

REVIEW

Open Access



Securing campus networks with intelligence: a review of machine learning techniques for ddos and arp protection

Kirungi Richard^{1*} , Bashir Olaniyi Sadiq^{2,3} and Venkateswarlu Maniniti¹

*Correspondence:

Kirungi Richard

kirungi@kiu.ac.ug

¹Department of Computing and Information Technology, Kampala International University, Kampala, Uganda

²Department of Electrical, Telecommunication and Computer Engineering, Kampala International University, Kampala, Uganda

³Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria

Abstract

The increasing digitization of academic environments has made campus networks essential for learning, research, and administration; however, these networks are highly vulnerable to evolving cyber threats. Among these threats, Distributed Denial of Service (DDoS) and Address Resolution Protocol (ARP) spoofing attacks pose significant risks to network availability, integrity, and confidentiality. Traditional rule-based and signature-based intrusion detection systems are limited by their static nature and poor adaptability to the dynamic traffic patterns typical of campus networks. This review systematically examines Machine Learning (ML) techniques for detecting and preventing DDoS and ARP attacks. Guided by the PRISMA framework, a total of 110 studies were selected from 206 peer-reviewed papers published from 2020 to 2025. Supervised, unsupervised, and hybrid ML models utilizing algorithms such as Random Forests, Support Vector Machines, Convolutional Neural Networks, Long Short-Term Memory networks, and CNN-LSTM ensembles demonstrate high detection accuracy and robust anomaly modeling under real-time, resource-constrained conditions. Integration with Software-Defined Networking (SDN), federated learning, and edge computing enhances scalability, privacy preservation, and low-latency mitigation. Despite these advances, challenges remain in dataset representativeness, model generalization, interpretability, computational overhead, and the development of unified frameworks capable of simultaneously mitigating volumetric DDoS, application-layer attacks, and Layer-2 ARP spoofing. Emerging approaches, such as reinforcement learning and explainable AI, offer promise for adaptive, zero-day, and adversarial threat mitigation. The review highlights the need for modular, context-aware, and scalable ML frameworks validated on real campus traffic to enable resilient and operationally feasible intrusion detection and prevention. These insights provide a foundation for designing secure, adaptive, and intelligent network defense strategies in modern campus environments.

Keywords Machine Learning, DDoS, ARP Spoofing, Campus Network Security, IDPS, Deep Learning Models, IoT and SDN



© The Author(s) 2026. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

1 Introduction

The growth and integration of digital technologies and reliance on interconnected systems have made campus networks essential for academic, administrative, and research activities, supporting various users and devices in a high-traffic environment [1]. However, their complexity makes them vulnerable to cyberattacks, particularly in higher education institutions [2]. Among the most common threats are Distributed Denial of Service (DDoS) attacks and Address Resolution Protocol (ARP) spoofing attacks, which pose significant challenges to network availability, confidentiality, and integrity [3].

DDoS attacks overwhelm network resources by flooding them with illegitimate requests, resulting in service degradation or complete denial of service for legitimate users [4]. These attacks are effective because they use multiple compromised computer systems as sources of attack traffic [5]. ARP spoofing manipulates the ARP process by sending falsified messages, allowing attackers to intercept, alter, or disrupt communication between devices [6]. Both types of attacks undermine campus services and create entry points for advanced intrusions, such as data theft and unauthorized access. Traditional defenses like firewalls and intrusion detection systems are limited in effectiveness due to their inability to adapt to modern attack patterns. This has spurred interest in machine learning (ML) techniques, which offer adaptive, data-driven methods for real-time anomaly detection and prediction of malicious behavior [7].

As identified by authors [8], ML techniques effectively detect anomalies and prevent attacks in network security by learning patterns from traffic. They distinguish between malicious activities and update detection strategies for new attack vectors. By analyzing large-scale traffic data, these models identify hidden patterns and differentiate between normal and malicious behaviors. Techniques such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Deep Learning are increasingly used to detect and prevent DDoS and ARP spoofing attacks [9]. Their ability to learn from historical and real-time traffic enables proactive defense strategies that are more resilient to zero-day attacks and dynamic threats [10].

In campus networks, ML-based security solutions significantly outperform traditional rule-based approaches by learning from historical and real-time data to detect anomalies and hidden threats [11]. This capability is essential for mitigating DDoS and ARP spoofing attacks that blend into legitimate traffic. By using supervised, unsupervised, or hybrid ML models, campus networks can implement adaptive defenses that identify malicious activity early and automate real-time responses [12]. Transitioning to ML requires algorithmic innovations, efficient feature engineering, privacy-preserving data collection, and integration with security frameworks [13]. Advancements in federated learning, reinforcement learning, and explainable AI enhance the accuracy, scalability, and trustworthiness of ML-based anomaly detection systems, making them reliable safeguards for campus networks against DDoS and ARP spoofing threats [14].

This review analyzes the existing literature on machine learning techniques to mitigate and prevent DDoS and ARP spoofing attacks in campus networks. It evaluates the methodologies, algorithms, and frameworks developed, highlighting their strengths, limitations, and practical implications. Additionally, it identifies research gaps and future directions, offering insights into effectively leveraging machine learning for more robust and adaptive network security systems for campus networks.

2 Background of DDoS and ARP prevention

ML has become a cornerstone in addressing the increasing sophistication of DDoS and ARP spoofing attacks, especially in complex environments like campus and IoT networks [15]. These environments are marked by high traffic variability, a range of devices, and dynamic topologies, making anomaly detection using traditional methods more challenging [16]. Compounding these challenges, botnets networks of compromised devices controlled by a single botmaster enable a variety of malicious activities, including DDoS attacks, spam campaigns, and phishing operations, thereby posing a significant threat to the integrity, availability, and security of networks. The proliferation of IoT devices, such as smartphones, smart home appliances, industrial sensors, and medical equipment, further expands the attack surface, as their inherent limitations in processing, memory, and power make them particularly vulnerable to compromise.

DDoS attacks target higher network layers and create high-volume anomalies, while ARP spoofing is a Layer 2 threat that exploits the trust-based characteristics of the ARP. Unlike higher-layer intrusions that produce noticeable flow deviations, ARP spoofing subtly alters IP–MAC bindings without authentication, resulting in low-volume poisoning patterns that can be mistaken for legitimate traffic. This poses challenges for anomaly detection, especially for machine learning methods that rely on strong feature representation and sufficient signal strength. In campus IoT environments marked by dynamic DHCP allocations, diverse devices, high broadcast traffic, and frequent device mobility these issues are intensified, limiting the effectiveness of models trained on controlled or synthetic datasets.

Numerous studies have demonstrated the effectiveness of ML-based approaches in detecting and preventing DDoS and ARP attacks across various datasets and network environments [17]. Traditional prevention mechanisms struggle with modern threats due to their scale and adaptability. Several studies [18, 19], have demonstrated the high accuracy of ML-based approaches in detecting and preventing DDoS and ARP attacks across diverse datasets and environments. RF classifiers have achieved detection accuracies that surpass those of baseline algorithms such as Naïve Bayes, K-Nearest Neighbors, Linear Discriminant Analysis, and Support Vector Machines [20]. In addition to their accuracy, RF models consistently demonstrate high precision, recall, and F1-scores, indicating robust classification performance. Similarly, deep learning-based neural network classifiers for DDoS flooding detection have reported accuracies that further validate the suitability of machine learning techniques for large-scale intrusion detection [18]. This further underscores the effectiveness of advanced ML models in intrusion detection.

Significant advancements have been made in mitigating ARP spoofing attacks, which operate at the link layer and can facilitate man-in-the-middle and denial-of-service scenarios. The ARP-PROBE framework, an explainable deep learning-based system designed for IoT environments, achieved the best accuracy results with extremely low false positive and false negative rates [21]. These results highlight the potential of explainable machine learning models to enhance both detection performance and operational trust.

Both DDoS and ARP attacks significantly degrade campus network performance by overwhelming infrastructure resources and compromising communication integrity. Global cyberattack reports indicate that these threats are widespread and continue to

increase in both frequency and sophistication across regions [22]. Figure 1 illustrates the global distribution of DDoS attacks, highlighting the pervasive nature of these threats.

Recent advancements in ML have enabled real-time analysis of high-volume traffic data, enhancing detection speed, accuracy, and response efficiency [23]. Integrating these techniques into campus networks fosters the development of proactive, resilient, and scalable security frameworks that can adapt to evolving cyber threats [24].

2.1 Historical Approaches and Challenges in DDOS and ARP prevention

Detecting and preventing DDoS attacks and ARP threats relied on rule-based systems that utilized expert knowledge and predefined policies. Network administrators and engineers established thresholds based on observed traffic patterns and past experiences to identify unusual behavior. Prevention of ARP spoofing depended on static ARP tables, host-based authentication, and manual network monitoring [25]. While these methods provided basic security, they struggled to adapt to the increasing sophistication and volume of attacks, particularly in dynamic environments like campus networks, where diverse devices and user activities generate complex traffic patterns. These methods proved ineffective in scaling within such environments due to the frequent addition of devices and user mobility [26].

ML began to play a role in anomaly detection and prevention due to the limitations of earlier methods. In the late 1990s and early 2000s, ML-based approaches used supervised learning models like decision trees, Naïve Bayes, and SVM to classify traffic as benign or malicious [27]. These models improved upon rule-based systems by identifying statistical deviations in network flows instead of relying on static signatures. In ARP spoofing, ML detected abnormal mapping patterns and packet inconsistencies, preventing man-in-the-middle attacks in campus LANs [28]. These early models relied on engineered features, and their accuracy was limited by the quality and size of training datasets.

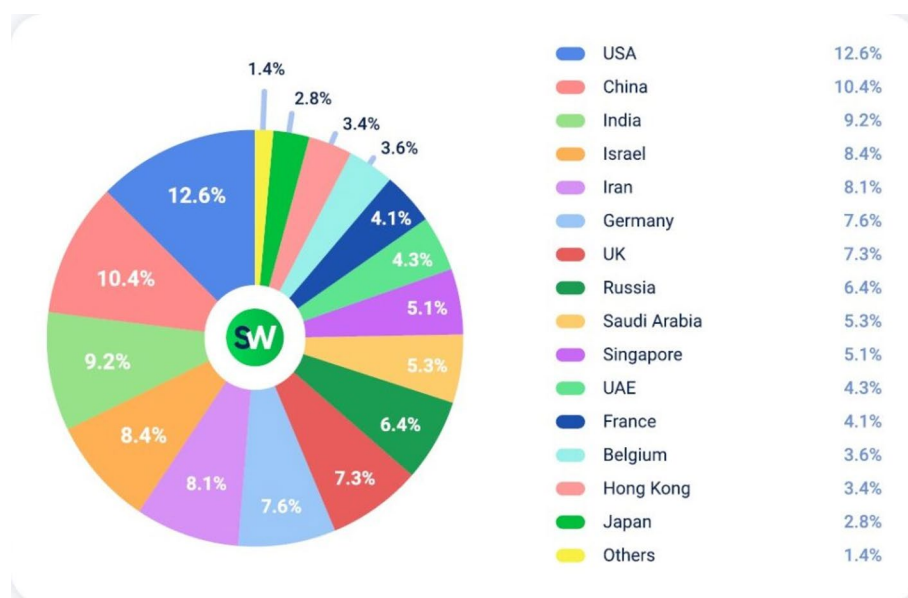


Fig. 1 A Pie Chart of Global DDoS Attack Report (Checkpoint research, 2024)

The earlier approaches faced limitations, including high false-positive rates, limited scalability, and an inability to detect novel attack vectors. These issues highlighted the need for more adaptive and intelligent mechanisms, especially for complex or distributed attack patterns. The influx of IoT devices and sensor networks in campus environments added further challenges, as conventional rule-based systems struggled to scale and accommodate diverse IoT traffic [29]. This resulted in limited protection, often causing false positives or delayed responses. The challenge of detecting and preventing evolving threats was particularly pronounced in dynamic university environments [30], characterized by high device turnover, diverse users, and varied traffic from academic, administrative, and research activities, the integration of Software-Defined Networks (SDN), IoT, and Wireless Body Area Networks (WBANs) in university networks complicates traditional prevention methods [31]. The evolution of network security strategies integrates ML, emphasizing the complexity of campus networks and the need for advanced ML systems for anomaly detection models that can adapt to heterogeneous traffic patterns [32]. This approach emphasizes hybrid deep learning methods such as CNN-LSTM, Variational Autoencoders, and Graph Neural Networks, which provide more accurate and real-time detection and mitigation of DDoS and ARP attacks in modern campus networks [33]. Table 1 Shows the historical Development of Machine Learning in DDoS and ARP Prevention on Campus Networks from 1990-present.

2.2 Developments and achievements of ML approaches in the field

Efforts to prevent DDoS and ARP attacks on campus networks combined protocol-level defenses with emerging machine learning techniques, marking a transition from static to adaptive approaches. Initial strategies relied on network- and link-layer mechanisms, such as ingress/egress filtering (e.g., BCP38) to block IP spoofing, router-based rate limiting to mitigate flooding attacks, and static ARP entries or VLAN segmentation to reduce exposure to spoofing [25]. While these methods provided foundational safeguards, they were largely reactive, protocol-specific, and unable to cope with the dynamic nature of campus environments, where devices frequently join, leave, and generate diverse traffic flows. To address these limitations, research shifted toward supervised machine learning

Table 1 Showing the historical Development of Machine Learning in DDoS and ARP Prevention on Campus Networks from 1990-present

Period	Methods/Technologies	Algorithms Used	Limitations
1990–2000	Rule-based anomaly detection, early intrusion detection systems (IDS) in campus LANs [34–36]	Threshold-based filtering, Signature-based IDS, Basic Statistical Models, Linear Regression, K-Nearest Neighbors (KNN)	Could only detect known attacks; poor scalability; high false negatives; manual tuning required
2000–2010	Early ML adoption for anomaly detection; KDD'99 & DARPA datasets widely used [37, 38]	Decision Trees (C4.5), Naïve Bayes, Support Vector Machines (SVM), k-Nearest Neighbors (kNN)	Depended heavily on feature engineering; struggled with high-dimensional data; limited real-time capability
2010–2020	Integration of ML with SDN, IoT, and campus network security frameworks [39–41]	Random Forest, Principal Component Analysis (PCA), Clustering (k-means), Neural Networks (ANN), Ensemble Learning	High false positive rates; limited adaptability to novel attacks; resource-intensive for IoT/WBAN devices
2020–Present	Advanced ML and Deep Learning for real-time detection in SDN-enabled campus and IoT/WBAN networks [42–44]	Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Hybrid ML-DL models, Reinforcement Learning	High computational cost; requires large labeled datasets; deployment complexity in resource-constrained environments (IoT/WBAN); explainability challenges

models, such as SVMs, Decision Trees, and RFs, which leveraged labeled datasets of normal versus malicious traffic to detect anomalies in real time [45]. This represented a breakthrough compared to static rule systems, as it enabled high-volume classification of traffic and adaptive anomaly detection and prevention. In parallel, clustering methods like k-Means and k-Nearest Neighbor were introduced to uncover hidden patterns of ARP spoofing within campus LANs, providing the first automated mechanisms for identifying insider threats and local man-in-the-middle attacks [46].

A critical limitation identified in traditional protocol-based defenses is their inability to scale in response to emerging trends such as the proliferation of IoT, the adoption of BYOD, the implementation of SDNs, and the increasing integration of WBANs within campus infrastructures. While mechanisms like Dynamic ARP Inspection and DHCP snooping have improved ARP security, their reliance on significant administrative overhead and specialized hardware has constrained deployment in resource-limited academic settings [47]. TCP hardening measures, such as SYN cookies, were effective against basic volumetric floods but fell short against more sophisticated multi-vector DDoS campaigns. These shortcomings highlighted a critical gap; although protocol rules provided baseline resilience, they lacked the intelligence to detect unknown anomalies, adapt to evolving adversarial strategies, or autonomously respond to subtle deviations in network behavior [48]. These challenges become more pronounced in environments shaped by SDN-driven traffic management, IoT device diversity, and WBAN communications [49].

Significant advancement in campus network prevention has been the integration of multiple machine learning algorithms into ensemble learning frameworks, improving detection and prevention accuracy, robustness, and reliability by leveraging the strengths of different models. Recent breakthroughs have increasingly focused on embedding ML intelligence into protocol monitoring and enforcement, transforming static defenses into adaptive and proactive prevention [50]. Supervised approaches, such as RFs and SVMs, facilitated the classification of malicious versus legitimate flows. Meanwhile, deep learning models, including CNN-LSTM hybrids, captured both spatial and temporal traffic features for more precise prevention of protocol misuse. More advanced architectures, such as CNNs, LSTMs, VAEs, and GNNs, further enhanced prevention precision and scalability by uncovering subtle anomalies and coordinated multi-vector DDoS or ARP spoofing attacks across distributed IoT and BYOD devices [51]. Reinforcement learning (RL) enhanced systems' ability to autonomously adjust defense strategies like dynamic throttling, traffic rerouting, and ARP validation based on evolving attack conditions. The integration of ensemble methods with supervised, deep, and RL marked a shift from reactive, protocol-centric defenses to intelligent, self-adaptive prevention systems that provide the scalability, adaptability, and accuracy needed to secure modern, heterogeneous campus networks [52].

2.3 ML methods and algorithm used in DDoS and ARP prevention

Supervised machine learning techniques are essential for detecting and preventing DDoS and ARP attacks in campus networks. Models such as SVM, RF, DT, and CNNs were trained on labeled datasets that distinguish normal traffic from malicious traffic [53]. These algorithms effectively identified known attack patterns when large, high-quality datasets were available, making them suitable for diverse campus traffic.

However, their reliance on pre-labeled data limited their ability to detect novel or zero-day attacks, reducing effectiveness against evolving threats [54].

Unsupervised and semi-supervised models have proven to be highly effective for DDoS and ARP detection and prevention in campus networks. Algorithms such as K-means, DBSCAN, and Autoencoders do not require labeled data, making them ideal for identifying unseen anomalies in dynamic traffic [55]. Supervised learning creates a knowledge base from reclassified patterns to classify new patterns, mapping input features to corresponding outputs (classes) and resulting in a model. Semi-supervised approaches, such as VAEs and GNNs, leverage small labeled datasets with larger unlabeled traffic, reducing labeling effort while maintaining accuracy. These methods are well-suited for campus networks, where massive, ever-changing traffic flows complicate manual labeling [56].

RL and adaptive ML models have improved real-time DDoS and ARP prevention in campus networks. RL systems utilize algorithms such as Q-Learning, Deep Q-Networks (DQN), and Policy Gradient methods to learn optimal defense strategies through network interactions [57]. They adjust actions such as traffic throttling or routing in response to attacks. Adaptive models, including online learning and ensemble frameworks with hybrid deep learning, continuously update to counter evolving threats [58]. In complex campus environments with IoT devices, SDNs, and WBANs, these approaches provide flexible, proactive, and self-adjusting security, effectively addressing the limitations of static detection systems [59]. The advancement of ML methods for DDoS and ARP detection and prevention in networks is presented in Fig. 2.

3 Current studies

Recent studies indicate that integrating diverse ML paradigms has significantly strengthened network defense mechanisms in campus environments by enabling timely detection and mitigation of both volumetric and protocol-level attacks. Supervised learning approaches are widely adopted for DDoS and ARP detection due to their strong discriminative capability when sufficient labeled data are available. However, their effectiveness is limited by labeling costs, dataset bias, and reduced adaptability to previously unseen attack patterns [60]. In contrast, unsupervised and semi-supervised methods are better suited for anomaly detection in dynamic campus networks, as they do not rely on labeled datasets and can identify novel or evolving threats, though this often comes at the expense of higher false-positive rates. Deep learning architectures, including CNN, LSTM, and Bi-LSTM models, are particularly effective in capturing spatial and temporal traffic dependencies, but their high computational overhead and limited interpretability pose challenges for real-time deployment and operational trust [61].

Hybrid and ensemble learning frameworks aim to balance these trade-offs by combining multiple ML techniques to enhance robustness and generalization across heterogeneous traffic conditions. Federated learning has emerged as a promising solution for distributed campus and IoT-enabled environments, enabling collaborative model training while preserving data privacy [62]. Nevertheless, it introduces additional communication overhead and assumes the availability of sufficient computational resources at edge devices. RL further extends ML-based security by enabling adaptive and proactive mitigation strategies, particularly when integrated with SDN. However, its training

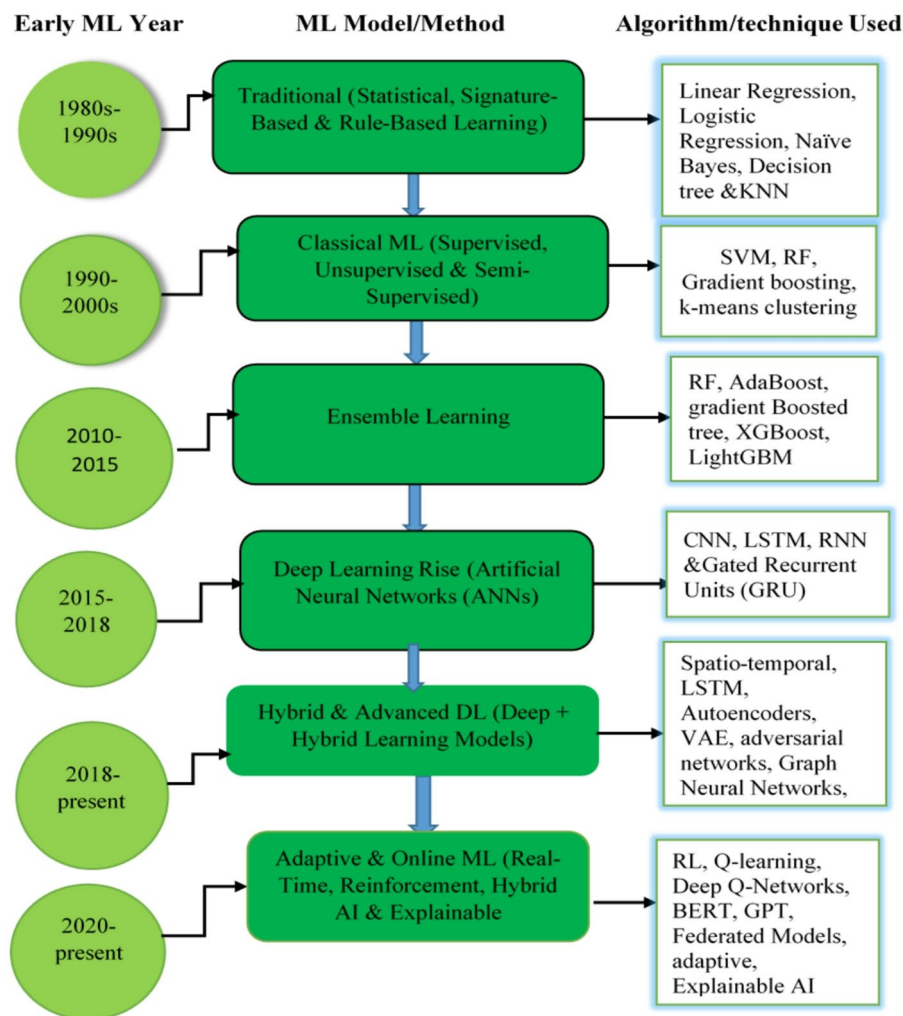


Fig. 2 Evolution of Early Machine Learning Models and Techniques for DDoS and ARP Spoofing Detection and prevention

complexity, convergence latency, and sensitivity to reward design limit its practicality in highly dynamic campus settings [63].

Despite these advances, existing studies primarily evaluate DDoS and ARP attack prevention in isolation, with limited exploration of integrated frameworks capable of addressing both threats simultaneously. Only a few works, such as Chai et al. (2023) and Chatterjee (2025), have demonstrated the feasibility of concurrently mitigating DDoS and ARP attacks by combining flow-level analysis with protocol-specific feature extraction or SDN-assisted multi-layer coordination. DDoS attacks occur at the network and transport layers and are characterized by high-volume, bursty traffic. In contrast, ARP spoofing operates at Layer 2 and involves low-rate manipulations of MAC-IP bindings [64]. These fundamental differences necessitate distinct feature representations, temporal resolutions, and detection logic, complicating unified modeling especially in heterogeneous campus environments with diverse devices, IoT integration, and variable traffic patterns. Despite their potential, existing approaches are hampered by dataset scarcity, challenges in cross-layer feature fusion, and inadequate validation in realistic campus network settings [65].

Integrating DDoS and ARP detection is challenging because it requires multi-layered feature engineering, hybrid learning architectures, and efficient models that can capture both volumetric and protocol-level anomalies in real time. Thus, there is a pressing need for adaptive, explainable, and scalable ML frameworks—such as hierarchical or modular architectures integrated with SDN control planes—that can detect multiple attack types while maintaining low false positives and high responsiveness, thereby enhancing the resilience of campus networks against complex, multi-vector threats.

DDoS attacks have received significant research attention due to their visibility and impact on service disruption, while ARP spoofing is underexplored despite its role in facilitating stealthy man-in-the-middle and traffic redirection attacks. Traditional ARP mitigation strategies, like static ARP binding, VLAN segmentation, Dynamic ARP Inspection, and DHCP snooping, provide baseline protection but face scalability limitations and administrative overhead. Recent research has shifted toward ML-driven ARP detection frameworks that model protocol specific characteristics, such as ARP request reply consistency, MAC-IP binding stability, packet timing irregularities, and anomalous resolution sequences. Temporal deep learning models, particularly LSTM and hybrid CNN-LSTM architectures, have improved detection of subtle Layer 2 anomalies, while SDN assisted frameworks enhance detection accuracy through centralized traffic monitoring and coordinated mitigation. However, ARP focused research is limited by the lack of large-scale, realistic datasets and insufficient campus scale experimental validation. Most studies rely on simulated or constrained datasets, restricting model generalizability and contributing to the disparity between the maturity of DDoS and ARP research. There is a need for realistic Layer 2 datasets, advanced cross-layer feature integration techniques, and scalable ML frameworks capable of detecting volumetric and protocol level attacks within dynamic campus environments.

3.1 Evaluation of ML techniques and metrics used for DDoS and ARP prevention

Several studies have reported the applicability of ML techniques for detecting DDoS and ARP spoofing attacks; however, the reported effectiveness should be interpreted cautiously due to limitations in dataset construction, experimental settings, and contextual relevance to campus networks. Benchmark datasets like CICIDS2017, CICIDS2019, and Kitsune have been useful for evaluating ML-based DDoS and ARP detection frameworks, but they mainly reflect enterprise or simulated IoT traffic under controlled conditions. These datasets do not capture the unique characteristics of real campus networks, such as mixed academic and administrative traffic, high user mobility, BYOD devices, heterogeneous IoT endpoints, and temporal traffic variability. As a result, models validated only on these datasets may lack generalizability in actual campus environments, where dynamic topologies and fluctuating traffic patterns can significantly affect detection performance.

Deep learning architectures, such as Bi-LSTM and GRU, along with traditional classifiers like RF and SVM) [66], are commonly evaluated using benchmark datasets such as CICIDS2017 and CICIDS2019 [67]. These datasets are frequently utilized because they provide labeled traffic, incorporate multiple DDoS attack variants, and reflect typical enterprise-style network services that partially resemble campus environments. Nevertheless, they are generated under controlled laboratory conditions and primarily rely on scripted attack scenarios and predefined traffic profiles, which limits their ability to

capture the heterogeneity, temporal variability, and encrypted traffic increasingly present in real campus networks [68]. Additionally, some protocol distributions and attack signatures within these datasets may not fully align with current network configurations, raising concerns about dataset aging and evaluation bias.

Regarding ARP spoofing detection, studies employing LSTM networks and Decision Tree classifiers on the Kitsune dataset demonstrate that ML-based models can identify anomalous ARP behavior [69]. Kitsune is particularly suited for evaluating lightweight intrusion detection due to its focus on resource-constrained environments and feature efficiency. However, the dataset is derived from simulated IoT traffic operating under constrained and relatively static network conditions, which may not adequately represent the scale, diversity, and dynamic user behavior typical of modern campus infrastructures [70]. As a result, the generalizability of findings derived from Kitsune to real campus deployments remains limited.

Furthermore, Emerging multi-layered ML frameworks aim to integrate ensemble methods, decision trees, and deep learning classifiers to enhance detection across various attack vectors [71]. Despite these methodological advances, most validations depend on synthetic or benchmark datasets rather than real campus traffic. Notably, few studies examine DDoS and ARP spoofing together, leaving campuses without comprehensive tools capable of mitigating both volumetric and link-layer attacks simultaneously [72].

Overall, the literature indicates that ML-based techniques hold significant potential for enhancing the detection and prevention of DDoS and ARP spoofing attacks in campus networks [73]. However, the heavy reliance on benchmark datasets, limited discussion of dataset bias, synthetic traffic generation, and evolving protocol usage highlights the need for more context-aware evaluation strategies [74]. Their effectiveness is currently constrained by dataset limitations, a narrow focus on individual attack types, and a lack of real-world validation. Future research should prioritize integrated DDoS and ARP detection frameworks, contextual evaluation of live campus traffic, cross-domain validation, and adaptive testing strategies to ensure readiness for practical deployment [72]. Accordingly, Table 2 summarizes the ML algorithms applied to DDoS and ARP prevention, emphasizing their methodological characteristics and dataset context rather than reported performance metrics.

3.2 Contextualization of ML techniques in DDoS and ARP prevention

Preventing DDoS and ARP attacks in modern campus networks requires processing high-volume, real-time traffic across heterogeneous devices and dynamic network conditions. These factors critically influence the choice and effectiveness of ML techniques, which must scale efficiently, capture temporal and spatial dependencies, and operate with low latency to ensure timely mitigation [106]. Traditional signature-based intrusion detection systems and firewalls often struggle against multi-vector or zero-day attacks, whereas ML offers a proactive framework that continuously learns from historical and live traffic to distinguish benign from malicious activity [107]. Supervised models, such as RF and SVM, are effective for classifying labeled traffic, while unsupervised approaches—including k-means, DBSCAN, and autoencoders—enable the detection of unknown or evolving threats [27]. Deep learning architectures, such as CNNs, LSTMs, and hybrid CNN-LSTM models, excel at capturing spatial and temporal traffic patterns for precise, near real-time prevention [108]. Reinforcement learning enhances

Table 2 Summary of Various ML Algorithms Used in DDoS and ARP Prevention

Algorithm	Category	Description	Key Features	Benefits	Challenges	Applications
DT [75]	Supervised	Tree-structured model for classification of attack patterns.	Rule-based learning, interpretable.	Easy to interpret, low computational cost.	Overfitting with large datasets.	DDoS traffic classification in campus networks.
RF [76]	Ensemble	Combines multiple decision trees for higher accuracy.	Bagging, feature randomness.	High accuracy, robustness to noise.	Computationally intensive.	DDoS anomaly detection in IoT-enabled labs.
SVM [77]	Supervised	Separates classes using hyperplanes.	Kernel trick, margin maximization.	Effective in high-dimensional spaces.	Slow for large datasets.	ARP spoofing detection in LANs.
KNN [78]	Supervised	Classifies samples based on nearest neighbors.	Distance-based learning.	Simple, non-parametric.	High latency for large data.	DDoS flow classification in academic networks.
Naïve Bayes (NB) [79]	Supervised	Probabilistic classifier based on Bayes' theorem.	Fast, probabilistic inference.	Handles noisy data.	Assumes feature independence.	ARP poisoning attack prediction.
Logistic Regression (LR)	Supervised	Regression-based binary classification.	Linear decision boundaries.	Fast, interpretable.	Poor with nonlinear data.	DDoS binary classification in campus traffic.
Artificial Neural Network ANN [80]	Supervised	Mimics biological neurons for classification.	Hidden layers, activation functions.	Captures complex patterns.	Requires large datasets.	Multi-class DDoS detection in hybrid networks.
DNN [81]	DL	Multi-layer neural architecture for feature learning.	Deep hierarchies, nonlinear modeling.	High accuracy, adaptability.	Computationally expensive.	DDoS and ARP integrated detection systems.
CNN [82]	DL	Extracts spatial-temporal traffic features.	Convolutional filters, pooling.	Efficient feature extraction.	Needs labeled data.	Packet-level anomaly detection.
RNN [83]	DL	Sequential model for temporal data.	Memory of past states.	Effective for time-series.	Vanishing gradient issues.	DDoS trend prediction in campus traffic.
LSTM [84]	DL	Variant of RNN solving long-term dependency.	Gates for information control.	Handles sequential data.	High training time.	Time-series DDoS traffic analysis.
GBM [85]	Ensemble	Sequential ensemble of weak learners.	Boosting technique.	High predictive power.	Risk of over fitting.	Feature-based DDoS classification.
XGBoost [86]	Ensemble	Optimized GBM for faster execution.	Regularization, parallelism.	High speed and accuracy.	Parameter tuning complexity.	ARP and DDoS hybrid detection.
AdaBoost [87]	Ensemble	Weighted combination of weak learners.	Adaptive weighting.	Improves weak learners.	Sensitive to noise.	Detecting spoofed ARP responses.
LightGBM [88]	Ensemble	Gradient boosting optimized for large data.	Histogram-based learning.	Fast training, scalability.	May overfit small data.	Real-time DDoS detection.

Table 2 (continued)

Algorithm	Category	Description	Key Features	Benefits	Challenges	Applications
Autoencoder [89]	DL	Learns compressed data representations.	Encoder-decoder structure.	Effective unsupervised learning.	Sensitive to noise.	ARP anomaly detection in LANs.
Gaussian Mixture Model (GMM) [90]	Unsupervised	Models data as Gaussian distributions.	Probabilistic clustering.	Handles uncertainty well.	Assumes Gaussian nature.	Network traffic clustering.
K-Means [91]	Unsupervised	Clusters data by minimizing intra-cluster variance.	Centroid-based learning.	Simple, fast.	Requires pre-defined k.	Unsupervised DDoS anomaly detection.
DBSCAN [92]	Unsupervised	Density-based clustering for outlier detection.	Density threshold.	Finds arbitrary clusters.	Sensitive to parameters.	ARP spoofing outlier detection.
PCA [93]	Dimensionality Reduction	Transforms data to principal components.	Variance maximization.	Reduces complexity.	Loses interpretability.	Feature reduction for DDoS detection.
RL [94]	Adaptive	Learns optimal actions via rewards.	Exploration vs. exploitation.	Adaptive decision-making.	Slow convergence.	Adaptive ARP prevention.
DQN [95]	RL	Deep learning with Q-learning.	Action-value function.	Real-time adaptability.	Complex implementation.	Self-learning DDoS mitigation.
ELM [96]	Supervised	Single-layer neural network.	Random weights, fast learning.	Rapid training.	Low interpretability.	DDoS traffic recognition.
Genetic Algorithm (GA) [97]	Optimization	Evolutionary search optimization.	Mutation, crossover.	Good global search.	Computationally expensive.	Feature optimization in DDoS models.
Hybrid CNN-LSTM [98]	DL	Combines CNN feature extraction with LSTM sequence modeling.	Spatio-temporal learning.	High detection accuracy.	Heavy training cost.	Joint DDoS-ARP detection.
CNN-GRU Hybrid [99]	DL	Combines CNN spatial and GRU temporal layers.	Sequence feature extraction.	Handles traffic dynamics.	High resource demand.	Dynamic DDoS detection.
Semi-Supervised Learning [100]	Hybrid	Learns from few labels + unlabeled data.	Self-training.	Reduces labeling cost.	Sensitive to noisy labels.	ARP spoofing in unlabeled data environments.
Deep Auto-encoder-LSTM [101]	DL	Combines feature compression and sequence learning.	Reconstruction error-based detection.	Detects zero-day attacks.	Long training time.	Integrated DDoS-ARP defense.
GNN [102]	DL	Learns from graph-structured data.	Node and edge embeddings.	Captures network topology.	High computation demand.	Network-level intrusion detection.
Transformer Model [103]	DL	Attention-based sequential model.	Self-attention layers.	Handles long dependencies.	Requires large datasets.	Real-time DDoS detection.

Table 2 (continued)

Algorithm	Category	Description	Key Features	Benefits	Challenges	Applications
Federated Learning [104]	Distributed ML	Trains models across decentralized devices.	Privacy-preserving learning.	Protects data privacy.	Communication overhead.	Collaborative ARP prevention in IoT labs.
DRL [105]	Adaptive	Combines deep learning and RL for adaptive defense.	Policy optimization.	Autonomous attack mitigation.	High complexity, resource heavy.	Self-learning DDoS-ARP prevention framework.

adaptability by enabling dynamic mitigation strategies, including traffic rerouting, rate limiting, or SDN-assisted control, in response to evolving attack behaviors [109].

ARP spoofing detection in campus IoT networks is complex due to Layer 2 protocol characteristics and network dynamics. Deviations in IP–MAC mappings, broadcast traffic, device mobility, and DHCP turnover present challenges for ML models. Existing ARP datasets often lack the diversity of real campus traffic, limiting model robustness, while dense broadcast domains, mixed topologies, VLAN segmentation, and network virtualization complicate anomaly differentiation. Incorporating protocol-aware features, such as IP–MAC binding stability, along with temporal and context-aware modeling, can improve detection accuracy and reduce false positives. Addressing these campus-specific dynamics is essential for developing reliable and generalizable ML frameworks for ARP spoofing mitigation.

However, deploying ML-based defenses in campus environments is limited by hardware constraints and emerging adversarial threats that manipulate input data to evade detection or degrade model performance. Real-time implementation is challenging because network switches and routers typically have limited processing capacity, memory buffers, and forwarding rates, which restrict the complexity of ML models executable at the network edge [110]. Throughput requirements during peak conditions often exceed hundreds of thousands of packets per second, while latency demands decision-making within milliseconds to prevent service disruption [111]. To address these challenges, lightweight or modular ML models, selective feature extraction, and hardware acceleration using GPUs or edge computing platforms are essential. Hybrid frameworks that distribute anomaly detection between edge devices and centralized controllers, along with SDN-based traffic orchestration, enable scalable, low-latency, and accurate DDoS and ARP prevention while respecting the computational limitations of campus network equipment [112]. Integrating adversarial defense mechanisms such as adversarial training, robust feature engineering, ensemble learning, and continuous model validation enhances resilience against evasion and poisoning attacks. Additionally, incorporating lightweight model optimization and distributed edge-cloud processing ensures computational efficiency without compromising detection accuracy. This combination supports secure, scalable, and adaptive ML-driven intrusion detection in resource-constrained campus network environments. Figure 3 summarizes the ML techniques applied in these environments, highlighting their suitability for real-time, resource-constrained deployment.

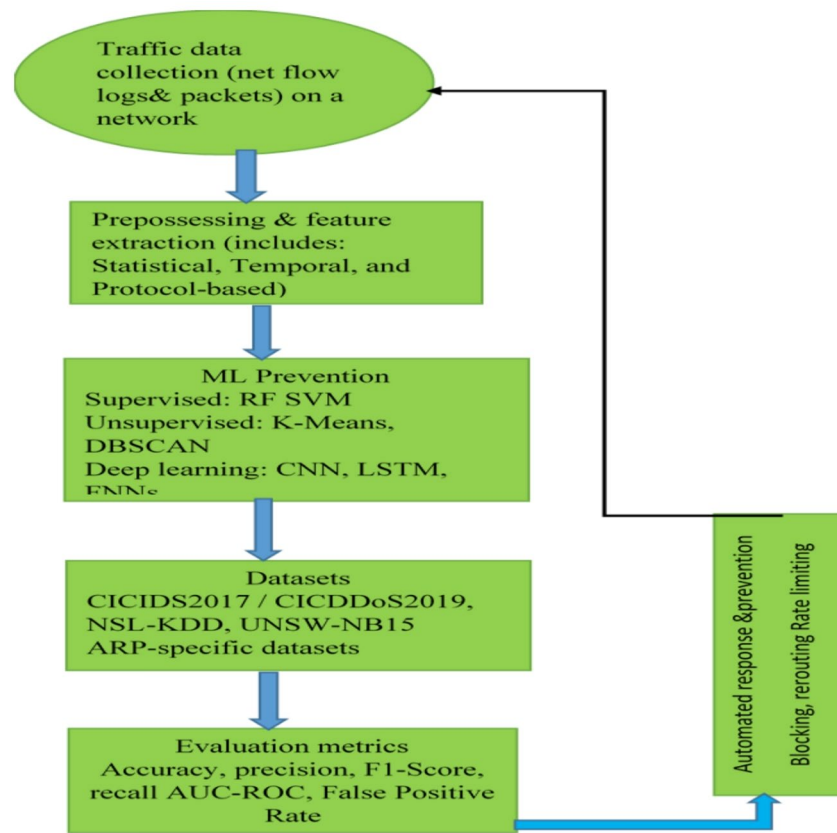


Fig. 3 ML techniques in DDoS and ARP prevention

4 Methodology

In this section, we outline our review methodology, employing the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework for selecting research papers. Following the guidelines established by Trifu et al. (2022), we conducted a manual revision process to screen the automatically selected publications, excluding those outside the study's scope. The final dataset includes 110 publications, ensuring the systematic inclusion of relevant studies.

4.1 Inclusion and exclusion criteria

This research explores the application of emerging technologies. Inclusion and exclusion criteria were established to focus on relevant studies analyzing DDoS and ARP prevention on campus networks using ML. The review included publications that addressed the use of ML for preventing DDoS and ARP attacks within university networks, SDN, IoT, and WBANs. Studies were selected based on their focus on network security challenges related to DDoS and ARP threats, empirical validation, and the scalability of ML techniques in campus environments. Papers lacking empirical evaluation or outside the realms of academic research, IoT, SDN, and WBANs were excluded. This selection ensured the review focused on state-of-the-art ML approaches for securing campus network thus detecting and preventing DDoS and ARP attacks.

A. Selection of keywords

A literature search was conducted in major academic databases, including Springer, IEEE, Elsevier, Science Direct, Research Gate, Google Scholar, and arXiv, to identify relevant studies. The search used keywords and Boolean operators related to ML, deep learning, intrusion detection, network security, DDoS, and ARP spoofing. Context-specific keywords like campus network, university network security, SDN, IoT, and WBAN were included to focus on academic environments. This strategy ensured the retrieval of studies on the application of ML techniques for detecting and preventing DDoS and ARP-based attacks in campus and smart network infrastructures.

A. Inclusion

Eligible papers were selected based on their relevance to machine learning techniques for preventing DDoS and ARP attacks in campus networks. The focus was on studies exploring emerging technologies, including IoT, SDN, and WBAN. Only peer reviewed journal articles, conference papers, and high-quality preprints in English were included if they provided empirical or experimental results demonstrating model performance using metrics such as accuracy, precision, F1 score, detection rate, or false positive rate. This framework ensured that all selected studies presented relevant, validated, and reproducible findings that contribute to understanding machine learning-based network security detection and prevention in academic and campus infrastructures.

I. Exclusion

Studies were excluded if they did not involve ML or deep learning techniques for securing campus networks, preventing DDoS or ARP attacks, lacked empirical validation, or focused solely on traditional detection methods. Papers unrelated to campus, IoT, SDN, or WBAN network environments, as well as those not written in English, were also omitted. Additionally, review papers, opinion articles, and studies lacking methodological detail or performance metrics were excluded to ensure the quality and relevance of the selected literature.

5 Research quality evaluation and data extraction

Given the increasing volume of research on ML applications for securing campus networks, including intrusion detection and prevention of DDoS and ARP attacks, we evaluated the selected studies using the PRISMA checklist. Two independent reviewers screened all titles, abstracts, and full-text articles. Inter-reviewer agreement was assessed using Cohen's kappa ($\kappa=0.88$), with discrepancies resolved through discussion and consensus with a third reviewer. Each study was critically evaluated for methodological quality, considering criteria such as dataset relevance, experimental design, empirical validation, performance metrics, and reproducibility. Studies that did not meet minimum quality thresholds, lacked a focus on ML or deep learning, or fell outside the scope of campus, IoT, SDN, or WBAN network environments were excluded. This approach ensured the inclusion of only high-quality, methodologically sound studies. The PRISMA framework facilitated a thorough evaluation of each paper, emphasizing the applicability of ML algorithms and novel techniques for intrusion detection and prevention in campus network environments.

As shown in Fig. 4, the literature search identified 206 articles from major academic databases, including Springer, IEEE, Elsevier, Research Gate, Science Direct, Google Scholar, and arXiv. During the screening process, 58 duplicate articles were removed. Subsequently, 11 articles were excluded for lacking a clear ML focus, and 10 articles were omitted due to the absence of empirical validation. Additionally, 17 studies were excluded for falling outside the scope of campus, IoT, SDN, or WBAN network contexts. After applying all criteria, a total of 110 studies were retained for full review and analysis.

Figure 5 illustrates the yearly distribution of studies included in the review for the period 2020–2025. A total of 110 research papers published between 2020 and 2025 were selected based on the established inclusion criteria. The distribution of these studies indicates the number of papers identified from each year: 14 in 2020, 10 in 2021, 19 in 2022, 16 in 2023, 23 in 2024, and 28 in 2025.

6 Recent Innovations in ML for DDoS and ARP prevention on campus network

Recent innovations in ML have significantly advanced the detection and prevention of DDoS and ARP spoofing attacks in campus networks, particularly under resource-constrained and real-time conditions. Lightweight ML models designed for IoT and edge environments employ feature selection techniques, such as Extremely Randomized Trees (Extra Trees Classifier), to reduce dimensionality and computational overhead

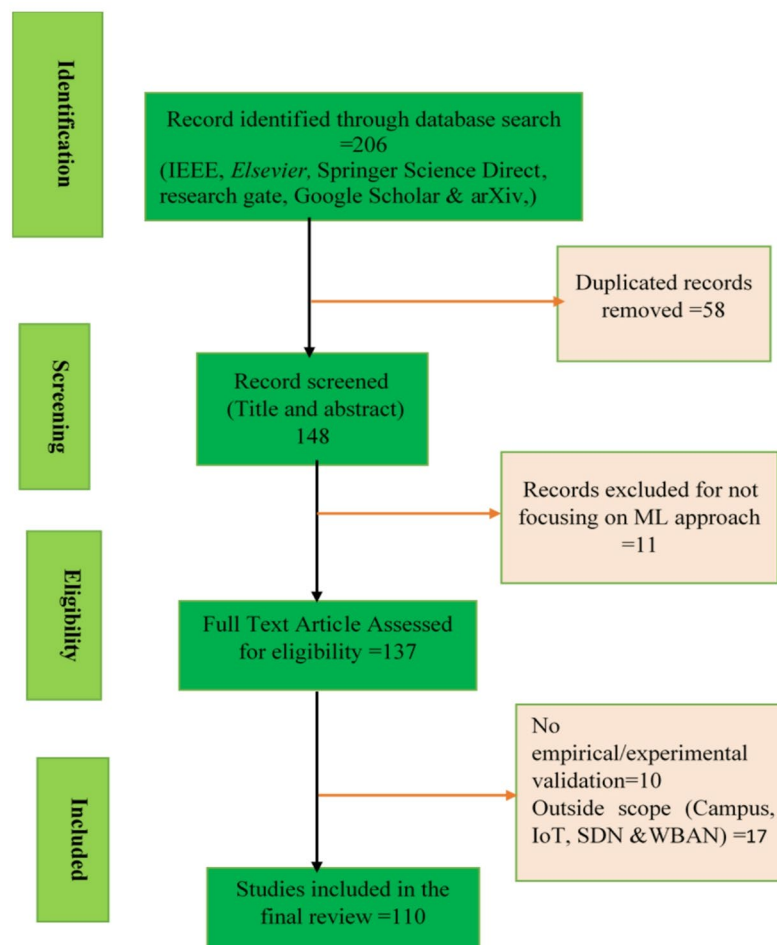


Fig. 4 The PRISMA-based process adopted for the review

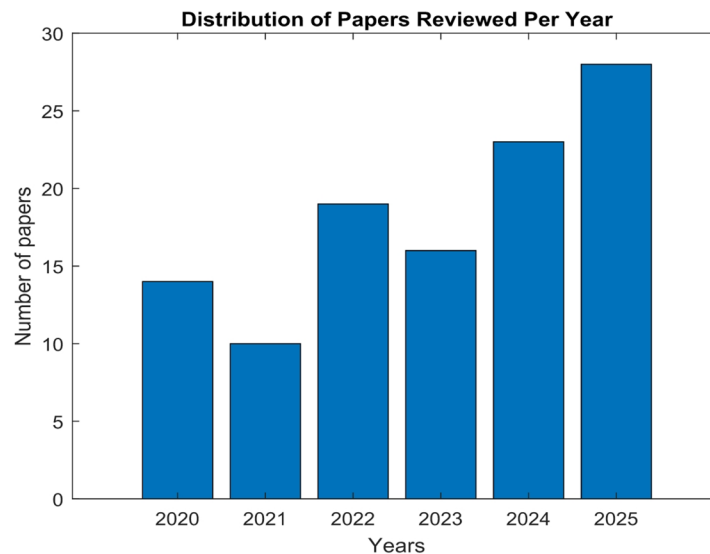


Fig. 5 A bar graph showing Yearly Distribution of Studies Included in the Review (2020–2025)

while maintaining effective detection capabilities [113]. Hybrid deep learning architectures that combine CNNs with LSTM networks further enhance performance by jointly modeling spatial traffic features and temporal dependencies, making them suitable for identifying complex and evolving attack patterns [114]. For ARP spoofing prevention, ML-based detection has been integrated into SDN architectures through multi-layered frameworks that combine lightweight edge-level classifiers with centralized ensemble-based mitigation modules [71]. These approaches exploit ARP-specific protocol dynamics and traffic behavior to enable timely detection and coordinated responses across campus infrastructures [115]. Frameworks such as MULTI-LF demonstrate the feasibility of achieving low latency and robust classification in multi-attack scenarios, highlighting the potential of ML-driven security mechanisms for proactive campus network defense.

However, despite these advances, existing ML-based intrusion detection and prevention systems remain vulnerable to adversarial machine learning threats, which are largely underexplored in current campus-focused studies. Adversarial examples can be crafted to evade trained models by subtly manipulating traffic features, while model poisoning attacks can degrade detection performance by injecting malicious samples during training or model updates. Additionally, evasion attacks that exploit model assumptions or feature dependencies pose a significant risk in real-world deployments. Addressing these challenges requires incorporating adversarial-aware training, robust feature engineering, ensemble diversity, and continuous model validation [116]. Promising solutions include adversarial training, anomaly-based pre-filters, federated learning with secure aggregation, and explainable ML mechanisms that enhance trust and resilience. The deployment of computationally intensive ML models, such as CNN–LSTM hybrids, in campus network environments is often limited by legacy infrastructure and resource constrained IoT devices. These challenges can be addressed through lightweight optimization techniques, including model pruning, quantization, and knowledge distillation, which help reduce computational complexity, memory usage, and energy consumption while maintaining detection performance. Additionally, edge cloud collaborative architectures

facilitate efficient task distribution by enabling lightweight anomaly detection at local or edge nodes, while offloading complex analytics to centralized servers. When integrated into SDN-enabled modular ML frameworks, these strategies enhance scalability, reduce latency, and support real-time, adaptive, and resilient detection of DDoS and ARP spoofing attacks in resource-constrained campus network environments, as summarized in Fig. 6.

6.1 Analysis of emerging ML algorithms and techniques

Recent Research and advances in ML have led to the development of hybrid algorithms and deployment methodologies that significantly enhance the detection and prevention of DDoS and ARP spoofing attacks in complex campus network environments [117]. Traditional rule-based intrusion detection systems struggle to cope with the high traffic volume, temporal variability, and device heterogeneity characteristic of academic networks. In contrast, modern ML techniques-including LSTM, CNNs, and gradient boosting methods like XGBoost-can model non-linear traffic behavior and temporal dependencies, enabling accurate identification of subtle anomalies under fluctuating load conditions [118]. Ensemble learning frameworks that combine shallow classifiers with deep models further enhance robustness and generalization, particularly against evolving or adversarial attack patterns that commonly bypass single-model systems [119].

Emerging methodologies increasingly embed ML models within SDN, edge computing, and federated learning architectures to address scalability, latency, and data privacy constraints in campus deployments. Edge-based ML facilitates early-stage detection of DDoS floods and ARP anomalies near the data source, reducing response latency and minimizing core network overload [120, 121]. Meanwhile, SDN controllers provide centralized visibility to coordinate mitigation actions such as traffic rerouting, rate limiting, and port isolation [122]. Federated learning complements this architecture by allowing multiple campus edge nodes or subnetworks to collaboratively train detection models without sharing raw traffic data, thereby preserving privacy and accommodating institution-specific traffic characteristics [123].

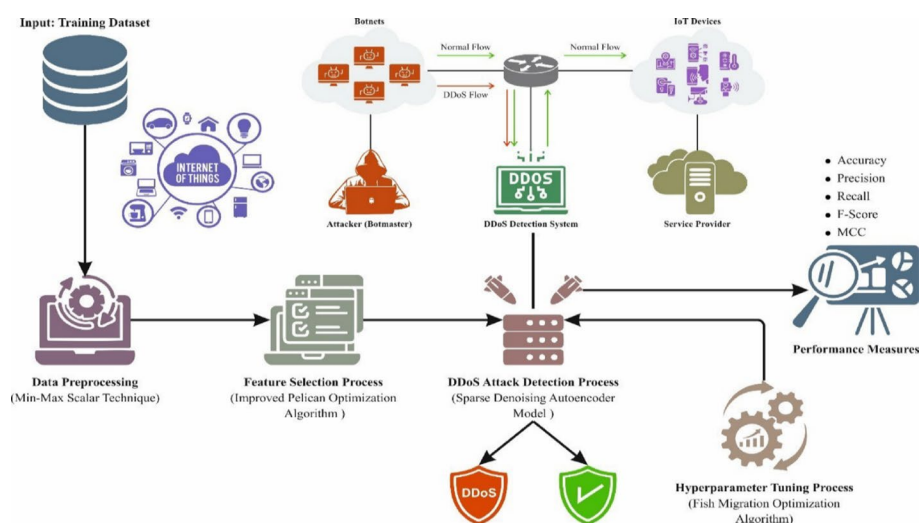


Fig. 6 Recent Machine Learning Innovations for DDoS and ARP Attack Prevention

This distributed learning paradigm is particularly relevant for ARP spoofing detection, where localized Layer-2 behaviors vary across network segments. Semi-supervised and reinforcement learning techniques enhance adaptability by enabling models to learn from limited labeled data and continuously refine defense strategies based on real-time feedback [124]. Deep reinforcement learning, when integrated with SDN control loops, supports proactive mitigation decisions under dynamic attack conditions, while explainable AI improves operational trust by providing interpretable insights into detection outcomes. Collectively, these algorithmic and architectural innovations form a scalable, privacy-aware, and adaptive solution for unified DDoS and ARP prevention in campus networks, as summarized in Table 3.

The reviewed algorithms and methodologies demonstrate that hybrid and ensemble-based models, such as CNN–LSTM and XGBoost, offer superior detection accuracy and adaptability compared to traditional single-model approaches. Unsupervised and reinforcement learning techniques have introduced intelligent, self-learning capabilities that enable real-time anomaly detection and proactive mitigation of evolving network threats [133]. Lightweight models, like the Extra Trees Classifier, and federated learning frameworks further enhance scalability and privacy preservation across distributed campus

Table 3 Summary of Novel Algorithms and Methodologies for DDoS and ARP Prevention

Algorithm/Methodology	Research Methodology	Application (DDoS and ARP)	Key Findings
CNN–LSTM Hybrid Model [125]	Deep learning combining convolutional and recurrent networks for sequential data analysis.	Used to detect and classify DDoS traffic patterns and ARP spoofing behaviors in IoT-based campus networks.	Achieved 97.89% detection accuracy with low false-positive rates and strong adaptability to dynamic attacks.
ETC with Feature Pruning [126]	Ensemble learning with optimized feature selection to enhance model efficiency.	Applied to lightweight DDoS detection in campus and WLAN IoT environments.	Reduced processing latency and maintained > 97% accuracy; effective for real-time detection.
Autoencoder-Based Deep Anomaly Detection [127]	Unsupervised learning to reconstruct normal traffic and identify deviations.	Used for early detection of DDoS and ARP spoofing attacks without labeled datasets.	Demonstrated high accuracy for zero-day attack detection and adaptive model performance.
Random Forest with Adaptive Thresholding [128]	Supervised ensemble method combining decision trees with adaptive threshold tuning.	Designed for mixed-traffic analysis in ARP spoofing and DDoS mitigation systems.	Achieved 0.5% false alarm rate, improving robustness in high-traffic campus networks.
SVM with RBF Kernel [129]	Supervised classification focusing on separating normal and malicious traffic patterns.	Used to classify ARP anomalies and detect DDoS traffic bursts.	Provided reliable detection for small to medium-scale campus networks with limited datasets.
XGBoost + Decision Tree Ensemble [130]	Hybrid ensemble learning integrating gradient boosting and tree-based classifiers.	Applied to DDoS and ARP detection in SDN-based campus networks.	Improved precision and recall by 5–8% compared to individual classifiers.
RL-IPS [131]	Adaptive ML approach that learns optimal mitigation policies through feedback loops.	Applied in dynamic DDoS and ARP prevention systems for campus networks.	Reduced response time by 30% and enhanced resilience to evolving attack vectors.
Federated Learning Framework [132]	Distributed ML allowing collaborative model training across multiple nodes.	Used for privacy-preserving DDoS and ARP detection in multi-campus environments.	Achieved scalable detection with high privacy protection and resistance to adversarial manipulation.

infrastructures [134]. Cooperatively, these innovations indicate a clear trend toward more adaptive, efficient, and autonomous ML-driven security systems capable of safeguarding modern campus networks against complex DDoS and ARP attacks.

6.2 Empirical data

Empirical evidence from the reviewed literature demonstrates that ML techniques effectively enhance the detection and prevention of both DDoS and ARP spoofing attacks in campus networks. This effectiveness is largely due to their ability to model high-volume, real-time, and dynamically evolving traffic patterns. DDoS detection predominantly relies on flow-level analysis at the network and transport layers (L3/L4), where features such as packet rate, flow duration, byte counts, entropy measures, and connection frequency enable the identification of volumetric and protocol-based flooding behaviors. Ensemble learning approaches, including RF and Extra Trees, are frequently adopted for DDoS mitigation because of their robustness to feature noise and their capacity to operate efficiently under large-scale traffic aggregation.

While DDoS prevention has garnered significant attention in the literature, mitigating ARP spoofing necessitates specialized detection mechanisms due to its low-rate and protocol-manipulation characteristics. Recent studies increasingly emphasize ARP specific behavioral modeling and cross-layer validation techniques. In contrast to DDoS attacks, ARP spoofing detection presents unique challenges because it operates at the data link layer (Layer 2), where attacks typically manifest through subtle temporal and behavioral deviations rather than high volume traffic anomalies. Consequently, ARP focused studies highlight protocol specific features such as ARP request reply consistency, MAC-IP binding stability, packet inter arrival times, and anomalous address resolution sequences. Although these features have limited relevance in DDoS detection, they are essential for distinguishing malicious ARP behavior.

Deep learning models, particularly LSTM-based and hybrid CNN-LSTM architectures, have shown promise in addressing these Layer 2 challenges by capturing both short-term packet dependencies and longer-term behavioral patterns associated with ARP poisoning. These temporal models are well-suited to campus environments characterized by device heterogeneity, frequent topology changes, and intermittent communication patterns. However, unlike DDoS detection-which benefits from multiple large-scale benchmark datasets-ARP spoofing research remains constrained by limited dataset availability. Existing evaluations often rely on datasets such as Kitsune or small-scale simulated traffic, which, while useful for validating lightweight detection mechanisms, do not fully reflect the diversity and scale of real campus networks. This dataset scarcity restricts cross-dataset validation and limits the generalizability of reported results.

Emerging adaptive approaches, including reinforcement learning, federated learning, and hybrid ML frameworks, offer promising directions for jointly addressing DDoS and ARP threats by enabling proactive, distributed, and privacy-preserving intrusion prevention. When integrated with SDN architectures, these models support real-time monitoring and dynamic mitigation across both Layer 2 and Layer 3/4 attack surfaces. Nevertheless, the literature reveals an imbalance in experimental depth, with ARP spoofing often receiving comparatively limited evaluation. This highlights the need for future research to develop ARP specific datasets, incorporate Layer 2 feature engineering, and

conduct realistic campus scale validations. Table 4 summarizes ML-driven prevention strategies for DDoS and ARP attacks, emphasizing methodological distinctions, protocol-layer considerations, and dataset limitations rather than isolated performance claims.

A. Overview of Datasets Used

The effectiveness of machine learning techniques for DDoS and ARP prevention highly depends on the datasets used for their development, training, and evaluation. The empirical evaluation of these techniques on campus networks relies on a variety of well-established and context-specific datasets that reflect real-world traffic patterns and attack scenarios. DDoS and ARP datasets, designed to mirror real-world conditions and challenges, provide a critical foundation for these methods. Below is a breakdown of the datasets commonly applied in the reviewed studies.

The CICIDS2017 dataset offers labeled flow-based features for HTTP, ICMP, and TCP flood attacks, allowing supervised ML models to differentiate between normal and malicious traffic. Its realistic traffic patterns and variety of attack types have established it as a standard benchmark for evaluating DDoS detection models in dynamic environments like campus networks. The CICIDS2019 dataset builds on this by incorporating modern multi-vector DDoS scenarios and high-volume traffic, which supports the development of adaptive and real-time machine learning-based intrusion detection systems. Both datasets facilitate the training, validation, and benchmarking of supervised algorithms, but they come with limitations: their reliance on historical attack patterns, potential class imbalances, and controlled traffic environments can result in near-perfect reported accuracies that may not generalize to live campus networks.

The Kitsune dataset allows for packet-level analysis of ARP spoofing and IoT anomalies, supporting both supervised and unsupervised learning. While it is useful for detecting known and emerging ARP attacks, its simulated IoT traffic and constrained network conditions may not fully reflect the diversity, device heterogeneity, and temporal variability of real campus networks. Likewise, simulated campus and IoT network datasets replicate high volume, heterogeneous traffic in controlled settings, enabling robust experimentation with adaptive and unsupervised machine learning models. However, they share the limitation of potential synthetic bias and restricted real-world representativeness.

Together, these datasets provide crucial resources for developing ML techniques for DDoS and ARP prevention, but their near-perfect detection results should be interpreted with caution. Future research should incorporate cross-dataset validation, real campus traffic traces, and strategies to mitigate class imbalance and overfitting to ensure that machine learning models remain robust, generalizable, and operationally reliable in live, heterogeneous campus network environments.

A. Performance metrics

Performance metrics are essential for evaluating the effectiveness of ML techniques in preventing DDoS and ARP attacks on campus networks. They provide a standardized way to assess how accurately and efficiently models detect and classify network anomalies.

Table 4 Summary of ML Techniques for DDoS and ARP Prevention on Campus Networks

Technique/Algorithm	Type of Attack (DDoS/ARP)	Research Methodology/Application	Key Empirical Findings
RF [119]	DDoS & ARP spoofing	Supervised ensemble classifier on labeled datasets; used in campus network traffic analysis	Achieved 99.99% accuracy, precision, recall, and F1-score; robust for large-scale networks; outperforms Naïve Bayes, k-NN, SVM
ETC with Feature Pruning [120]	DDoS	Lightweight ensemble ML with optimized feature selection; suitable for IoT/WLAN campus environments	> 97% accuracy; reduced processing latency; effective for real-time detection
CNN-LSTM Hybrid Model [121]	DDoS & ARP spoofing	Deep learning combining convolutional and recurrent networks for sequential traffic analysis	98.69% accuracy and 98.66% F1-score; captures spatial and temporal patterns; effective against multi-vector attacks
Bi-LSTM [122]	DDoS	Deep recurrent network on CICIDS2017 dataset; volumetric and protocol-based attack detection	99.76% accuracy, 98.90% precision; very low false positive rate (0.053%); effective in dynamic campus traffic
DT [123]	ARP spoofing	Supervised classifier on ARP traffic dataset (e.g., Kitsune dataset)	Up to 100% detection accuracy; minimal false positives; effective in real-time prevention
Autoencoder-Based Deep Anomaly Detection [124]	DDoS & ARP	Unsupervised deep learning; reconstructs normal traffic to detect anomalies	High accuracy for zero-day attack detection; adaptive to dynamic traffic without labeled data
Hybrid ML Models (Ensemble + Deep Learning) [125]	DDoS & ARP spoofing	Combination of multiple ML and DL models; supervised/unsupervised	Improved accuracy, robustness, and adaptability against evolving attacks; effective in SDN and IoT networks
Reinforcement Learning (RL-IPS, Deep RL) [125]	DDoS & ARP spoofing	Adaptive learning to optimize mitigation policies in real-time campus networks	Reduces response time by ~30%; self-optimizing defense; dynamic traffic throttling and rerouting
Federated Learning Framework [126]	DDoS & ARP spoofing	Distributed ML across multiple campus nodes; privacy-preserving	Scalable collaborative detection; high privacy protection; resilient to adversarial attacks

Table 4 (continued)

Technique/Algorithm	Type of Attack (DDoS/ARP)	Research Methodology/Application	Key Empirical Findings
XGBoost+ Decision Tree Ensemble [127]	DDoS & ARP spoofing	Hybrid gradient boosting and tree-based ensemble; applied in SDN campus networks	Precision and recall improved by 5–8% over single classifiers; suitable for real-time SDN-based prevention

Table 5 Summary of some ML techniques used in DDoS & ARP prevention

Technique	Ac- cu- racy (%)	Pre- ci- sion (%)	Re- call (%)	F1 Score (%)	Compu- tation Time (ms)	Scalability
RF [138]	99.99	99.90	99.87	99.88	2.8	High: efficient for large-scale datasets
SVM [139]	97.60	96.80	95.40	96.10	6.2	Moderate: limited for very large datasets
KNN [140]	95.40	94.20	93.60	93.90	8.5	Low: performance drops with data volume
DT [141]	98.70	98.10	97.80	97.90	3.6	High: suitable for real-time detection
XGBoost) [142]	99.20	98.80	98.60	98.70	4.5	High: scalable and robust in SDN/IoT
CNN [143]	98.90	98.50	98.10	98.30	5.7	High: effective with GPU acceleration
LSTM) [144, 145]	99.10	98.70	98.60	98.65	6.4	High: excellent for temporal traffic data
Autoencoder (Unsu- pervised) [146]	97.80	97.30	96.90	97.00	3.9	High: adaptable for zero-day anomaly detection
Reinforcement Learn- ing (RL) [147]	98.50	98.10	97.70	97.80	5.3	Very High: adaptive in dynamic environments
FL [148]	97.90	97.40	97.00	97.10	7.2	Very High : scalable across distributed nodes

[135]. Frequently used metrics include accuracy, precision, recall, and the F1-score, which measure the predictive performance of ML algorithms. Accuracy indicates the overall correctness of predictions, while precision measures the proportion of true attack detections among all identified attacks, thereby reducing false positives [136]. Recall reflects a model's ability to identify actual attacks, minimizing false negatives, while the F1-score balances precision and recall. Additionally, computation time and scalability are crucial for evaluating the suitability of ML models in real-time network environments, ensuring responsiveness to varying traffic loads. Other evaluation measures, such as Receiver Operating Characteristic (ROC) curves, Area under the Curve (AUC), and confusion matrices, provide insights into model behavior and classification trade-offs [137].

These performance metrics form the foundation for comparing and optimizing ML-based intrusion detection systems, allowing researchers to identify models that deliver high detection accuracy and operational efficiency in dynamic campus network settings, as presented in Table 5.

Implementing ML techniques allows network engineers to enhance campus network security by proactively detecting and preventing DDoS and ARP attacks. These systems identify anomalous traffic patterns for rapid response and mitigation before disruptions occur. Integrating performance metrics ensures ongoing evaluation and optimization of detection accuracy and efficiency. This enables effective preventive maintenance, minimizes downtime, and maintains seamless connectivity, resulting in improved service reliability, higher user satisfaction, and reduced operational costs.

I. Integration of ML Techniques and Performance Metrics

The integration of ML techniques with performance metrics is essential for advancing network security systems, particularly in detecting and preventing DDoS and ARP attacks in campus networks. This integration creates a framework that aligns algorithm design with measurable performance outcomes, ensuring model development addresses predictive accuracy and operational efficiency. By combining ML algorithms such as RF, SVM, DT, and DNN with evaluation metrics like accuracy, precision, recall, F1-score, computation time, and scalability, researchers can assess model performance across multiple dimensions. This approach enhances the interpretability, reliability, and reproducibility of findings while facilitating continuous model refinement based on real-world dynamics. It also identifies trade-offs between detection accuracy and resource utilization, ensuring deployed models are effective and computationally efficient. Ultimately, the synergy between ML techniques and performance metrics bridges the gap between theoretical development and practical implementation, guiding the creation of data-driven, scalable, and performance optimized intrusion detection and prevention systems for complex campus networks.

I. Challenges and limitations

ML techniques have strong potential to enhance the prevention of DDoS and ARP spoofing attacks in campus networks. However, several challenges limit their practical deployment. The dynamic and heterogeneous nature of academic environments—marked by frequent device turnover, diverse user behaviors, and fluctuating traffic patterns—complicates accurate anomaly modeling and increases the risk of false positives. Many ML models depend on large, high-quality labeled datasets, yet real-world campus traffic datasets are often scarce, imbalanced, privacy-sensitive, or outdated, which constrains model generalization and robustness.

Deployment is further complicated by computational complexity, as deep learning and hybrid models require substantial processing and memory resources that are difficult to support on legacy campus switches, routers, and resource constrained IoT or SDN edge devices. Privacy concerns stemming from packet-level inspection, particularly for ARP analysis, introduce regulatory and ethical constraints. Furthermore, scalability requirements for large student populations impose strict throughput and latency demands. Cost limitations common in academic institutions also restrict the adoption of specialized hardware or large-scale centralized processing infrastructures.

The limited adaptability of models trained on historical data to zero-day attacks, along with the lack of interpretability in complex deep learning or reinforcement learning systems, further undermines operational trust and hinders actionable decision-making. Addressing these challenges necessitates a holistic solution that combines lightweight, modular ML architectures, privacy-preserving feature extraction, adaptive and continual learning mechanisms, and SDN-assisted orchestration to ensure interoperability with legacy hardware, cost-efficient scalability, and real-time responsiveness. Moreover, standardized evaluation frameworks and longitudinal campus-scale deployment studies are essential to validate performance and support the reliable integration of ML-based security solutions into operational campus networks.

7 Conclusion

The literature shows that ML techniques are transforming the detection and prevention of DDoS and ARP spoofing attacks in campus networks. Compared to traditional signature and rule-based IDS, supervised, unsupervised, and hybrid ML approaches are more adaptable and effective in identifying complex malicious traffic patterns. Empirical studies indicate that ensemble deep learning models and reinforcement learning strategies improve detection accuracy, reduce false positive rates, and enable near real-time threat responses. Advanced architectures, such as CNN–LSTM hybrids, Bi-LSTM networks, and federated learning frameworks, effectively capture both spatial and temporal traffic dependencies, facilitating adaptive anomaly detection and automated mitigation of multi-vector attacks.

However, there is an uneven emphasis between DDoS and ARP spoofing mitigation strategies. While DDoS prevention has been extensively studied across various traffic layers and datasets like CICIDS2017 and CICIDS2019, ARP spoofing remains underexplored despite its role in man-in-the-middle attacks. Unlike volumetric DDoS attacks that generate high-rate traffic anomalies, ARP spoofing exploits vulnerabilities at the data link layer by manipulating MAC–IP binding relationships. Effective ARP mitigation requires specialized detection methodologies focusing on protocol-specific behavioral modeling and temporal traffic correlation. Recent studies have introduced ARP-focused ML frameworks that leverage features like ARP request-reply consistency and anomalous resolution sequences. Temporal deep learning models, primarily LSTM and hybrid CNN–LSTM architectures, have shown promise in detecting ARP poisoning patterns, while SDN-assisted frameworks enhance ARP defense through centralized visibility and dynamic port isolation. Nonetheless, ARP-focused solutions face challenges due to limited dataset availability, narrow validation, and insufficient studies on campus-scale deployment.

The evolving cyber threat landscape complicates ML-based intrusion prevention. DDoS attacks increasingly combine volumetric flooding with application-layer exploitation, while ARP spoofing attacks vary, including targeted cache poisoning and broadcast-based spoofing, each requiring distinct detection logic. Emerging threats, such as IoT-driven botnet attacks and adversarial machine learning techniques, challenge existing detection models by exploiting feature dependencies. These developments necessitate adaptive, context-aware ML frameworks that integrate packet-level, flow-level, and protocol-layer features to capture both large-scale volumetric anomalies and low-rate behavioral deviations.

Despite methodological advancements, several deployment challenges persist. The computational complexity of deep learning and hybrid ML frameworks often exceeds the capabilities of resource-constrained IoT devices and legacy infrastructure. Additionally, the scarcity and potential obsolescence of publicly available datasets limit model generalizability, particularly for ARP spoofing. Privacy and regulatory concerns related to packet-level inspection complicate implementation, while the limited interpretability of complex ML models reduces trust and delays responses. Addressing these limitations involves integrating modular and lightweight ML architectures, SDN-enabled orchestration mechanisms, and federated learning for distributed, privacy-preserving model training.

Furthermore, standardized evaluation frameworks and continuously updated multi-layer traffic datasets are essential for validating model robustness against evolving threats. Future research should prioritize large-scale data collection from live campus networks, use protocol-aware and context-specific feature engineering, and evaluate models in realistic, heterogeneous traffic scenarios. These steps will improve the robustness and practical relevance of ML-based anomaly detection, ensuring effective detection of stealthy threats like ARP spoofing and multi-layer DDoS attacks in real-world campus settings.

In conclusion, this review demonstrates that the shift from rule-based defenses to intelligent ML-based intrusion detection represents a paradigm shift in campus cybersecurity. By leveraging supervised, unsupervised, deep, and reinforcement learning, modern ML frameworks enable proactive, self-adaptive defense strategies capable of addressing both known and zero-day attacks, as well as volumetric and application-layer DDoS and ARP cache poisoning variations. While challenges related to computational complexity, dataset limitations, and evolving threat vectors remain, ML provides a scalable, resilient, and forward-looking foundation for securing campus network environments against an increasingly sophisticated and heterogeneous threat landscape.

8 Recommendations for future research

Recommendation for future research in ML for DDoS and ARP prevention on campus networks should focus on:

Adaptive, Hybrid, and Lightweight Models Future research should focus on developing lightweight, hybrid ML frameworks that integrate deep learning, reinforcement learning, and federated learning. These frameworks should dynamically extract features from heterogeneous campus traffic and adapt to evolving multi-layer threats, including DDoS attacks. For mitigating ARP spoofing, it is essential to prioritize protocol-aware feature engineering, utilizing IP–MAC binding stability metrics and temporal sequence modeling to detect Layer 2 attacks. Large-scale data from operational campus networks is crucial for enhancing generalizability and reproducibility, ensuring effective countermeasures against stealthy attacks, such as man-in-the-middle intrusions, while improving the scientific rigor and practical relevance of ML-based anomaly detection.

Interpretability and Explain ability Future models must enhance transparency, allowing network administrators to validate decisions, understand the causes of anomalies, and maintain trust in automated defenses. Explainable AI techniques should be embedded without compromising computational efficiency, particularly in resource constrained edge devices and SDN-enabled environments.

Scalability and real-time responsiveness ML models must operate efficiently across large-scale campus networks with diverse devices, fluctuating traffic, and IoT integration, providing immediate threat mitigation without introducing latency. Achieving this requires modular architectures, optimized inference pipelines, and SDN assisted orchestration to distribute computation between edge and centralized controllers.

Efficient data preprocessing Automated frameworks leveraging techniques such as auto-encoders, principal component analysis, and Synthetic Minority Oversampling (SMOTE)

can enhance feature extraction, address class imbalance, and improve model performance in both DDoS and ARP scenarios.

Finally, standardized evaluation frameworks are essential for objective assessment. Benchmark datasets, metrics, and experimental protocols should reflect the evolving and heterogeneous nature of campus networks, including IoT, WBAN, and SDN components, to facilitate meaningful comparisons across ML approaches.

By focusing on lightweight adaptability, interpretability, efficient data preprocessing, real-time scalability, and standardized evaluation, future research can produce ML-based solutions that are both reliable and practical. Integrating these strategies will enable campus networks to maintain high security, operational reliability, and resilience against increasingly sophisticated and multi-vector threats.

Author contributions

Each author listed has made significant contributions to the development and composition of this manuscript. Richard conceived the initial idea, while Sadiq and Maninit provided supervision throughout the research process. Richard and Sadiq participated in revising and refining the final manuscript. All authors have reviewed the manuscript and given their approval for publication.

Funding

No funding was received in writing this article.

Data availability

No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate

Formal ethical approval from an institutional review board or research ethics committee was not required for this study, as it did not involve human participants, animal subjects, or personally identifiable data. The research relied solely on secondary data and analytical evaluations of machine learning-based intrusion detection in campus and IoT network environments. All datasets used are anonymized, publicly accessible, and ethically approved by their original developers. The study adhered to internationally accepted research and publication ethics, ensuring transparency, data integrity, and responsible data utilization.

Consent for publication

This research did not involve human participants, primary data collection, or direct interaction with individuals. The study is based exclusively on the analysis of publicly available benchmark datasets, peer-reviewed literature, and analytically generated evaluations related to machine learning-based intrusion detection in campus and IoT network environments. All datasets used are anonymized and publicly accessible; therefore, informed consent from human participants was not required. Each author listed made significant scholarly contributions to the study. All authors reviewed, approved, and consented to participate in this research and its publication, ensuring compliance with institutional and international research ethics standards.

Competing interests

The authors declare no competing interests.

Received: 14 November 2025 / Revised: 16 April 2026 / Accepted: 17 April 2026

Published online: 07 May 2026

References

1. Mahdi ZS, Zaki RM, Alzubaidi L. Advanced hybrid techniques for cyberattack detection and defense in IoT networks. *Secur Priv*. 2025. <https://doi.org/10.1002/spy2.471>.
2. Alsamhi SH, et al. Machine learning for smart environments in B5G networks: connectivity and QoS. *Comput Intell Neurosci*. 2021. <https://doi.org/10.1155/2021/6805151>.
3. Zubairu B, Gide AI. Machine Learning-Based Framework for Detecting and Mitigating DoS Attacks in Mobile Ad-Hoc Networks (MANETs), 10, 2025.
4. Xie K, Darus MY, Liao B, Ding N, Ramli A. Distributed denial of service (DDoS) framework in software-defined networking (SDN): A comprehensive review, challenges and future directions. *Malaysian J Comput*. 2025;10(1):2038–58. <https://doi.org/10.24191/mjoc.v10i1.4422>.
5. Banerjee S S., Chakraborty P P. To detect the distributed denial-of-service attacks in SDN using machine learning algorithms. *Proc - IEEE 2021 Int Conf Comput Commun Intell Syst ICCIS 2021*. 2021;966–71. <https://doi.org/10.1109/ICCIS51004.2021.9397068>.
6. Morsy SM, Nashat D. An efficient scheme to detect and prevent ARP spoofing. *IEEE Access*. 2022;10:49142–53. <https://doi.org/10.1109/ACCESS.2022.3172329>.

7. Bello AB, Ogundipe AO, George AA, Anifowose O. The role of AI and machine learning in cybersecurity: Advancements in threat detection, anomaly detection and automated response. *Int J Sci Res Arch*. 2025;14(2):1587–97. <https://doi.org/10.30574/ijstra.2025.14.2.0542>.
8. Sharma A, Babbar H. Machine Learning-Based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks, 2024 5th Int. Conf. Emerg. Technol. INCET 2024, pp. 1–6, 2024. <https://doi.org/10.1109/INCET61516.2024.10593167>
9. Firdhaust RS, Wati KM, Tsabitah AZ, Wijayanto I. Comparative Analysis of Malicious Traffic Detection in IoT Network Using Machine Learning and Deep Learning Approaches, 2025 4th Int. Conf. Electron. Represent. Algorithm, pp. 18–23, 2025. <https://doi.org/10.1109/icera66156.2025.11086629>
10. Prasad A, Chandra S. Defending ARP Spoofing-based MitM Attack using Machine Learning and Device Profiling. 3rd IEEE 2022 Int Conf Comput Commun Intell Syst ICCIS 2022. 2022;978–82. <https://doi.org/10.1109/ICCIS56430.2022.10037723>.
11. Venturi A, Stabili D, Pollicino F, Bianchi E, Marchetti M. Comparison of Machine Learning-based anomaly detectors for Controller Area Network. NCA 2022–2022 IEEE 21st Int Symp Netw Comput Appl. 2022;21:81–8. <https://doi.org/10.1109/NCA57778.2022.10013527>.
12. Schummer P, del Rio A, Serrano J, Jimenez D, Sánchez G, Llorente Á. Machine learning-based network anomaly detection: Design, implementation, and evaluation. *AI*. 2024;5(4):2967–83. <https://doi.org/10.3390/ai5040143>.
13. Asharf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A. A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions. *Electronics Basel*. 2020. <https://doi.org/10.3390/electronics9071177>.
14. Bithi M, Hossain MA, Ahmed MK, Sultana R, Ahammad I, Islam MS. Enhanced DDoS Detection in Software Defined Networking Using Ensemble-Based Machine Learning, *Proc. – 6th Int. Conf. Electr. Eng. Inf. Commun. Technol. ICEEICT 2024*, no. May, pp. 1032–1037, 2024. <https://doi.org/10.1109/ICEEICT62016.2024.10534483>
15. Rajendra GTRN. DDoS protection using machine learning: A modern approach to cybersecurity. *J Eng Appl Sci Technol*. 2021;3(4):1–11. [https://doi.org/10.47363/jeast/2021\(3\)e128](https://doi.org/10.47363/jeast/2021(3)e128).
16. Wang Y, et al. Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey. *IEEE Commun Surv Tutor*. 2023;25(4):2245–98. <https://doi.org/10.1109/COMST.2023.3319492>.
17. Patil D, Rane NL, Desai P, Rane J. *Machine learning and deep learning: Methods, techniques, applications, challenges, and future research opportunities*, no. 2024. 2024. https://doi.org/10.70593/978-81-981367-4-9_2
18. Sawah MS, Elmannai H, El-Bary AA, Lotfy K, Sheta OE. Distributed denial of service (DDoS) classification based on random forest model with backward elimination algorithm and grid search algorithm. *Sci Rep*. 2025. <https://doi.org/10.1038/s41598-025-03868-x>.
19. Tuteja G, Singh AR, Kumar GR, Fallaah MH. XGBoost-Based Anomaly Detection in IoT Networks Using the RT-IoT2022 Dataset. 2025 4th OPIU Int Technol Conf Smart Comput Innov Adv Ind 5 0 OTCON 2025. 2025;1–6. <https://doi.org/10.1109/OTCON65728.2025.11070793>.
20. Yang Y. Random Forest-Based Machine Failure Prediction: A Performance Comparison. no. MI, 2025.
21. Karmous N, Ben Dhiab Y, Ould-Elhassen Aouelelyne M, Youssef N, Bouallegue R, Yazidi A. Deep learning approaches for protecting IoT devices in smart homes from MitM attacks. *Front Comput Sci*. 2024. <https://doi.org/10.3389/fcomp.2024.1477501>.
22. Checkpoint research. Cyber Security Report 2024 | Check Point Software, <https://www.checkpoint.com/Security-Report/?flz-category=Items&flz-item=Report-Cyber-Security-Report-2024>, 2024, [Online]. Available: <https://www.checkpoint.com/Security-Report/?flz-category=Items&flz-item=Report-Cyber-Security-Report-2024>
23. Bing A, Chai Z, Theng B, Kit M, Tee T, McCarthy C. Engineering applications of artificial intelligence enhancing road safety with machine learning: current advances and future directions in accident prediction using non-visual data. *Eng Appl Artif Intell*. 2024;137(PA):109086. <https://doi.org/10.1016/j.engappai.2024.109086>.
24. Aminu M, Akinsanya A. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *Int J Comput Appl Technol Res*. 2024;July:10–27. <https://doi.org/10.7753/ijcatr1308.1002>.
25. Nasser HI, Hussain MA. An effective approach to detect and prevent ARP spoofing attacks on WLAN. *Iraqi J Electr Electron Eng*. 2023;19(2):8–17. <https://doi.org/10.37917/ijeee.19.2.2>.
26. Zahid M, Bharati TS. Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection. *Discover Internet Things*. 2025. <https://doi.org/10.1007/s43926-025-00156-y>.
27. Cipriano C, Noce S, Mereu S, Santini M. Algorithms going wild – a review of machine learning techniques for terrestrial ecology. *Ecol Modell*. 2025;506(January):111164. <https://doi.org/10.1016/j.ecolmodel.2025.111164>.
28. Alsaaidah A, Almomani O, Abu-Shareha AA, Abualhaj MM, Achuthan A. ARP spoofing attack detection model in IoT network using machine learning: complexity vs. accuracy. *J Appl Data Sci*. 2024;5(4):1850–60. <https://doi.org/10.47738/jad.s.v5i4.374>.
29. Sathyamoorthy S, Matthew UO, Adekunle TS, Okafor NU. Advances and challenges in IoT sensors data handling and processing in environmental monitoring networks. *HAFED POLY J Sci Manag Technol*. 2024;5(2):40–60. <https://doi.org/10.4314/hpjsmt.v5i2.3>.
30. Hnamte V, Hussain J. Dependable intrusion detection system using deep convolutional neural network: a novel framework and performance evaluation approach. *Telemat Informatics Rep*. 2023;11(April):100077. <https://doi.org/10.1016/j.tele.r.2023.100077>.
31. Ahmed AS, Salah HA. Development a Software Defined Network (SDN) with Internet of Things (IoT) Security for Medical Issues. *J Al-Qadisiyah Comput Sci Math*. 2023;15(3). <https://doi.org/10.29304/jqcm.2023.15.3.1268>.
32. Sumanasekara SG, Abeysinghe DVDS. Machine learning-based detection of ARP spoofing attacks using behavioral analysis. *Proc - Int Res Conf Smart Comput Syst Eng SCSE*. 2025;2025:1–6. <https://doi.org/10.1109/SCSE65633.2025.11030930>.
33. Aldhaheer A, Alwahedi F, Ferrag MA, Battah A. Deep learning for cyber threat detection in IoT networks: a review. *Internet Things Cyber-Phys Syst*. 2024;4(September 2023):110–28. <https://doi.org/10.1016/j.iotcps.2023.09.003>.
34. Alnasser O, Muhtadi JA, Saleem K, Shrestha S. Signature and anomaly based intrusion detection system for secure IoTs and V2G communication. *Alexandria Eng J*. 2025;125(March):424–40. <https://doi.org/10.1016/j.aej.2025.03.068>.
35. Security N. *Networking Security*, pp. 1–44, 2025.
36. 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. <https://doi.org/10.1109/ACCESS.2021.3071263>.

37. Nassif AB, Talib MA, Nasir Q, Dakalbab FM. Machine learning for anomaly detection: a systematic review. *IEEE Access*. 2021;9:78658–700. <https://doi.org/10.1109/ACCESS.2021.3083060>.
38. Emirmahmutoglu E, Atay Y. A feature selection-driven machine learning framework for anomaly-based intrusion detection systems. *Peer-to-Peer Netw Appl*. 2025. <https://doi.org/10.1007/s12083-025-01947-4>.
39. Bagaa M, Taleb T, Bernabe JB, Skarmeta A. A Machine Learning Security Framework for IoT Systems. no May. 2020. <https://doi.org/10.1109/ACCESS.2020.2996214>.
40. Mishra SR, Shanmugam B, Yeo KC. SDN-Enabled IoT Security Frameworks — A Review of Existing Challenges, pp. 1–38, 2025.
41. Bashaa MH. Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking: A Review Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking : A Revi, 1, 1, 2025.
42. Sarma B, Kumar R, Tuithung T. Machine learning enabled network and task management in SDN based fog architecture. *Comput Electr Eng*. 2023;108:108705. <https://doi.org/10.1016/j.compeleceng.2023.108705>.
43. Chaganti R, Suliman W, Ravi V. Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks, pp. 1–21, 2023.
44. Solutions S, Rathore MS, Iqbal J, Abdelhaq M, Alsaqour R, Ullah SS. Network Threat Detection Using Machine / Deep Learning in SDN-Based Platforms. *A Comprehensive Analysis of*; 2022.
45. Okunola A. Optimizing Anomaly Detection in Network Traffic: A Comparative Study of Machine Learning Algorithms for Real-time Incident Prevention and Response. no. July, 2025.
46. Karthickkumar A, Rathnamala S, Parameswari C, Prabhananthakumar M. Design and Development of A Novel CNN- BiLSTM Hybrid Deep Learning Model for Cyber Attacks Detection in an IoT Environment. 2025 IEEE Int Conf Interdiscip Approaches Technol Manag Soc Innov. 2025;3:1–6. <https://doi.org/10.1109/IATMSI64286.2025.10985456>.
47. Purnomo A. Implementation of DHCP Snooping Method to Improve Security on Computer Networks, *bit-Tech*, vol. 6, no. 3, 2024, <https://doi.org/10.32877/bt.v6i3.1174>
48. Chinnasamy R, Subramanian M, Easwaramoorthy SV, Cho J. Deep learning-driven methods for network-based intrusion detection systems: a systematic review. *ICT Express*. 2025;11(1):181–215. <https://doi.org/10.1016/j.icte.2025.01.005>.
49. Jazaeri SS, Jabbehdari S, Asghari P, Haj Seyyed Javadi H. Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions. *Cluster Comput*. 2021;24(4):3187–228. <https://doi.org/10.1007/s10586-021-03311-6>.
50. Mohamed N. Cutting-edge advances in AI and ML for cybersecurity: a comprehensive review of emerging trends and future directions. *Cogent Bus Manag*. 2025;12(1). <https://doi.org/10.1080/23311975.2025.2518496>.
51. Patil VT. Deep Learning-Driven IoT Defence: Comparative Analysis of CNN and LSTM for DDoS Detection and Mitigation, *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 8s, pp. 08–21, 2025, <https://doi.org/10.52783/jisem.v10i8s.951>
52. Raio S, et al. Reinforcement learning as a path to autonomous intelligent cyber-defense agents in vehicle platforms. *Applied Sciences*. 2023. <https://doi.org/10.3390/app132111621>.
53. Hirsi A, Audah L, Salh A, Alhartomi MA, Ahmed S. Detecting DDoS threats using supervised machine learning for traffic classification in software defined networking. *IEEE Access*. 2024;12(November):166675–702. <https://doi.org/10.1109/ACCESS.2024.3486034>.
54. Dai Z, et al. An intrusion detection model to detect zero-day attacks in unseen data using machine learning. *PLoS One*. 2024;19(9):1–25. <https://doi.org/10.1371/journal.pone.0308469>.
55. Jasim MN, Gaata MT. K-Means clustering-based semi-supervised for DDoS attacks classification. *Bull Electr Eng Inform*. 2022;11(6):3570–6. <https://doi.org/10.11591/eei.v11i6.4353>.
56. Duarte JM, Berton L. A review of semi-supervised learning for text classification. *Artif Intell Rev*. 2023. <https://doi.org/10.1007/s10462-023-10393-8>.
57. Cassidy C. Reinforcement Learning with Deep Q-Networks (DQN), *SSRN Electron. J.*, vol. 16, no. August 2016, pp. 575–582, 2016.
58. Kumar MA, Purohit KC, Bhatt J, Semuwal GS. Advanced ARP Attack Protection in SDNs Using Deep Learning Approach. 2024 IEEE Int Conf Blockchain Distrib Syst Secur ICBDS 2024. 2024;1–6. <https://doi.org/10.1109/ICBDS61829.2024.10837534>.
59. Yasarathna TL, Liyanage M, Le-Khac NA. Deep learning based autonomous anomaly detection for security in SDN-IoT networks. *IEEE Open J Commun Soc*. 2025;PP:1. <https://doi.org/10.1109/OJCOMS.2025.3610365>.
60. Zulfiqar Z, Malik SUR, Moqurrah SA, Zulfiqar Z, Yaseen U, Srivastava G. DeepDetect: an innovative hybrid deep learning framework for anomaly detection in IoT networks. *J Comput Sci*. 2024;83(August):102426. <https://doi.org/10.1016/j.jocs.2024.102426>.
61. Nabi F, Zhou X. Cyber Security and Applications Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security, vol. 2, no. December 2023, 2024. <https://doi.org/10.1016/j.csa.2023.100033>
62. Lakshmi V, Rajkumar S. Results in engineering hybrid ensemble federated learning using SMOTE-Tomek for efficient DDoS detection on constrained edge devices over 5G networks. *Results Eng*. 2025;28(July):107601. <https://doi.org/10.1016/j.rine.2025.107601>.
63. Najjar AA, Naik SM. DDoS attack detection using CNN-BiLSTM with attention mechanism. *Telemat Inform Rep*. 2025;18(May):100211. <https://doi.org/10.1016/j.teler.2025.100211>.
64. Butt HA, Al Harthy KS, Shah MA, Hussain M, Amin R, Rehman MU. Enhanced DDoS detection using advanced machine learning and ensemble techniques in software defined networking. *Comput Mater Contin*. 2024;81(2):3003–31. <https://doi.org/10.32604/cmc.2024.057185>.
65. Mustafa R, Sarkar NI, Mohaghegh M, Pervez S. Cross-Layer Analysis of Machine Learning Models. for Secure and Energy-Efficient IoT Networks; 2025.
66. Abiramasundari S, Ramaswamy V. Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms. *Sci Rep*. 2025. <https://doi.org/10.1038/s41598-024-84879-y>.
67. Mondragon JC, Biswal RR, Branco P, Andres GJ. Advanced IDS: A comparative study of datasets and machine learning algorithms for network flow-based intrusion detection systems. *Appl Intell*. 2025. <https://doi.org/10.1007/s10489-025-06422-4>.
68. Okolie SA, Amadi CA, Odii JN, Nwokorie EC, Onyemauche UC. Franklin open anomaly detection in heterogeneous cybersecurity data. *Franklin Open*. 2025;13(July):100426. <https://doi.org/10.1016/j.fraope.2025.100426>.

69. Usmani M, Anwar M, Farooq K, Ahmed G, Siddiqui S. Predicting ARP spoofing with Machine Learning, 2022 *Int. Conf. Emerg. Trends Smart Technol. ICETST* 2022, no. January, 2022. <https://doi.org/10.1109/ICETST55735.2022.9922925>
70. Sinha P, Sahu D, Prakash S, Rathore RS. An efficient data driven framework for intrusion detection in wireless sensor networks using deep learning, pp. 1–25, 2025.
71. Ali A, Husain M, Hans P. Intelligent ARP Spoofing Detection using Multi-layered Machine Learning (ML) Techniques for IoT Networks, pp. 1–5, 2025, [Online]. Available: <http://arxiv.org/abs/2507.21087>
72. Abbas A et al. Machine learning-based hybrid technique to enhance cyber-attack perspective, 2025.
73. Alashhab AA, Zahid MS, Isyaku B, Elnour AA. Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. *IEEE Access*. 2024;12(March):51630–49. <https://doi.org/10.1109/ACCESS.2024.3384398>.
74. Firouzi A, Dadkhah S, Maret SA, Ghorbani AA. DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection, 2025.
75. Alfathe M, Mustapha A, Mohamed HL, Mostafa SA, Yousif YK, Al-Shakarchi AH. Detecting DDoS attacks in network traffic based on supervised machine learning techniques. *Al-Noor J Inf Technol Cybersecurity*. 2024;1:23–48. <https://doi.org/10.69513/jnft.v1.i0.a2>.
76. Raza MS, Nowzin M, Sheikh A, Hwang I. Ensemble Learning-Based DDOS Attack Recognition in IoT Networks Ensemble Learning - Based DDOS Attack Recognition in IoT Networks. no July. 2025. <https://doi.org/10.37256/cnc.3220256755>.
77. Du KL, Jiang B, Lu J, Hua J, Swamy MNS. Exploring kernel machines and support vector machines: principles, techniques, and future directions. *Mathematics Basel*. 2024;12(24):1–58. <https://doi.org/10.3390/math12243935>.
78. Halder RK, Uddin MN, Uddin MA, Aryal S, Khraisat A. Enhancing K-nearest neighbor algorithm: a comprehensive review and performance analysis of modifications. *J Big Data*. 2024. <https://doi.org/10.1186/s40537-024-00973-y>.
79. Berrar D. Bayes' Theorem and Naive Bayes Classifier, *Encycl. Bioinforma. Comput. Biol.*, no. January 2024, pp. 483–494, 2025. <https://doi.org/10.1016/b978-0-323-95502-7.00118-4>
80. Fathima A, Devi GS, Faizaanuddin M. Improving distributed denial of service attack detection using supervised machine learning. *Meas Sensors*. 2023;30(October):100911. <https://doi.org/10.1016/j.measen.2023.100911>.
81. Inspiration T, Model NN. *Fundamentals of Artificial Neural Networks and Deep Learning*. 2022.
82. Liu H, Wang H. Real-time anomaly detection of network traffic based on CNN. *Symmetry (Basel)*. 2023. <https://doi.org/10.3390/sym15061205>.
83. Sumathi S, Rajesh R, Lim S. Recurrent and deep learning neural network models for DDoS attack detection. *J Sensors*. 2022. <https://doi.org/10.1155/2022/8530312>.
84. Aydin H, Orman Z, Aydin MA. A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Comput Secur*. 2022;118:102725. <https://doi.org/10.1016/j.cose.2022.102725>.
85. Ali ZA, Abduljabbar ZH, Tahir HA, Sallow AB, Almufti SM. eXtreme Gradient Boosting algorithm with machine learning: a review. *Acad J Nawroz Univ*. 2023;12(2):320–34. <https://doi.org/10.25007/ajnu.v12n2a1612>.
86. Nzuva SM, Nder L, Mwalili T. A novel bagging- XGBoost ensemble model for attaining high accuracy and computational efficiency in network intrusion detection. *E3S Web Conf*. 2024;501. <https://doi.org/10.1051/e3sconf/202450101007>.
87. Hussain SS, Zaidi SSH. AdaBoost ensemble approach with weak classifiers for gear fault diagnosis and prognosis in DC motors. *Appl Sci (Basel)*. 2024. <https://doi.org/10.3390/app14073105>.
88. Chen W, Yang H, Yin L, Luo X. Large-scale IoT attack detection scheme based on LightGBM and feature selection using an improved salp swarm algorithm. *Sci Rep*. 2024;14(1):1–25. <https://doi.org/10.1038/s41598-024-69968-2>.
89. Lin YD, Liu ZQ, Hwang RH, Nguyen VL, Lin PC, Lai YC. Machine learning with Variational AutoEncoder for imbalanced datasets in intrusion detection. *IEEE Access*. 2022;10:15247–60. <https://doi.org/10.1109/ACCESS.2022.3149295>.
90. Lu W, Ding D, Wu F, Yuan G. An efficient Gaussian mixture model and its application to neural networks. *Knowl Based Syst*. 2025. <https://doi.org/10.1016/j.knsys.2024.112942>.
91. Dinh T, et al. Journal of Data Science Management. 2025. <https://doi.org/10.1016/j.dsm.2025.08.001>.
92. Huang Z, Liang Z, Zhou S, Zhang S. An improved density-based spatial clustering of applications with noise algorithm with an adaptive parameter based on the sparrow search algorithm. *Algorithms*. 2025. <https://doi.org/10.3390/a18050273>.
93. Balaji K, Balachandra M. Applying principal component analysis for categorized dimensionality reduction in DDoS detection for software-defined networks. *F1000Res*. 2025;14:743. <https://doi.org/10.12688/f1000research.163778.1>.
94. Omoosebi A, Max L. Reinforcement Learning (RL): Adaptive decision-making through rewards/punishments (e.g., optimizing chatbot responses). no May, 2025.
95. Alavizadeh H, Alavizadeh H, Jang-Jaccard J. Deep Q-Learning based reinforcement learning approach for network intrusion detection. *Computers*. 2022;11(3):1–19. <https://doi.org/10.3390/computers11030041>.
96. Zhang X, Yin J. Optimized extreme learning machines with deep learning for high-performance network traffic classification. *Sci Rep*. 2025;15(1):1–15. <https://doi.org/10.1038/s41598-025-16980-9>.
97. Talpur F, Korejo IA, Chandio AA, Ghulam A, Talpur MSH. ML-based detection of DDoS attacks using evolutionary algorithms optimization. *Sensors Basel*. 2024. <https://doi.org/10.3390/s24051672>.
98. For U, Ethinking R, Achine M, Earning L, Odel M, Valuation E. vol. 16, no. 5, pp. 1–8, 2022, <https://doi.org/10.5121/jjaia.2025.16501>
99. Mulissa YG, Li W, Kumar A, Wang L. A Hybrid Deep Learning Model for IoT Network Anomaly Detection. *Conf Proc - IEEE SOUTHEASTCON*. 2025;1370–5. <https://doi.org/10.1109/SoutheastCon56624.2025.10971453>.
100. Chung J, Chen IY. Enhancing Semi-supervised Learning with Zero-shot Pseudolabels, pp. 1–24, 2025, [Online]. Available: <http://arxiv.org/abs/2502.12584>
101. Wei Y, Jang-Jaccard J, Sabrina F, Xu W, Camtepe S, Dunmore A. Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data. no July. 2023. <https://doi.org/10.48550/arXiv.2305.09475>.
102. Bilal T, El Madhoun N, Al Agha K, Zouaoui A. Graph Neural Networks for intrusion detection: a survey. *IEEE Access*. 2023;11:49114–39. <https://doi.org/10.1109/ACCESS.2023.3275789>.
103. Harshdeep K, Sumalatha K, Mathur R. DeepTransIDS: transformer-based deep learning model for detecting DDoS attacks on 5G NIDD. *Results Eng*. 2025;26(April):104826. <https://doi.org/10.1016/j.rineng.2025.104826>.
104. Khraisat A, Alazab A, Alazab M, Obeidat A, Singh S, Jan T. Federated learning for intrusion detection in IoT environments: a privacy-preserving strategy. *Discov Internet Things*. 2025;5(1):1–17. <https://doi.org/10.1007/s43926-025-00169-7>.

105. Hammad AA, Ahmed SR, Abdul-Hussein MK, Ahmed MR, Majeed DA, Algburi S. *Deep Reinforcement Learning for Adaptive Cyber Defense in Network Security*, vol. 1, no. 1. Association for Computing Machinery, 2024. <https://doi.org/10.1145/3660853.3660930>
106. Ruan L, Dias MPI, Wong E. Enhancing latency performance through intelligent bandwidth allocation decisions: a survey and comparative study of machine learning techniques. *J Opt Commun Netw*. 2020;12(4):B20–32. <https://doi.org/10.1364/JOCN.379715>.
107. Alfahaid A, Alalwany E, Almars AM, Alharbi F, Atlam E, Mahgoub I. Machine learning-based security solutions for IoT networks: a comprehensive survey. *Sensors Basel*. 2025;25(11):1–48. <https://doi.org/10.3390/s25113341>.
108. Ahuja N, Singal G, Mukhopadhyay D. DLSN: Deep learning for DDOS attack detection in software defined networking, *Proc. Conflu*. 2021 11th Int. Conf. Cloud Comput. Data Sci. Eng., pp. 683–688, 2021. <https://doi.org/10.1109/Confluence51648.2021.9376879>
109. Ullah I, Mahmoud QH. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access*. 2021;9:103906–26. <https://doi.org/10.1109/ACCESS.2021.3094024>.
110. De Elias EM, et al. A Hybrid CNN-LSTM Model for IIoT Edge Privacy-Aware Intrusion Detection. 2022 IEEE Latin-American Conf Commun LATINCOM 2022. 2022. <https://doi.org/10.1109/LATINCOM56090.2022.10000468>.
111. Adisheshaiah M, Sailaja M. A parallel decision-making design for highly speedy packet classification. *Microprocess Microsyst*. 2023;99:104826. <https://doi.org/10.1016/j.micpro.2023.104826>.
112. Hua H, Li Y, Wang T, Dong N, Li W, Cao J. Edge computing with artificial intelligence: a machine learning perspective. *ACM Comput Surv*. 2023. <https://doi.org/10.1145/3555802>.
113. Li J, Chen H, Othman M, Mi L. Intelligent systems with applications enhancing IoT security: a comparative study of feature reduction techniques for intrusion detection system. *Intell Syst with Appl*. 2024;23(June):200407. <https://doi.org/10.1016/j.iswa.2024.200407>.
114. Venkatraman S, Kanthimathi S, Jayasankar KS, Jiljith TP, Jashwanth R. A novel self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification. *IEEE Access*. 2024;12:151515–31. <https://doi.org/10.1109/ACCESS.2024.3478764>.
115. Ahmad SZ, et al. A GAN-based approach for enhancing security in satellite based IoT networks using MPI enabled HPC. *PLoS One*. 2025. <https://doi.org/10.1371/journal.pone.0331019>.
116. Alobaid A, Bonny T, Alrahhal M. Intelligent Systems with Applications Disruptive attacks on artificial neural networks: A systematic review of attack techniques, detection methods, and protection strategies, *Intell. Syst. with Appl*, vol. 26, no. September 2024, p. 200529, 2025. <https://doi.org/10.1016/j.iswa.2025.200529>
117. Ain NU, Sardaraz M, Tahir M, Abo Elsoud MW, Alourani A. Securing IoT networks against DDoS attacks: a hybrid deep learning approach. *Sensors Basel*. 2025;25(5):1–23. <https://doi.org/10.3390/s25051346>.
118. Bechere M, Barkat A, Ghenabzia A, Yiltas-Kaplan D. Urban traffic prediction using hybrid XGBoost–LSTM model. *International Journal of Computing and Digital Systems*. 2025. <https://doi.org/10.12785/ijcds/1571136041>.
119. Cherukuri S, Prasad SDV. EnsembleSkinNet: a transfer learning-based framework for efficient skin cancer detection with explainable AI integration. *Front Oncol*. 2025;December:1–26. <https://doi.org/10.3389/fonc.2025.1699960>.
120. Hamad NA, Bakar KAA, Qamar F, Jubair AM, Mohamed RR, Mohamed MA. Systematic analysis of federated learning approaches for intrusion detection in the Internet of Things environment. *IEEE Access*. 2025;13:95410–44. <https://doi.org/10.1109/ACCESS.2025.3574672>.
121. Makris I, Karampasi A, Radoglou-grammatikis P. Review article A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions, *Comput. Sci. Rev*, vol. 56, no. November 2024, p. 100717, 2025. <https://doi.org/10.1016/j.cosrev.2024.100717>
122. Qin X, Doss R, Jiang F, Qin X, Long B. Securing ICS networks: SDN-based automated traffic control and MTD defensive framework against DDoS attacks. *Comput Commun*. 2025;241(January):108252. <https://doi.org/10.1016/j.comcom.2025.108252>.
123. Li L, Zhu L, Li W. Privacy-Preserving Federated Learning for Space – Air – Ground Integrated Networks: A Bi-Level Reinforcement Learning and Adaptive Transfer Learning Optimization Framework, 2025.
124. Uddin S, He J, Tunio S, Zhu N, Nazir A, Wajahat A. Journal of King Saud University - Computer and Information Sciences systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *J King Saud Univ - Comput Inf Sci*. 2024;36(8):102164. <https://doi.org/10.1016/j.jksuci.2024.102164>.
125. Harshavardhan A, Sree Vani M, Patil A, Yamsani N, Archana K. Hybrid deep learning framework for intrusion detection: integrating Cnn, Lstm, and attention mechanisms to enhance cybersecurity. *J Theor Appl Inf Technol*. 2025;103(1):63–78.
126. Saiyedand MF, Al-Anbagi I. Deep ensemble learning with pruning for DDOS attack detection in IoT networks. *IEEE Trans Mach Learn Commun Netw*. 2024;2:596–616. <https://doi.org/10.1109/tmlcn.2024.3395419>.
127. Yasarithna TL, Liyanage M, Le-Khac NA. Deep learning based autonomous anomaly detection for security in SDN-IoT networks. *IEEE Open J Commun Soc*. 2025. <https://doi.org/10.1109/OJCOMS.2025.3610365>.
128. Alluraiah K, Sheela M, Chetty R. International Journal of INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Ensemble Learning Method for DDOS Attack Mitigation in Web Based Networks, *Orig. Res. Pap. Int. J. Intell. Syst. Appl. Eng. IJISAE*, vol. 2024, no. 3, pp. 743–753, 2024, [Online]. Available: www.ijisae.org.
129. Anyanwu G, Nwakanma C, Lee JM, Kim D-S. RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network. *Ad Hoc Netw*. 2023;140:103026. <https://doi.org/10.1016/j.adhoc.2022.103026>.
130. Rozam NF, Riaseatiawan M. XGBoost classifier for DDOS attack detection in software defined network using sFlow protocol. *Int J Adv Sci Eng Inf Technol*. 2023;13(2):718–25. <https://doi.org/10.18517/ijaseit.13.2.17810>.
131. Kheddar H, Dawoud DW, Awad AI, Himeur Y, Khan MK. Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review. Volume 27. *IEEE*; 2024. 410.1109/COMST.2024.3484491.
132. Manzano R, Zaman M, Upadhyay D, Goel N, Sampalli S. Federated learning framework based on distributed storage and diffusion model for intrusion detection on IoT networks. *IEEE Access*. 2025;13(May):79571–95. <https://doi.org/10.1109/ACCESS.2025.3565409>.
133. Kampa S. Advanced Machine Learning Techniques for Anomaly Detection in Edge Computing Security: A Framework for Real-Time Threat Mitigation Advanced Machine Learning Techniques for Anomaly Detection in Edge Computing Security : A Framework for Real-Time Threat Mi. no. March, 2025.

134. Zhan S, Huang L, Luo G, Zheng S, Gao Z, Chao HC. A review on federated learning architectures for privacy-preserving AI: lightweight and secure cloud–edge–end collaboration. *Electronics*. 2025. <https://doi.org/10.3390/electronics14132512>.
135. Sinha H. An Efficient Machine Learning Based Models for Anomaly Detection in Network Traffic, 2024 Int. Conf. Intell. Comput. Sustain. Innov. Technol. IC-SIT 2024, no. January, 2024. <https://doi.org/10.1109/IC-SIT63503.2024.10862888>
136. Ness S, Eswarakrishnan V, Sridharan H, Shinde V, Janapareddy NVP, Dhanawat V. Anomaly detection in network traffic using advanced machine learning techniques. *IEEE Access*. 2025;13(January):16133–49. <https://doi.org/10.1109/ACCESS.2025.3526988>.
137. Hassan SEH, Duong-Trung N. Machine learning in cybersecurity: advanced detection and classification techniques for network traffic environments. *EAI Endorsed Trans Ind Networks Intell Syst*. 2024;11(3):1–22. <https://doi.org/10.4108/eetinis.v11i3.5237>.
138. Zakariah M. Classification of large datasets using random forest algorithm in various applications: survey. *Int J Eng Innov Technol*. 2014;4(3):189–98.
139. Thakur DS, Kumar Tiwari DV, Agrawal DJ. Performance analysis of linear kernel support vector machine models on real-world datasets. *Int J Adv Netw Appl*. 2025;17(01):6753–60. <https://doi.org/10.35444/ijana.2025.17106>.
140. Yang Q. Performance analysis of k-Nearest Neighbors classification on Reuters news article datasets. *Applied and Computational Engineering*. 2024;55(1):175–80. <https://doi.org/10.54254/2755-2721/55/20241444>.
141. Mienye ID, Jere N. A survey of decision trees: concepts, algorithms, and applications. *IEEE Access*. 2024;12:86716–27. <https://doi.org/10.1109/ACCESS.2024.3416838>.
142. Ravikumar H, Vidyalaya RM. Based Botnet Detection Architecture for IoT Networks in Cloud Platforms Research Article XGBoost-Based Botnet Detection Architecture for IoT Networks in Cloud Platforms, no. July 2024, 2025.
143. Liang Y, Tan J, Xie Z, Chen Z, Lin D, Yang Z. Research on Convolutional Neural Network Inference Acceleration and Performance Optimization for Edge Intelligence. *Sensors*. 2024;24(1). <https://doi.org/10.3390/s24010240>.
144. Leinonen M, Al-Tachmeesschi A, Turkmen B, Atashi N, Ruotsalainen L. Long short term memory based traffic prediction using multi-source data. *Int J Intell Transp Syst Res*. 2025;23(1):354–71. <https://doi.org/10.1007/s13177-024-00451-y>.
145. Azzouni A, Pujolle G. A Long Short-Term Memory Recurrent Neural Network Framework for Network Traffic Matrix Prediction, 2017, [Online]. Available: <http://arxiv.org/abs/1705.05690>
146. Nazir S, Patel S, Patel D. Autoencoder based anomaly detection for SCADA networks. *Int J Artif Intell Mach Learn*. 2021;11(2):83–99. <https://doi.org/10.4018/ijaiml.20210701.oa6>.
147. Oladele S. Reinforcement Learning for Dynamic Model Selection and Adaptation in Real-Time Streaming Analytics. no. April, 2025.
148. Zhang Z, Gao Z, Guo Y, Gong Y. Scalable and low-latency federated learning with cooperative mobile edge networking. *IEEE Trans Mob Comput*. 2024;23(1):812–22. <https://doi.org/10.1109/TMC.2022.3216837>.

Publisher's note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.