nature of edge devices increases the number of potential attack vectors, making the network more susceptible to intrusions, data tampering, device hijacking, and denial-of-service attacks (Mohammed *et al*., 2020; Gyamfi and Jurcut, 2022). Furthermore, edge nodes often operate in unsecured environments, lack physical protection, and possess heterogeneous configurations, all of which make them attractive targets for malicious actors. The absence of centralized oversight further complicates real-time threat detection and mitigation, creating significant vulnerabilities in edge-based ecosystems (Ferrag *et al*., 2023; Serôdio *et al*., 2023).

In this context, artificial intelligence (AI), particularly machine learning (ML), has gained prominence as a promising solution for proactive and adaptive cybersecurity. Among AI techniques, anomaly detection using deep learning models has demonstrated effectiveness in identifying subtle, previously unseen, and complex attack patterns. AI-powered anomaly detection surpasses traditional signature-based and rule-based systems by learning from dynamic behaviors and adapting to evolving threats (Tanikonda *et al*., 2022; Tanikonda, 2023). This adaptability is especially valuable in edge computing, where threat landscapes are diverse and continuously changing.

Despite the promise of AI, the computational limitations of edge devices such as limited processing power, memory, and battery life necessitate the development of lightweight neural network models (Chang *et al*., 2021; Shuvo *et al*., 2022). These models, including architectures like MobileNets, SqueezeNet, and TinyML frameworks, are optimized for low-resource environments while maintaining high detection performance. Lightweight models reduce latency, enable on-device inference, and minimize the need for continuous communication with central servers, thereby preserving bandwidth and enhancing privacy. As a result, they form a critical backbone for embedding intelligent anomaly detection capabilities directly into edge systems (Eskandari *et al*., 2021; Huang *et al*., 2021).

The integration of lightweight AI models into edge cybersecurity frameworks represents a necessary evolution toward decentralized, autonomous, and resilient security systems (Molokomme *et al*., 2022; Biswas, A. and Wang, 2023). As edge computing becomes increasingly ubiquitous, ensuring the safety and integrity of these distributed environments through efficient, AI-powered mechanisms is imperative. This calls for a concerted research effort to design, implement, and evaluate neural models that align with the stringent resource constraints and dynamic threat landscapes characteristic of edge computing environments (Bommasani *et al*., 2021; Casper *et al*., 2023).

2. Methodology

This systematic review employed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology to identify, screen, and analyze relevant literature addressing the integration of lightweight neural models for anomaly detection within AI-powered cybersecurity frameworks in edge computing environments.

A comprehensive literature search was conducted using electronic databases including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus. Keywords used in the search strategy included combinations of terms such as “edge computing,” “cybersecurity,” “anomaly detection,” “lightweight neural networks,” “AI-based security,” “resource-constrained devices,” and “TinyML.” The search included publications from 2015 to 2025 to reflect the recent developments in edge AI technologies and threat landscapes.

The inclusion criteria comprised peer-reviewed journal articles, conference proceedings, and systematic reviews that specifically addressed the design, development, or evaluation of lightweight AI or deep learning models for security or anomaly detection in edge computing environments. Exclusion criteria involved articles not written in English, those not involving edge or AI technologies, and papers that focused solely on cloud-based or non-AI security solutions.

The initial search yielded 354 records. After removing 102 duplicates, 252 articles underwent title and abstract screening. Of these, 148 articles were excluded based on irrelevance to the core topic. The full texts of the remaining 104 studies were assessed for eligibility, resulting in 47 studies that met the inclusion criteria and were included in the qualitative synthesis.

Data extraction from selected studies focused on research objectives, model architecture (e.g., MobileNet, SqueezeNet, LSTM), deployment platforms (e.g., Raspberry Pi, Jetson Nano), datasets used, anomaly detection methods, and performance metrics including accuracy, latency, and energy efficiency. The final analysis synthesized the findings to identify trends, gaps, and future directions in the use of lightweight neural models for real-time anomaly detection in edge computing security systems.

2.1 Background and Related Work

Traditional cybersecurity techniques have long served as the foundational defense mechanisms in networked systems, relying predominantly on signature-based detection, rule-based engines, and perimeter-based security models such as firewalls, intrusion detection systems (IDS), and antivirus software (Zave and Rexford, 2020; Mogadem *et al*., 2022). While effective in centralized and static environments, these methods face significant limitations when applied to edge computing. Signature-based methods, for instance, depend on predefined attack patterns and fail to detect novel or evolving threats (zero-day attacks). Furthermore, the dynamic and decentralized nature of edge networks makes it difficult to maintain up-to-date signature databases on each device. The computational overhead associated with traditional IDS, often designed for high-performance servers, is impractical for resource-constrained edge devices. Perimeter security models are also less effective in edge environments, where data is generated and processed across

distributed nodes, often bypassing centralized controls entirely.

To address these shortcomings, anomaly detection has emerged as a critical tool in modern cybersecurity frameworks. Unlike signature-based methods, anomaly detection focuses on identifying deviations from expected behavior, enabling the discovery of unknown or emerging threats. Anomaly detection approaches are broadly categorized into statistical methods, rule-based systems, and machine learning-based techniques. Statistical approaches rely on probabilistic modeling and thresholds, while rule-based systems use predefined logical patterns to flag irregularities (Liu *et al*., 2021; Uszko *et al*., 2023). However, these conventional methods often lack the adaptability required for complex and evolving threat landscapes. Machine learning-based anomaly detection offers greater flexibility, as it can learn normal behavior patterns from data and identify outliers with higher precision. Supervised learning, unsupervised clustering, and time-series analysis are commonly used techniques. In edge environments, unsupervised and semi-supervised methods are particularly valuable due to the scarcity of labeled data.

The integration of artificial intelligence (AI), especially deep learning, has significantly advanced the field of cybersecurity. Initially applied in data-rich environments such as enterprise networks and cloud systems, AI has demonstrated remarkable success in detecting complex attack vectors, reducing false positives, and enabling predictive security analytics. Neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders have all been employed for various cybersecurity tasks including malware classification, intrusion detection, and user behavior analysis. Deep learning models can extract hierarchical and non-linear patterns in high-dimensional data, making them well-suited for identifying subtle anomalies that traditional algorithms might overlook (Pedro, 2023; Yang and Zhang, 2023).

As edge computing gains prominence, the need for AI models that can operate under constrained conditions has driven the development of lightweight neural architectures. Unlike conventional deep learning models that require substantial computational resources, lightweight models are designed to function efficiently on devices with limited memory, power, and processing capabilities. Examples include MobileNets, which use depthwise separable convolutions to reduce model complexity, and SqueezeNet, which achieves AlexNet-level accuracy with significantly fewer parameters. TinyML, a growing subfield of machine learning, focuses on deploying inference models directly on microcontrollers and low-power embedded systems (Schizas *et al*., 2022; Alajlan and Ibrahim, 2022). These models are optimized using techniques such as model pruning, quantization, and knowledge distillation to reduce size and improve efficiency without compromising performance.

Numerous studies have demonstrated the effectiveness of lightweight AI models in real-time anomaly detection on edge devices. For instance, variants of MobileNet have been used in intrusion detection systems deployed on Raspberry Pi platforms, achieving high detection accuracy with minimal latency. Similarly, compressed autoencoders have been applied for unsupervised anomaly detection in industrial IoT settings. These advancements underscore the growing feasibility of embedding intelligent security features directly into edge nodes, thereby enabling decentralized and responsive cybersecurity frameworks.

In summary, while traditional cybersecurity methods struggle to adapt to the decentralized, heterogeneous, and resource-constrained landscape of edge computing, AI-driven anomaly detection particularly through lightweight neural models offers a robust alternative. The evolution of such models is crucial for building secure, scalable, and efficient edge systems capable of defending against the increasingly sophisticated threats targeting modern cyber-physical infrastructures (Garg *et al*., 2021; Ometov *et al*., 2022).

2.2 Edge Computing Security Challenges

Edge computing has emerged as a pivotal technological framework to support real-time, decentralized processing in domains such as smart cities, autonomous vehicles, telemedicine, and industrial automation as shown in figure 1. Unlike traditional cloud models that centralize data and computation in remote data centers, edge computing processes data locally on devices such as gateways, sensors, and embedded systems close to the source of data generation. This architectural shift offers significant advantages in latency reduction, bandwidth efficiency, and context-aware decision-making (Islam *et al*., 2021; Cheng *et al*., 2021). However, it also introduces a unique set of security challenges that must be addressed to ensure the integrity, confidentiality, and availability of systems and data operating at the network's edge.

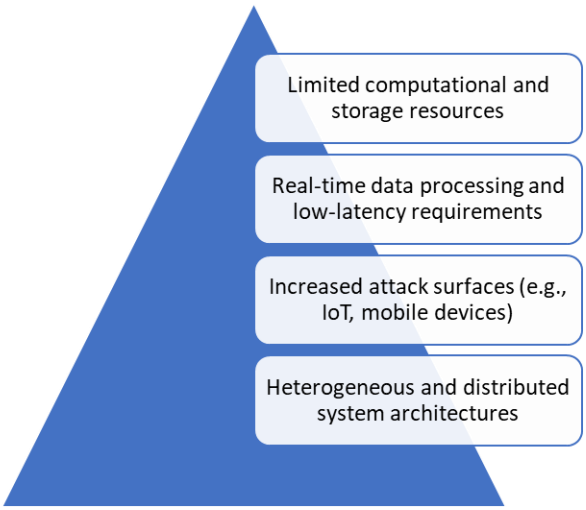

Fig 1: Edge Computing Security Challenges

One of the most significant challenges in securing edge computing systems is the limitation of computational and storage resources. Edge devices, often deployed in compact or embedded environments, typically possess far less processing power, memory, and energy capacity than centralized cloud servers. These constraints hinder the implementation of conventional security measures, such as complex encryption schemes, deep packet inspection, and heavyweight anomaly detection algorithms. As a result, developers are compelled to trade off between security strength and computational feasibility, potentially exposing edge nodes to cyber threats. The limited resources also challenge the deployment of real-time threat mitigation systems that require rapid, local inference and decision-making.

Furthermore, edge computing applications often demand real-time data processing and ultra-low latency, especially in

time-sensitive systems like autonomous vehicles, robotic control, and emergency response networks. These latency requirements limit the extent to which edge devices can rely on cloud-based security monitoring or decision-making. Security operations, including authentication, anomaly detection, and data validation, must occur locally to avoid delay-induced risks. This decentralization of security responsibilities increases the complexity of implementing consistent protection across a widely distributed infrastructure and amplifies the need for lightweight yet effective cybersecurity mechanisms.

The shift to edge computing also increases the attack surface due to the proliferation of connected devices particularly those in the Internet of Things (IoT) ecosystem. Each connected sensor, actuator, or mobile device serves as a potential point of vulnerability. These devices may lack proper security configurations or firmware updates and are often deployed in physically unsecured environments, making them susceptible to physical tampering, eavesdropping, or man-in-the-middle attacks. Moreover, compromised edge nodes can act as gateways for lateral movement across networks, threatening the security of not only local operations but also upstream systems connected to the broader architecture (Ali *et al.*, 2021; Kowalski and Mazurczyk, 2023).

In addition, edge systems are characterized by heterogeneous and distributed architectures, complicating the deployment and enforcement of uniform security policies. Edge environments typically integrate a diverse set of hardware platforms, operating systems, communication protocols, and vendor-specific components. This heterogeneity makes it difficult to apply standardized security protocols or intrusion detection schemes across all devices. The distributed nature of edge computing also reduces central oversight, creating blind spots in threat visibility and response coordination. Furthermore, the dynamic topology of edge networks where devices frequently join, leave, or move between networks poses additional challenges for identity management, secure communication, and trust establishment.

Collectively, these security challenges highlight the need for tailored solutions that are adaptable, scalable, and resource-efficient. Traditional, monolithic security architectures are ill-suited for the edge paradigm. Instead, novel approaches such as decentralized authentication, federated learning, and lightweight AI-based anomaly detection are being explored to safeguard edge computing environments. These approaches must account for device constraints while enabling robust detection of and response to evolving threats. The growing complexity of edge computing systems necessitates a rethinking of cybersecurity strategies to ensure that they evolve in tandem with the architectural and operational shifts defining the modern digital edge (Angel *et al.*, 2021; Judijanto *et al.*, 2023).

2.3 Lightweight Neural Network Architectures

The rise of edge computing and the proliferation of resource-constrained devices such as sensors, mobile phones, and microcontrollers have driven the need for lightweight neural network architectures capable of performing complex machine learning tasks efficiently. These models must deliver high performance while operating under strict limitations on memory, computation, and power consumption. To meet these demands, several innovative neural network architectures and optimization techniques have emerged, including MobileNets, SqueezeNet, and the broader field of TinyML as shown in figure 2. These models are supported by compression strategies such as pruning, quantization, and knowledge distillation that further enhance their deployability on edge and embedded systems (Kim *et al.*, 2021; Aghli and Ribeiro, 2021).

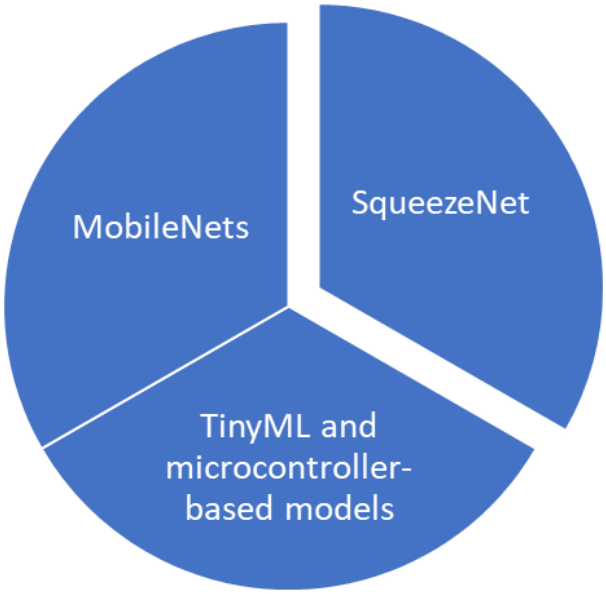

Fig 2: Lightweight Neural Network Architectures

MobileNets are a family of convolutional neural networks (CNNs) specifically designed for mobile and embedded vision applications. Introduced by Google, MobileNets achieve computational efficiency by replacing standard convolution operations with *depthwise separable convolutions*, which split the convolution into two parts: a depthwise convolution and a pointwise convolution. This significantly reduces the number of parameters and floating-point operations required without a substantial loss in accuracy. Variants such as MobileNetV2 and MobileNetV3 further improve efficiency through techniques like inverted residual blocks and neural architecture search. MobileNets have been widely adopted for tasks including image classification, object detection, and anomaly detection in edge-based systems due to their excellent balance between performance and computational cost.

SqueezeNet is another lightweight CNN architecture that achieves comparable accuracy to larger networks such as AlexNet while requiring 50 times fewer parameters. The core idea behind SqueezeNet is the use of "fire modules," which consist of a squeeze layer using 1×1 convolutions followed by an expand layer with a mix of 1×1 and 3×3 convolutions. This configuration drastically reduces the model size while maintaining high representational power. SqueezeNet is especially useful in environments where memory footprint and model download size are critical constraints, making it a preferred choice for deployment on low-power IoT devices and embedded processors.

TinyML represents a burgeoning field that focuses on deploying machine learning models on ultra-low-power microcontrollers. TinyML models are designed to operate within kilobytes of memory and milliwatts of power, making them ideal for deeply embedded edge applications such as real-time anomaly detection, gesture recognition, and speech processing. These models are typically trained on more

powerful machines and then compressed and optimized for deployment. Microcontroller platforms such as ARM Cortex-M, ESP32, and Arduino boards are commonly used for TinyML applications. Frameworks like TensorFlow Lite for Microcontrollers (TFLM) and Edge Impulse facilitate the deployment of lightweight inference engines directly on these constrained devices (Manor and Greenberg, 2022; Saha *et al*., 2022).

To further enhance the efficiency of these architectures, a range of model optimization techniques are employed. *Pruning* involves removing redundant or non-critical weights and neurons from the network, thus reducing model size and inference time. Pruning can be structured (removing entire filters or layers) or unstructured (removing individual weights), and is often followed by fine-tuning to recover lost accuracy. *Quantization* converts 32-bit floating-point weights and activations into lower-precision formats such as 8-bit integers, substantially reducing memory usage and computational overhead while maintaining acceptable accuracy. This is particularly beneficial for running models on hardware with limited support for floating-point arithmetic. *Knowledge distillation* involves training a smaller "student" model to mimic the behavior of a larger, more accurate "teacher" model. This approach enables the student model to retain much of the performance of the teacher while being significantly smaller and faster, making it well-suited for edge deployment.

Lightweight neural network architectures such as MobileNets, SqueezeNet, and TinyML models, combined with advanced optimization techniques like pruning, quantization, and knowledge distillation, provide a robust foundation for deploying AI capabilities in edge computing environments. These developments enable real-time, intelligent decision-making on devices with constrained resources, paving the way for more secure, efficient, and scalable edge-based systems (Coito *et al*., 2021; Diraco *et al*., 2023).

2.4 Anomaly Detection Methodologies

Anomaly detection is a critical component of cybersecurity in edge computing environments, where early identification of irregular behavior can prevent significant operational disruptions or data breaches. Given the decentralized and heterogeneous nature of edge systems, anomaly detection techniques must be robust, adaptive, and capable of operating in resource-constrained settings. Edge environments are particularly vulnerable to several types of anomalies, including *network intrusions*, *device malfunctions*, and *data leakage*. Network intrusions involve unauthorized access or suspicious traffic patterns, such as port scanning or denial-of-service attacks. Device malfunctions, often caused by hardware degradation or firmware errors, can lead to abnormal behavior in sensors or actuators (Gaddam *et al*., 2020; Ayeb *et al*., 2020). Data leakage occurs when sensitive data is accessed or transmitted without authorization, potentially violating user privacy or exposing confidential information.

To detect these diverse threat scenarios, machine learning-based approaches have become prominent, particularly those involving *supervised* and *unsupervised learning*. Supervised learning techniques require labeled datasets with examples of both normal and anomalous behavior. Algorithms such as support vector machines (SVMs), decision trees, and convolutional neural networks (CNNs) are trained to classify input data into normal or anomalous categories. While effective when labeled data is available, supervised methods are often impractical for edge cybersecurity due to the scarcity of labeled anomalies and the evolving nature of threats. By contrast, unsupervised learning techniques do not require labeled data and instead focus on learning patterns of normal behavior. Anomalies are identified as deviations from these learned patterns. Clustering algorithms (e.g., k-means, DBSCAN), autoencoders, and isolation forests are frequently employed in unsupervised anomaly detection. These methods are particularly well-suited for edge environments, where new and previously unseen anomalies may emerge, and labeled datasets are limited or unavailable.

Among the more advanced techniques for anomaly detection are *time-series and sequence-based models*, which are designed to capture temporal dependencies in data. Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRUs) are popular architectures within this category. LSTM and GRU models are capable of learning long-term dependencies and trends from sequences of data, making them ideal for identifying anomalies in streaming data such as CPU usage, network traffic, and sensor readings over time. For instance, an LSTM model can be trained to predict expected values in a time-series, and significant deviations from predictions can be flagged as anomalies. These models are especially useful in edge computing scenarios where real-time monitoring of behavior patterns is essential, such as detecting abrupt changes in energy consumption in a smart grid or identifying irregular telemetry data in autonomous vehicles (Qiu *et al*., 2020; Wu *et al*., 2021).

Effective anomaly detection at the edge also depends heavily on *data collection and preprocessing*. Edge devices generate large volumes of heterogeneous data, often in real time. Efficient data acquisition frameworks must be in place to ensure data quality while minimizing latency and power consumption. Preprocessing steps such as data normalization, noise reduction, feature extraction, and dimensionality reduction are crucial for enhancing model performance and reducing computational load. For example, converting raw network traffic into meaningful features like packet size, duration, and protocol type can improve the accuracy of anomaly detection models. In resource-constrained environments, feature selection is vital to ensure only the most informative data is retained for model input, reducing the burden on edge hardware.

Moreover, privacy and bandwidth considerations often necessitate local data processing and on-device inference. This creates an additional challenge: ensuring that preprocessing and detection pipelines are lightweight and optimized for edge execution. Techniques like federated learning can complement local detection by enabling collaborative model training across multiple edge nodes without sharing raw data, thus preserving privacy while improving detection capabilities (Qayyum *et al*., 2022; Bao and Guo, 2022).

Anomaly detection in edge computing requires a combination of versatile learning approaches, temporal modeling, and efficient data handling. The integration of LSTM/GRU models, unsupervised learning algorithms, and intelligent preprocessing pipelines enables effective identification of cyber threats and system faults in real-time, even in the face of constrained resources and dynamic environments. These methodologies form the foundation of resilient, autonomous edge cybersecurity systems.

2.5 Model Deployment on Edge Devices

Deploying machine learning models on edge devices represents a critical step toward achieving real-time, intelligent cybersecurity and anomaly detection in distributed computing environments as shown in figure 3. Unlike traditional cloud-based AI systems that rely on centralized processing, edge-based deployment enables local inference, allowing data to be analyzed and acted upon directly at or near the source (Duan *et al*., 2022; Solanke, 2023). This architectural shift supports applications with strict latency requirements and limited connectivity while enhancing privacy and reducing bandwidth usage. The two dominant deployment strategies in edge AI are on-device deployment and edge-server deployment, each with distinct advantages and trade-offs.

On-device deployment refers to running the trained AI model directly on the edge device, such as a sensor, gateway, or microcontroller. This approach minimizes latency and supports real-time decision-making without relying on cloud services. It also offers enhanced data privacy, as sensitive information remains on the device. However, it requires models to be highly optimized due to limited computational, memory, and energy resources. In contrast, edge-server deployment involves running models on more powerful, local edge servers that aggregate and process data from multiple devices. While this setup offers greater computational capabilities and flexibility in model complexity, it introduces communication latency and potential network dependencies. Selecting the appropriate deployment method depends on application-specific requirements for response time, power consumption, and data privacy.

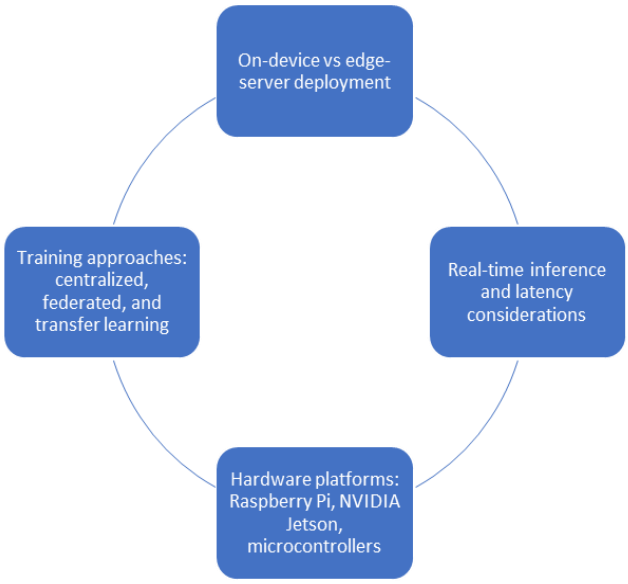

Fig 3: Model Deployment on Edge Devices

Training AI models for edge deployment can follow several paradigms, including centralized, federated, and transfer learning. In centralized learning, all training data is collected and processed in a central server or cloud environment, where a global model is developed and later deployed to edge devices. While effective, this method raises concerns about data privacy and communication overhead. Federated learning offers a privacy-preserving alternative by training models locally on multiple edge devices. The devices compute model updates based on local data and share only these updates (not raw data) with a central coordinator to construct a global model (Zhang *et al*., 2021; Shen *et al*., 2022). This approach enables collaboration without compromising user data privacy and reduces the risks of data breaches during transmission. Transfer learning involves adapting a pre-trained model to a specific edge environment or task using a small amount of local data. This is particularly beneficial in scenarios where edge devices have limited training data and computational power. It allows edge applications to benefit from large-scale models trained on generic datasets while customizing them for local anomaly detection needs.

Real-time inference is a primary driver for edge AI deployment, and latency considerations play a pivotal role in model selection and optimization. Cybersecurity applications often require immediate response to detected threats, such as halting malicious processes or sending alerts. Any delay in inference can reduce the effectiveness of the response. On-device inference eliminates network latency entirely, whereas edge-server deployment introduces some communication delay. To minimize inference time, models must be compact and computationally efficient. Techniques such as model pruning, quantization, and optimized runtime engines (e.g., TensorFlow Lite, ONNX Runtime, TensorRT) are frequently used to accelerate performance.

A range of hardware platforms supports model deployment at the edge, with varying capabilities. Raspberry Pi devices are popular due to their affordability, Linux compatibility, and moderate computational power, making them suitable for lightweight models like MobileNet or SqueezeNet in applications such as home security or smart monitoring. NVIDIA Jetson platforms, including Jetson Nano and Xavier, provide GPU-accelerated computing for more complex models, offering higher performance for applications like video surveillance or autonomous navigation. These devices support advanced deep learning frameworks and enable real-time inference for more demanding AI tasks. At the smallest scale, microcontrollers such as ARM Cortex-M series and ESP32 are used for ultra-low-power TinyML applications (Abadade *et al*., 2023; Ray, 2022). These platforms operate within strict memory and energy budgets, yet they are capable of running quantized neural networks for tasks like sensor anomaly detection or keyword spotting.

The deployment of AI models on edge devices requires careful consideration of architectural strategies, training methodologies, latency constraints, and hardware capabilities. Combining efficient model design with the right deployment framework ensures robust and responsive anomaly detection systems that meet the unique demands of edge computing environments (Martins *et al*., 2022; Ullah and Mahmoud, 2022).

2.6 Performance Evaluation

Evaluating the performance of lightweight neural models deployed in edge computing environments is essential to ensure their effectiveness in real-world cybersecurity applications. These evaluations must consider not only the predictive performance of the model but also the operational constraints inherent to edge devices, such as energy consumption, latency, and hardware limitations. Key metrics typically used to assess model performance include accuracy, precision, recall, latency, and energy consumption (Vakili *et al*., 2020; Naidu *et al*., 2023).

Accuracy indicates the overall correctness of the model's predictions, while precision and recall offer more nuanced

insights. Precision reflects the proportion of true positive predictions among all predicted positives, and is especially important in minimizing false alarms in anomaly detection. Recall measures the ability to identify all relevant anomalies, crucial for avoiding missed threats in cybersecurity scenarios. In edge computing, latency the time taken to process and infer from a single data point is a critical performance indicator, particularly in real-time applications like intrusion detection. Energy consumption is also a key consideration, as many edge devices operate on battery power or energy-harvesting mechanisms. Models that deliver high accuracy but demand excessive energy may be impractical for long-term or mobile deployments.

To comprehensively evaluate lightweight neural architectures, researchers often use real-world edge datasets as benchmarks. These datasets simulate practical edge scenarios, such as the UNSW-NB15 and NSL-KDD for network intrusion detection, and SWaT (Secure Water Treatment) for industrial IoT anomaly detection. Benchmarks based on actual telemetry from edge devices provide realistic conditions under which to assess both detection efficacy and operational efficiency (Varghese *et al*., 2021; Yang *et al*., 2022). These datasets include diverse patterns, temporal behaviors, and noisy signals, offering a robust testing ground for evaluating a model's ability to distinguish between normal and anomalous behavior.

A comparative study of different lightweight models such as MobileNets, SqueezeNet, and TinyML-optimized autoencoders demonstrates varied performance profiles across tasks and environments. For instance, in anomaly detection tasks involving time-series data, LSTM-based models outperform CNNs in recall due to their capacity to capture temporal dependencies. However, they often suffer from higher latency and energy use. MobileNets, with their depthwise separable convolutions, tend to offer a good balance between speed and accuracy, making them ideal for real-time intrusion detection on Raspberry Pi platforms. SqueezeNet achieves significant parameter reduction but may trade off some predictive accuracy in more complex detection tasks. TinyML-optimized models, such as quantized autoencoders or shallow MLPs (multilayer perceptrons), perform well in microcontroller environments where memory and power constraints are severe, though with limited adaptability to complex anomalies.

Use cases across domains illustrate the practical relevance of these models in edge-based anomaly detection. In smart homes, lightweight CNN models deployed on Raspberry Pi devices monitor Wi-Fi traffic or device behavior to detect unauthorized access or unusual activity patterns. The models must respond in real-time, prioritize user privacy, and operate on low-power hardware. In industrial IoT environments, models like GRUs and LSTMs are deployed on edge gateways to monitor sensor streams from machinery, enabling early fault detection and predictive maintenance (Ray *et al*., 2021; Vermesan *et al*., 2022). The performance of these models is evaluated not only on accuracy but also on their ability to operate continuously in harsh, bandwidth-limited settings. In healthcare monitoring, wearable devices use TinyML models to track physiological signals such as heart rate variability or gait patterns. These models detect anomalies that may signal health deterioration or emergency conditions. Their evaluation emphasizes energy efficiency and latency, ensuring that critical alerts are triggered without delay or frequent battery recharge.

Performance evaluation of lightweight neural models for edge anomaly detection must incorporate a multi-dimensional framework that goes beyond conventional accuracy metrics (Luo *et al*., 2021; Kumar, R. and Agrawal, 2023). Latency, energy efficiency, and contextual relevance to real-world applications are equally important. Through comparative studies and deployment in use cases like smart homes, industrial IoT, and healthcare monitoring, researchers and developers can refine these models to meet the unique challenges posed by edge computing environments. The continual evolution of benchmarks and evaluation strategies will be crucial for guiding future innovations in secure, efficient, and intelligent edge-based anomaly detection.

2.7 Challenges and Future Directions

As AI-powered anomaly detection becomes increasingly integrated into edge computing environments, a range of pressing challenges must be addressed to ensure security, adaptability, and long-term effectiveness (Gill *et al*., 2022; Abimannan *et al*., 2023). While lightweight neural models offer a promising solution for real-time threat detection on resource-constrained edge devices, the evolving complexity of threats and operational environments demands ongoing research and innovation. Key areas of concern include adversarial robustness, privacy-preserving learning, adaptive model updates, and the scalability of edge AI systems.

One of the most critical challenges in deploying machine learning at the edge is the susceptibility of models to adversarial attacks. These attacks involve subtly crafted inputs that are designed to deceive the model into making incorrect predictions. In cybersecurity contexts, adversarial examples could allow malicious activities to go undetected by the anomaly detection system. Lightweight models, by nature of their reduced complexity and representational capacity, are particularly vulnerable to such manipulation. Enhancing model robustness against adversarial perturbations is essential. Strategies such as adversarial training, input sanitization, and model ensembling have been proposed, but many remain computationally intensive and thus difficult to implement on constrained edge devices. Future research must develop efficient robustness techniques that can be embedded in lightweight architectures without compromising their operational feasibility.

Another critical area is the implementation of privacy-preserving AI, particularly through federated learning. In traditional centralized training, data from edge devices must be uploaded to a central server, raising significant privacy and security concerns especially in domains like healthcare and finance. Federated learning allows models to be trained locally on devices, with only model updates being shared. This preserves data privacy and reduces bandwidth usage. However, federated learning introduces its own challenges, such as communication overhead, model heterogeneity, and vulnerability to poisoning attacks, where malicious devices can corrupt the global model (Xia *et al*., 2023; Almutairi and Barnawi, 2023). Future advancements must focus on robust aggregation methods, efficient update protocols, and secure communication channels to make federated learning more scalable and resilient in large, heterogeneous edge networks.

The dynamic nature of edge environments also necessitates support for lifelong and online learning, where models can continuously adapt to new data without requiring full retraining. Anomaly detection systems must be able to recognize previously unseen patterns, evolving threats, and

concept drift—the gradual change in data distribution over time (Seraj and Ahmed, 2020; Pillai, 2022). Implementing online learning at the edge poses significant computational and memory challenges. Lightweight, incremental learning algorithms and memory-efficient neural architectures are needed to allow real-time updates with minimal resource overhead. Additionally, mechanisms for model validation and drift detection must be developed to ensure that updates do not degrade performance or introduce instability.

Scalability and maintainability are further challenges in real-world edge AI deployments. As edge systems expand across numerous devices and environments, ensuring consistent model performance and manageability becomes increasingly complex. Each device may differ in hardware capabilities, data characteristics, and threat exposure, requiring models to be customized or fine-tuned accordingly. This heterogeneity complicates large-scale deployment, version control, and remote maintenance. Solutions such as modular AI pipelines, automated deployment tools, and cloud-assisted orchestration frameworks can help manage and update edge AI systems at scale (Goethals *et al*., 2021; Mungoli, 2023). However, there remains a need for standardized APIs, lightweight model update protocols, and fault-tolerant deployment strategies that can seamlessly integrate with diverse edge infrastructures.

While lightweight neural models for anomaly detection offer considerable promise for enhancing cybersecurity in edge computing, realizing their full potential requires addressing key technical challenges. Robustness against adversarial threats, privacy-preserving learning mechanisms, continual adaptation through lifelong learning, and scalable system maintenance are all crucial for the long-term viability of edge AI. Future research must strive to develop integrated frameworks that balance performance, security, and resource efficiency, enabling intelligent, resilient, and privacy-conscious edge computing systems to meet the demands of next-generation applications (Chen *et al*., 2021; Nimsarkar *et al*., 2023; Gami *et al*., 2023).

Conclusion

This has explored the integration of lightweight neural network architectures for anomaly detection in AI-powered cybersecurity systems within edge computing environments. The review highlights the pressing need for adaptive, real-time security solutions capable of operating under resource constraints, given the increasing vulnerability of decentralized and heterogeneous edge networks. Lightweight models such as MobileNets, SqueezeNet, and TinyML frameworks offer a promising balance between computational efficiency and detection performance, enabling effective on-device inference with minimal latency and energy consumption. Additionally, techniques like pruning, quantization, and knowledge distillation further enhance the deployability of AI models in constrained edge settings.

The findings emphasize that while traditional security approaches are insufficient for edge systems, AI-driven anomaly detection especially when informed by time-series models like LSTM and GRU provides superior adaptability and accuracy. Furthermore, deployment strategies such as federated learning and transfer learning offer privacy-preserving and scalable pathways for training and updating models across distributed edge nodes. Real-world use cases in smart homes, industrial IoT, and healthcare demonstrate the practical impact of these methods.

The implications of this work suggest a transformative role for AI in securing the edge, making it possible to detect and respond to cyber threats autonomously and efficiently. However, several challenges remain, particularly in ensuring model robustness against adversarial attacks, supporting lifelong learning, and maintaining system scalability.

Therefore, continued interdisciplinary research is essential to develop more resilient, efficient, and secure AI models tailored for the edge. Future advancements must address the balance between performance and resource consumption while reinforcing data privacy and system adaptability, ultimately contributing to the evolution of secure, intelligent edge computing infrastructures.

References

1. Abadade Y, Temouden A, Bamoumen H, Benamar N, Chtouki Y, Hafid AS. A comprehensive survey on TinyML. IEEE Access. 2023;11:96892-922.
2. Abimannan S, El-Alfy ESM, Hussain S, Chang YS, Shukla S, Satheesh D, *et al*. Towards federated learning and multi-access edge computing for air quality monitoring: literature review and assessment. Sustainability. 2023;15(18):13951.
3. Aghli N, Ribeiro E. Combining weight pruning and knowledge distillation for CNN compression. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2021 Jun; [place unknown]. Piscataway (NJ): IEEE; 2021. p. 3191-8.
4. Alajlan NN, Ibrahim DM. TinyML: enabling of inference deep learning models on ultra-low-power IoT edge devices for AI applications. Micromachines. 2022;13(6):851.
5. Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: a review. IEEE Access. 2021;9:18706-21.
6. Almutairi S, Barnawi A. Federated learning vulnerabilities, threats and defenses: a systematic review and future directions. Internet Things. 2023;24:100947.
7. Angel NA, Ravindran D, Vincent PDR, Srinivasan K, Hu YC. Recent advances in evolving computing paradigms: cloud, edge, and fog technologies. Sensors. 2021;22(1):196.
8. Angel NA, Ravindran D, Vincent PDR, Srinivasan K, Hu YC. Recent advances in evolving computing paradigms: cloud, edge, and fog technologies. Sensors. 2021;22(1):196.
9. Ayeb N, Rutten E, Bolle S, Coupaye T, Douet M. Coordinated autonomic loops for target identification, load and error-aware device management for the IoT. In: 2020 15th Conference on Computer Science and Information Systems (FedCSIS); 2020 Sep; [place unknown]. Piscataway (NJ): IEEE; 2020. p. 491-500.
10. Bao G, Guo P. Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. J Cloud Comput. 2022;11(1):94.
11. Biswas A, Wang HC. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors. 2023;23(4):1963.
12. Bommasani R, Hudson DA, Adeli E, Altman R, Arora S, von Arx S, *et al*. On the opportunities and risks of foundation models. arXiv [Preprint]. 2021 [cited 2025 Aug 8]. Available from:

https://arxiv.org/abs/2108.07258.
13. Casper S, Davies X, Shi C, Gilbert TK, Scheurer J, Rando J, *et al*. Open problems and fundamental limitations of reinforcement learning from human feedback. arXiv [Preprint]. 2023 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2307.15217.
14. Chang Z, Liu S, Xiong X, Cai Z, Tu G. A survey of recent advances in edge-computing-powered artificial intelligence of things. IEEE Internet Things J. 2021;8(18):13849-75.
15. Chen J, Ramanathan L, Alazab M. Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. Microprocess Microsyst. 2021;81:103722.
16. Cheng B, Wang M, Lin X, Chen J. Context-aware cognitive QoS management for networking video transmission. IEEE/ACM Trans Netw. 2021;29(3):1422-34.
17. Coito T, Firme B, Martins MS, Vieira SM, Figueiredo J, Sousa JM. Intelligent sensors for real-time decision-making. Automation. 2021;2(2):62-82.
18. Diraco G, Rescio G, Siciliano P, Leone A. Review on human action recognition in smart living: sensing technology, multimodality, real-time processing, interoperability, and resource-constrained processing. Sensors. 2023;23(11):5281.
19. Duan S, Wang D, Ren J, Lyu F, Zhang Y, Wu H, *et al*. Distributed artificial intelligence empowered by end-edge-cloud computing: a survey. IEEE Commun Surv Tutor. 2022;25(1):591-624.
20. Eskandari M, Janjua ZH, Vecchio M, Antonelli F. Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet Things J. 2020;7(8):6882-97.
21. Ferrag MA, Friha O, Kantarci B, Tihanyi N, Cordeiro L, Debbah M, *et al*. Edge learning for 6G-enabled internet of things: a comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Commun Surv Tutor. 2023;25(4):2654-713.
22. Gaddam A, Wilkin T, Angelova M, Gaddam J. Detecting sensor faults, anomalies and outliers in the internet of things: a survey on the challenges and solutions. Electronics. 2020;9(3):511.
23. Gami B, Agrawal M, Mishra DK, Quasim D, Mehra PS. Artificial intelligence-based blockchain solutions for intelligent healthcare: a comprehensive review on privacy preserving techniques. Trans Emerg Telecommun Technol. 2023;34(9):e4824.
24. Garg S, Kaur K, Kaddoum G, Garigipati P, Aujla GS. Security in IoT-driven mobile edge computing: new paradigms, challenges, and opportunities. IEEE Netw. 2021;35(5):298-305.
25. Gill SS, Xu M, Ottaviani C, Patros P, Bahsoon R, Shaghaghi A, *et al*. AI for next generation computing: emerging trends and future directions. Internet Things. 2022;19:100514.
26. Goethals T, Volckaert B, De Turck F. Enabling and leveraging AI in the intelligent edge: a review of current trends and future directions. IEEE Open J Commun Soc. 2021;2:2311-41.
27. Gupta R, Reebadiya D, Tanwar S. 6G-enabled edge intelligence for ultra-reliable low latency applications: vision and mission. Comput Stand Interfaces. 2021;77:103521.
28. Gyamfi E, Jurcut A. Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors. 2022;22(10):3744.
29. Huang H, Yang L, Wang Y, Xu X, Lu Y. Digital twin-driven online anomaly detection for an automation system based on edge intelligence. J Manuf Syst. 2021;59:138-50.
30. Islam MSU, Kumar A, Hu YC. Context-aware scheduling in fog computing: a survey, taxonomy, challenges and future directions. J Netw Comput Appl. 2021;180:103008.
31. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, *et al*. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access. 2021;9:130264-328.
32. Judijanto L, Hindarto D, Wahjono SI. Edge of enterprise architecture in addressing cyber security threats and business risks. Int J Softw Eng Comput Sci. 2023;3(3):386-96.
33. Khalil U, Malik OA, Uddin M, Chen CL. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions. Sensors. 2022;22(14):5168.
34. Kim J, Chang S, Kwak N. PQK: model compression via pruning, quantization, and knowledge distillation. arXiv [Preprint]. 2021 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2106.14681.
35. Kowalski M, Mazurczyk W. Toward the mutual routing security in wide area networks: a scoping review of current threats and countermeasures. Comput Netw. 2023;230:109778.
36. Kumar R, Agrawal N. Analysis of multi-dimensional Industrial IoT (IIoT) data in edge–fog–cloud based architectural frameworks: a survey on current state and research challenges. J Ind Inf Integr. 2023;35:100504.
37. Liu Q, Hagenmeyer V, Keller HB. A review of rule learning-based intrusion detection systems and their prospects in smart grids. IEEE Access. 2021;9:57542-64.
38. Luo Y, Xiao Y, Cheng L, Peng G, Yao D. Deep learning-based anomaly detection in cyber-physical systems: progress and opportunities. ACM Comput Surv. 2021;54(5):1-36.
39. Manor E, Greenberg S. Custom hardware inference accelerator for tensorflow lite for microcontrollers. IEEE Access. 2022;10:73484-93.
40. Martins I, Resende JS, Sousa PR, Silva S, Antunes L, Gama J. Host-based IDS: a review and open issues of an anomaly detection system in IoT. Future Gener Comput Syst. 2022;133:95-113.
41. Modupe OT, Otitoola AA, Oladapo OJ, Abiona OO, Oyeniran OC, Adewusi AO, *et al*. Reviewing the transformational impact of edge computing on real-time data processing and analytics. Comput Sci IT Res J. 2024;5(3):603-702.
42. Mogadem MM, Li Y, Meheretie DL. A survey on internet of energy security: related fields, challenges, threats and emerging technologies. Cluster Comput. 2022;25:1-37.
43. Mohammed H, Hasan SR, Awwad F. Fusion-on-field security and privacy preservation for IoT edge devices: concurrent defense against multiple types of hardware

trojan attacks. IEEE Access. 2020;8:36847-62.
44. Molokomme DN, Onumanyi AJ, Abu-Mahfouz AM. Edge intelligence in smart grids: a survey on architectures, offloading models, cyber security measures, and challenges. J Sens Actuator Netw. 2022;11(3):47.
45. Mungoli N. Scalable, distributed AI frameworks: leveraging cloud computing for enhanced deep learning performance and efficiency. arXiv [Preprint]. 2023 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2304.13738.
46. Naidu G, Zuva T, Sibanda EM. A review of evaluation metrics in machine learning algorithms. In: Computer Science On-line Conference; 2023 Apr; Cham: Springer International Publishing; 2023. p. 15-25.
47. Nimsarkar SA, Gupta RR, Ingle RB. RuCIL: enabling privacy-enhanced edge computing for federated learning. In: International Conference on Edge Computing; 2023 Dec; Cham: Springer Nature Switzerland; 2023. p. 24-36.
48. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022;22(3):927.
49. Pedro F. A review of data mining, big data analytics, and machine learning approaches. J Comput Nat Sci. 2023;3(4):169-81.
50. Pillai V. Anomaly detection for innovators: transforming data into breakthroughs. Hyderabad: Libertatem Media Private Limited; 2022.
51. Qayyum A, Ahmad K, Ahsan MA, Al-Fuqaha A, Qadir J. Collaborative federated learning for healthcare: multi-modal COVID-19 diagnosis at the edge. IEEE Open J Comput Soc. 2022;3:172-84.
52. Qiu T, Chi J, Zhou X, Ning Z, Atiquzzaman M, Wu DO. Edge computing in industrial internet of things: architecture, advances and challenges. IEEE Commun Surv Tutor. 2020;22(4):2462-88.
53. Qiu Y, Niu J, Zhu X, Zhu K, Yao Y, Ren B, *et al*. Mobile edge computing in space-air-ground integrated networks: architectures, key technologies and challenges. J Sens Actuator Netw. 2022;11(4):57.
54. Rangaraju S. AI sentry: reinventing cybersecurity through intelligent threat detection. EPH-Int J Sci Eng. 2023;9(3):30-5.
55. Ray P, Kaluri R, Reddy T, Lakshmanna K. Contemporary developments and technologies in deep learning–based IoT. In: Deep learning for internet of things infrastructure. Boca Raton: CRC Press; 2021. p. 61-82.
56. Ray PP. A review on TinyML: state-of-the-art and prospects. J King Saud Univ Comput Inf Sci. 2022;34(4):1595-623.
57. Saha SS, Sandha SS, Srivastava M. Machine learning for microcontroller-class hardware: a review. IEEE Sens J. 2022;22(22):21362-90.
58. Schizas N, Karras A, Karras C, Sioutas S. TinyML for ultra-low power AI and large scale IoT deployments: a systematic review. Future Internet. 2022;14(12):363.
59. Seraj R, Ahmed M. Concept drift for big data. In: Combating security challenges in the age of big data: powered by state-of-the-art artificial intelligence techniques. Cham: Springer; 2020. p. 29-43.
60. Serôdio C, Cunha J, Candela G, Rodriguez S, Sousa XR, Branco F. The 6G ecosystem as support for IoE and private networks: vision, requirements, and challenges. Future Internet. 2023;15(11):348.
61. Shen S, Zhu T, Wu D, Wang W, Zhou W. From distributed machine learning to federated learning: in the view of data privacy and security. Concurrency Comput Pract Exp. 2022;34(16):e6002.
62. Shuvo MMH, Islam SK, Cheng J, Morshed BI. Efficient acceleration of deep learning inference on resource-constrained edge devices: a review. Proc IEEE. 2022;111(1):42-91.
63. Solanke A. Edge computing integration with enterprise cloud systems: architectural patterns for distributed intelligence. Int J Eng Comput Sci. 2023;12(03).
64. Tanikonda A, Pandey BK, Peddinti SR, Katragadda SR. Advanced AI-driven cybersecurity solutions for proactive threat detection and response in complex ecosystems. J Sci Technol. 2022;3(1).
65. Ullah I, Mahmoud QH. Design and development of RNN anomaly detection model for IoT networks. IEEE Access. 2022;10:62722-50.
66. Uszko K, Kasprzyk M, Natkaniec M, Chołda P. Rule-based system with machine learning support for detecting anomalies in 5G WLANs. Electronics. 2023;12(11):2355.
67. Vakili M, Ghamsari M, Rezaei M. Performance analysis and comparison of machine and deep learning algorithms for IoT data classification. arXiv [Preprint]. 2020 [cited 2025 Aug 8]. Available from: https://arxiv.org/abs/2001.09636.
68. Varghese B, Wang N, Bermbach D, Hong CH, Lara ED, Shi W, *et al*. A survey on edge performance benchmarking. ACM Comput Surv. 2021;54(3):1-33.
69. Vermesan O, Coppola M, Bahr R, Bellmann RO, Martinsen JE, Kristoffersen A, *et al*. An intelligent real-time edge processing maintenance system for industrial manufacturing, control, and diagnostic. Front Chem Eng. 2022;4:900096.
70. Wu D, Xu H, Jiang Z, Yu W, Wei X, Lu J. EdgeLSTM: towards deep and sequential edge computing for IoT applications. IEEE/ACM Trans Netw. 2021;29(4):1895-908.
71. Xia G, Chen J, Yu C, Ma J. Poisoning attacks in federated learning: a survey. IEEE Access. 2023;11:10708-22.
72. Yang M, Zhang J. Data anomaly detection in the internet of things: a review of current trends and research challenges. Int J Adv Comput Sci Appl. 2023;14(9).
73. Yang Y, Elsinghorst R, Martinez JJ, Hou H, Lu J, Deng ZD. A real-time underwater acoustic telemetry receiver with edge computing for studying fish behavior and environmental sensing. IEEE Internet Things J. 2022;9(18):17821-31.
74. Zave P, Rexford J. Patterns and interactions in network security. ACM Comput Surv. 2020;53(6):1-37.
75. Zhang C, Xie Y, Bai H, Yu B, Li W, Gao Y. A survey on federated learning. Knowl Based Syst. 2021;216:106775.