

OPEN ACCESS

EDITED BY

Rogério Dionísio,
Polytechnic Institute of Castelo Branco,
Portugal

REVIEWED BY

M. Prasad,
Shri Vishnu Engineering College for
Women, India
Agus Tedyyana,
Politeknik Negeri Bengkalis, Indonesia
Abraham Tetteh,
Bia Lamplighter College of Education,
Ghana

*CORRESPONDENCE

Kirungi Richard
✉ kirungi@kiu.ac.ug

RECEIVED 04 June 2026

REVISED 16 September 2026

ACCEPTED 17 September 2026

PUBLISHED 09 October 2026

CITATION

Richard K, Sadiq BO and
Maniniti V (2026) Enhancing university
network security through ML-based
detection of DDoS and ARP spoofing
attacks: a systematic review.
Front. Comput. Sci. 8:1900515.
doi: 10.3389/fcomp.2026.1900515

COPYRIGHT

© 2026 Richard, Sadiq and Maniniti. This
is an open-access article distributed
under the terms of the [Creative
Commons Attribution License \(CC BY\)](#).
The use, distribution or reproduction in
other forums is permitted, provided the
original author(s) and the copyright
owner(s) are credited and that the
original publication in this journal is
cited, in accordance with accepted
academic practice. No use, distribution
or reproduction is permitted which does
not comply with these terms.

Enhancing university network security through ML-based detection of DDoS and ARP spoofing attacks: a systematic review

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

¹Faculty of Science and Technology, Department of Computing, Kampala International University, Kampala, Uganda, ²Department of Electrical, Telecommunication and Computer Engineering, Kampala International University, Kampala, Uganda

Introduction: University networks are increasingly vulnerable to Distributed Denial-of-Service (DDoS) and Address Resolution Protocol (ARP) spoofing attacks due to open-access architectures, Bring Your Own Device (BYOD) practices, Internet of Things (IoT) integration, and dynamic traffic patterns. This study systematically reviews machine learning (ML)-based approaches for detecting these threats in university and related network environments.

Methods: Following PRISMA 2020 guidelines, peer-reviewed studies published from January 2021 to January 2026 were identified through IEEE Xplore, SpringerLink, ScienceDirect, Taylor & Francis Online, and Web of Science, with the final database search completed on 31 January 2026. Of 400 identified records, 200 studies met the predefined eligibility and quality criteria and were included in the synthesis. The review examined supervised, unsupervised, semi-supervised, deep learning, hybrid, and ensemble approaches with respect to detection performance, validation strategies, deployment readiness, computational efficiency, adaptability, and explainability.

Results: The findings indicate that many reviewed studies reported strong detection performance across supervised, unsupervised, deep learning, hybrid, and ensemble approaches. Hybrid and ensemble models frequently demonstrated strong reported results; however, these findings were not directly comparable across studies because of differences in datasets, attack scenarios, feature sets, validation procedures, and experimental environments. Benchmark datasets were used in 48% of the reviewed studies, whereas only 12% evaluated real university networks. Real-time detection was assessed in 40% of studies, while continuous learning, concept-drift detection, and model adaptation received comparatively limited attention.

Discussion: The evidence does not establish universal superiority of any particular learning paradigm and suggests that reported performance depends substantially on the evaluation context and methodological conditions. These findings highlight the need for adaptive, context-aware, cross-layer, and explainable intrusion detection approaches capable of addressing the operational characteristics of university networks.

KEYWORDS

anomaly detection, ARP spoofing, cybersecurity, DDoS attacks, intrusion detection system, IoT and BYOD, machine learning

1 Introduction

The rapid development of digital connectivity in universities has transformed academic, research, and administrative operations. Institutions increasingly rely on interconnected systems for online learning, virtual classrooms, student management, and cloud services. This expansion has dramatically increased network traffic and introduced complex cybersecurity challenges across multiple layers and devices. University networks, characterized by open-access policies, BYOD practices, and extensive IoT integration, are particularly vulnerable to cyber threats such as DDoS attacks, ARP spoofing, man-in-the-middle attacks, and zero-day intrusions. Recent reports confirm that open-access and BYOD-friendly campus environments significantly increase the attack surface and complicate continuous monitoring (Sharma K. V. et al., 2024). Traditional security mechanisms, including rule-based firewalls and signature-based intrusion detection systems, often struggle to cope with dynamic and sophisticated attacks in heterogeneous and rapidly evolving environments (Hasan et al., 2023).

ML-based anomaly detection has emerged as a promising approach for enhancing intrusion detection and prevention in complex network environments, including university networks. Unlike conventional signature-based IDS, ML models learn underlying patterns from both normal and malicious network traffic, enabling the identification of previously unseen and evolving attack behaviors (Kaur and Singh, 2020). Empirical studies demonstrate that ML-based approaches achieve higher detection accuracy, lower false-positive rates, real-time threat identification, and greater scalability compared to traditional methods, which is critical given the increasing frequency and sophistication of DDoS and ARP-based attacks (Alfahaid et al., 2025; Chukwuani et al., 2025; Hirsi and Member, 2025).

1.1 Background

University networks are inherently complex, open, and highly heterogeneous digital environments designed to support a wide range of academic and multifunctional activities, unlike corporate or government networks that operate under strict access controls (Xu, 2022; Ngoie, 2022). These infrastructures support diverse systems such as e-learning platforms, cloud-hosted research repositories, and IoT-enabled smart campus technologies (Pham et al., 2020). This diversity leads to irregular, high-volume, and rapidly fluctuating traffic patterns, expanding the network attack surface through unmanaged devices and insecure endpoints (Mallick and Nath, 2024).

This unique environment has contributed to a rise in sophisticated cyber threats targeting universities globally (Fouad, 2021). Attackers exploit vulnerabilities in open Wi-Fi, insecure IoT devices, and outdated systems, exposing institutions to DDoS attacks, ARP spoofing, phishing, and ransomware (Hussain et al., 2024). Traditional rule-based intrusion detection mechanisms struggle to cope with such threats due to unpredictable traffic and evolving attack patterns (Liu et al., 2021). This therefore highlights the need for intelligent, adaptive cybersecurity approaches, particularly ML-based anomaly detection models that can learn complex network behaviors and enhance intrusion detection and prevention in university environments (Dong and Kotenko, 2025).

University networks are dynamic digital ecosystems that allow unrestricted access for diverse users and a variety of devices (Rojas and Chiappe, 2024). Unlike government, military, or corporate

environments with strict access controls, universities support thousands of students, staff, researchers, visitors, and collaborators who connect personal devices and cloud-based platforms (Ulven and Wangen, 2021). This openness, rooted in academic freedom and collaborative learning, creates shifting traffic patterns, inconsistent security configurations, and limited oversight of devices (Schiefer et al., 2023).

The mix of managed systems and unmanaged personal devices, along with BYOD practices and reduced firewall restrictions, increases heterogeneity and introduces vulnerabilities such as insecure endpoints and weak authentication. As the ecosystem grows to include smart classroom technologies and large research data centers, maintaining uniform security controls and full network visibility becomes more difficult (Singh et al., 2025).

University networks also face elevated cybersecurity risks due to dynamic traffic patterns, BYOD practices, student experimentation, and reliance on third-party cloud services. Combined with legacy infrastructure and unmanaged devices, these factors increase vulnerability to DDoS attacks, ARP spoofing, ransomware, and botnet activity (Sadiqzade and Alisoy, 2025; Umoke et al., 2025). Consequently, adaptive ML-based anomaly detection is needed to identify subtle traffic deviations that traditional intrusion detection systems often miss (Nabi et al., 2024).

1.2 Problem statement

Despite significant advances in ML-based intrusion detection, existing studies remain fragmented across attack types, learning paradigms, datasets, and deployment contexts. DDoS and ARP spoofing detection are often investigated independently, and most proposed models are evaluated using benchmark datasets that do not adequately represent the openness, heterogeneity, BYOD activity, IoT integration, user mobility, and resource constraints of university networks. Consequently, consolidated evidence on how ML-based intrusion detection systems can jointly detect high-volume DDoS attacks and low-volume Layer-2 ARP spoofing attacks in real-world university network environments remains limited.

1.3 Contributions of this review

Existing reviews on ML-based intrusion detection often treat DDoS detection, ARP spoofing detection, IoT security, and campus network security as separate research areas. This separation limits understanding of how ML-based IDS can jointly detect high-volume DDoS attacks and low-volume Layer-2 ARP spoofing in heterogeneous university networks.

The main contributions of this review are as follows:

- The review synthesizes recent ML-based DDoS and ARP spoofing detection studies in the context of university network environments.
- The review compares supervised, unsupervised, semi-supervised, deep learning, ensemble, and hybrid IDS approaches based on detection performance, dataset realism, scalability, explainability, and deployment readiness.
- The review identifies key gaps in existing studies, including benchmark-dataset dependency, limited cross-layer detection, weak real-time validation, high computational overhead, and limited interpretability.

- (d) The review proposes a context-aware taxonomy for classifying ML-based IDS approaches by learning paradigm, attack layer, deployment mode, dataset source, evaluation focus, and explainability.
- (e) The review develops a review-derived unified framework for adaptive, real-time, and explainable ML-based IDS deployment in university networks.

1.4 Comparison with previous reviews

To further clarify the novelty of this review and the research gap addressed, [Table 1](#) compares the present review with selected existing reviews on ML-based intrusion detection. The comparison considers their focus on DDoS and ARP spoofing detection, IoT and SDN environments, university or campus networks, and the joint consideration of these attack types. This comparison highlights how the present review integrates these fragmented research areas within a unified university-network perspective.

2 Methodology

This review utilized a structured systematic literature review (SLR) approach to critically evaluate ML techniques for detecting DDoS and ARP spoofing attacks in university networks. To ensure methodological rigor, transparency, and reproducibility, the review adheres strictly to the PRISMA 2020 framework.

2.1 Research design

A non-experimental, descriptive SLR design was employed, relying exclusively on secondary data from peer-reviewed publications, online repositories, and publicly available cybersecurity datasets. The study systematically synthesizes empirical evidence on DDoS and ARP attack patterns, intrusion detection methods, and ML models applied in university and similar open network environments. Key aspects analyzed include ML techniques, dataset characteristics and realism, feature engineering, validation strategies, performance metrics, and reported limitations. Data were collected through structured searches of reputable databases, organized, coded, and examined using integrated thematic and comparative analysis to identify prevailing trends, methodological inconsistencies, and research gaps. This approach generates rigorous, evidence-based insights to inform the selection, justification, and refinement of ML-driven anomaly detection frameworks. The review protocol was not prospectively registered; this is reported transparently in accordance with PRISMA 2020 reporting requirements.

2.2 PRISMA compliance

This systematic literature review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines to ensure methodological transparency, reproducibility, and reporting quality. The study followed the four PRISMA stages: identification, screening, eligibility assessment, and study inclusion. A structured search strategy, predefined eligibility

TABLE 1 Comparison of the present review with existing reviews on ML-based intrusion detection in university networks.

Existing review	Main focus	DDoS	ARP spoofing	IoT/SDN	University/campus focus	Joint DDoS + ARP	Main limitation addressed by this review
Ahmad (2025)	ML for network anomaly detection	✓	Partial	General	X	X	Broad network focus
Salvador-Najar et al. (2025)	IDS in IoT	✓	Partial	✓	X	X	IoT-focused rather than campus-focused
Khraisat and Alazab (2021)	IDS in IoT networks	✓	Partial	✓	X	X	Does not specifically address university networks
Elbertsen et al. (2025)	ML-based IDS for critical infrastructure	✓	Partial	Partial	X	X	Critical-infrastructure focus
Mahendar and Shivakanth (2025)	IoT-enabled smart campus security	Partial	Partial	✓	✓	X	Smart-campus focus without joint ML-based DDoS/ARP analysis.
Folarin Ogunjinmi (2025)	ML/DL for DDoS detection in SDN	✓	X	✓	X	X	DDoS and SDN focused.
Present review	ML-based IDS for university networks	✓	✓	✓	✓	✓	Integrates the fragmented areas into one university-network perspective

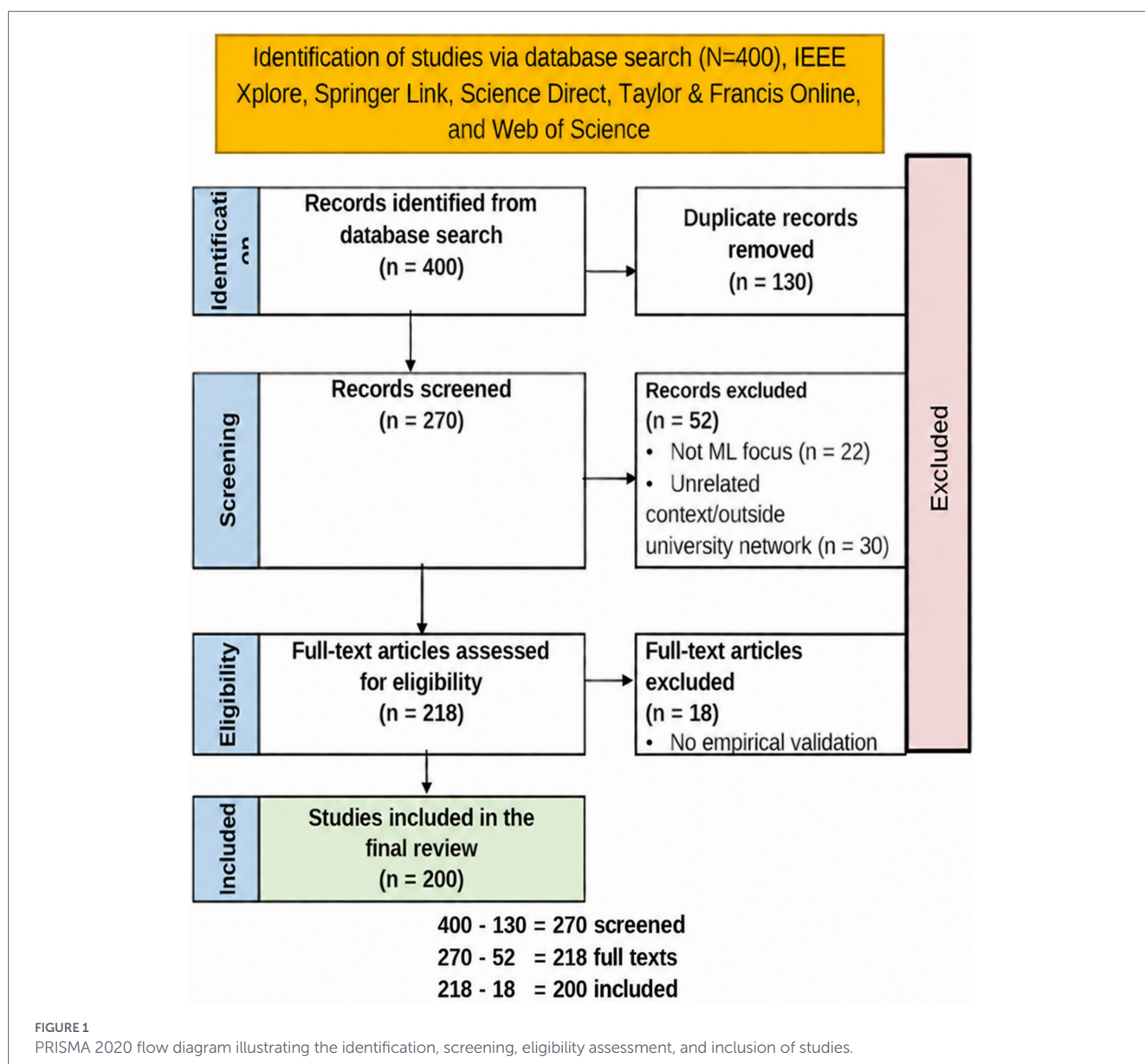
criteria, independent screening, quality assessment, and systematic data extraction were applied throughout the review. The PRISMA 2020 flow diagram illustrating the study selection process is presented in Figure 1, while the completed PRISMA 2020 Checklist is provided in Appendix A.

2.3 Search strategy

A systematic literature search was conducted in IEEE Xplore, SpringerLink, ScienceDirect, Taylor & Francis Online, and Web of Science between 1 November 2025 and 31 January 2026. The formal evidence-synthesis eligibility window covered studies published from January 2021 to January 2026 and focused on machine learning (ML)-based intrusion detection, DDoS attacks, ARP spoofing, and university network security. Database-specific search strings, Boolean operators, filters, and search dates were systematically documented to enhance the transparency and reproducibility of the review process. The search syntax was adapted to the specific requirements and functionalities of each database while maintaining consistent core

concepts, keywords, and eligibility parameters across all information sources. Searches were restricted to English-language, peer-reviewed journal articles and conference papers that met the predefined inclusion criteria. The final database search was completed on 31 January 2026 to ensure that all eligible 2021–2026 publications had been captured. Duplicate records were subsequently removed before screening.

The literature search used predefined Boolean search strings combining terms related to ML, intrusion detection, university networks, DDoS, and ARP spoofing. The main search strings were: (“Machine Learning” OR “Deep Learning”) AND (“Intrusion Detection” OR “Intrusion Detection System”) AND (“University Network” OR “Campus Network”); (“DDoS” OR “Distributed Denial-of-Service”) AND (“Machine Learning”); and (“ARP Spoofing” OR “ARP Poisoning”) AND (“Anomaly Detection”). Search syntax was adapted to the requirements of each database. Studies were eligible if they were peer-reviewed, available in full text, published in English, and reported research relevant to machine-learning-based intrusion detection, DDoS or ARP spoofing detection, or university network security.



Editorials, abstracts, conference posters, book chapters, pre-prints, duplicate records, and studies outside the scope of the review were excluded. Reference lists of the included studies were also screened to identify additional relevant publications. The complete database-specific search strategies, applied filters and limits, and dates on which the searches were conducted are presented in Table 2.

2.3.1 Inclusion and exclusion criteria

The study selection process was guided by explicit inclusion and exclusion criteria to ensure methodological relevance, empirical validity, and alignment with the review focus on ML-based intrusion detection for smart university network security. Table 3 presents the inclusion and exclusion criteria used in the study selection process.

2.4 Study screening and reviewer roles

Two reviewers independently screened all 270 non-duplicate records using the predefined eligibility criteria. Each reviewer independently assessed the titles and abstracts and recorded an inclusion or exclusion decision before the screening results were compared. Any disagreements regarding inclusion or exclusion were resolved through discussion until consensus was reached. Where consensus could not be reached, a third reviewer adjudicated the final decision.

2.4.1 Reviewer agreement

Inter-reviewer agreement was assessed for the independent screening of the 270 non-duplicate records. Both reviewers screened

the same records using the predefined eligibility criteria and recorded their inclusion or exclusion decisions independently before comparison. Agreement between the two reviewers was assessed using Cohen’s kappa (κ). Disagreements were subsequently resolved through discussion and consensus before the final inclusion decisions were made. The Inter-Reviewer Agreement for Study Screening is presented in Table 4.

Equation 1 defines observed agreement as the number of matching screening decisions divided by all decisions. Equation 2 substitutes the observed counts, Equation 3 calculates the proportion, and Equation 4 expresses it as a percentage.

Observed agreement (P_o)

$$P_o = \frac{\text{Number of agreements}}{\text{Total number of decisions}} \tag{1}$$

The reviewers agreed in two situations:

Both said include = 205.

Both said Exclude = 43.

The observed agreement is therefore:

$$P_o = \frac{205 + 43}{270} \tag{2}$$

$$P_o = \frac{248}{270} = 0.9185 \tag{3}$$

$$P_o = 0.9185 \times 100 = 91.85\% \tag{4}$$

Therefore, the observed agreement between the two reviewers was 91.85%.

Expected agreement by Chance (P_e).

TABLE 2 Database-specific search strings, filters, and search dates.

Database	Search string	Filters/limits	Search date
IEEE Xplore	("machine learning" OR "deep learning" OR "artificial intelligence") AND ("intrusion detection" OR "intrusion detection system" OR IDS) AND ("DDoS" OR "distributed denial-of-service" OR "ARP spoofing" OR "ARP poisoning") AND ("university network" OR "campus network" OR "academic network")	January 2021–January 2026; English; Journals and Conferences	1 November 2025
SpringerLink	("machine learning" OR "deep learning" OR "artificial intelligence") AND ("intrusion detection" OR "intrusion detection system") AND ("DDoS" OR "distributed denial-of-service" OR "ARP spoofing" OR "ARP poisoning") AND ("university network" OR "campus network" OR "academic network")	January 2021–January2026; English; Research Articles & Conference Papers	15 November 2025
ScienceDirect	("machine learning" OR "deep learning" OR "artificial intelligence") AND ("intrusion detection" OR "intrusion detection system") AND ("DDoS" OR "distributed denial-of-service" OR "ARP spoofing" OR "ARP poisoning") AND ("university network" OR "campus network" OR "academic network")	January 2021–January2026; English; Research Articles	1 December 2025
Taylor and Francis online	("machine learning" OR "deep learning") AND ("intrusion detection" OR "intrusion detection system") AND ("DDoS" OR "distributed denial-of-service" OR "ARP spoofing" OR "ARP poisoning") AND ("university network" OR "campus network")	January 2021–January 2026; English; Research Articles	15 December 2025
Web of science	TS = (("machine learning" OR "deep learning" OR "artificial intelligence") AND ("intrusion detection" OR "intrusion detection system") AND ("DDoS" OR "distributed denial-of-service" OR "ARP spoofing" OR "ARP poisoning") AND ("university network" OR "campus network" OR "academic network"))	January 2021–January 2026; English; Articles & Proceedings Papers	31 January 2026

TABLE 3 Inclusion and exclusion criteria for study selection.

Criterion	Inclusion criteria	Exclusion criteria
Research focus	Studies focusing on machine learning or deep learning-based intrusion detection systems for DDoS, ARP spoofing, or related network anomalies.	Studies focusing only on signature-based, rule-based, or traditional IDS approaches without ML or deep learning integration.
Application context	Studies addressing network security challenges in university, campus, IoT-driven, SDN, WBAN, or smart network environments.	Studies unrelated to university, campus, IoT, SDN, WBAN, or smart network security contexts.
Attack relevance	Studies examining DDoS, ARP spoofing, or similar anomaly-based threats relevant to smart university network security.	Studies addressing attacks or domains not directly related to DDoS, ARP spoofing, anomaly detection, or network intrusion detection.
Methodological approach	Studies presenting empirical ML/DL models, feature engineering methods, datasets, evaluation procedures, or deployment-oriented IDS approaches.	Studies lacking clear methodological details, experimental design, dataset description, or model evaluation procedure.
Performance reporting	Studies reporting validated empirical performance metrics such as accuracy, precision, recall, F1-score, detection rate, false positive rate, or related evaluation measures.	Studies without experimental validation or without clearly reported performance metrics.
Publication type	Peer-reviewed journal articles and peer-reviewed conference papers.	Preprints, review papers, opinion papers, editorials, incomplete studies, white papers, and other non-peer-reviewed works.
Language	Studies published in English.	Non-English publications.
Analytical relevance	Studies suitable for thematic analysis of models, datasets, feature engineering approaches, evaluation outcomes, strengths, limitations, and research gaps.	Studies whose scope, results, or methods do not provide sufficient evidence for synthesis in the context of smart university network security.

TABLE 4 Inter-rater agreement matrix for study screening decisions.

Reviewers	Reviewer 2: include	Reviewer 2: exclude	Total
Reviewer 1: include	205	13	218
Reviewer 1: exclude	9	43	52
Total	214	56	270

Probability that both reviewers say “Include”.

Reviewer 1 included: 218.

Reviewer 2 included: 214.

Probability that both reviewers say Exclude.

Reviewer 1 excluded: 52.

Reviewer 2 excluded: 56.

Equation 5 combines the independent Include and Exclude probabilities. Equation 6 gives the expected-agreement proportion, and Equation 7 converts it to a percentage.

The expected agreement combines the probability that both reviewers independently select Include and the probability that both independently select Exclude.

Therefore:

$$P_e = \left(\frac{218}{270} \times \frac{214}{270} \right) + \left(\frac{52}{270} \times \frac{56}{270} \right) \quad (5)$$

$$P_e = 0.6399 + 0.0399 = 0.6799 \quad (6)$$

$$P_e = 0.6799 \times 100 = 67.99\% \quad (7)$$

Therefore, the expected agreement by chance was 67.99%.

Equation 8 defines Cohen's κ from observed and chance-expected agreement. Equation 9 substitutes the calculated proportions, and Equation 10 evaluates the coefficient.

$$\kappa = \frac{P_o - P_e}{1 - P_e} \quad (8)$$

Cohen's kappa (κ)

$$\kappa = \frac{0.9185 - 0.6799}{1 - 0.6799} \quad (9)$$

$$\kappa = \frac{0.2386}{0.3201} \approx 0.745 \quad (10)$$

Thus, Cohen's κ was 0.745 (approximately 0.75), indicating substantial agreement beyond chance. Cohen's κ is reported as a coefficient, not a percentage.

The search identified 400 records, of which 130 duplicates were removed, leaving 270 records for screening. Two reviewers independently assessed these records, with substantial agreement (Cohen's $\kappa = 0.75$). 52 records were excluded during screening, including 22 that lacked a relevant ML focus and 30 that were outside the predefined scope. The remaining 218 articles underwent full-text assessment, of which 18 were excluded because they lacked sufficient empirical validation. Consequently, 200 studies were included in the final review.

2.5 Data extraction and synthesis procedure

A structured data extraction framework was employed to systematically collect key attributes from each study, including the dataset used (e.g., CIC-IDS2017, CAIDA), model type (such as SVM, RF, CNN, LSTM, and hybrid approaches), validation strategy, reported

performance metrics, and identified strengths and limitations. This standardized extraction facilitated a comprehensive comparative analysis across studies, focusing on dataset dependency, model complexity, and real-world applicability within network intrusion detection contexts. These studies constitute the core evidence base for the review titled “Enhancing University Network Security Through ML-Based Detection of DDoS and ARP Spoofing Attacks: A Systematic Review”.

2.6 Study selection process

This review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) framework to ensure transparency, reproducibility, and methodological rigor. The review process comprised identification, duplicate removal, title and abstract screening, full-text eligibility assessment, quality appraisal, and thematic synthesis. The systematic literature search identified 400 records. After removing 130 duplicate records, 270 records remained for title and abstract screening. At this screening stage, 52 records were excluded, including 22 that lacked a relevant machine learning focus and 30 that were outside the predefined study context. The remaining 218 records underwent full-text eligibility assessment, during which 18 studies were excluded because they lacked sufficient empirical validation. Consequently, 200 studies met all eligibility criteria and were included in the final review and thematic synthesis, as presented in [Figure 1](#). A completed PRISMA 2020 Checklist accompanies this manuscript as [Supplementary material](#).

2.7 Study quality assessment

Each study was assessed across four quality criteria: dataset realism, validation method, reproducibility, and risk of bias. Each criterion was scored from 0 to 2, giving a maximum quality score of 8. A minimum score of 5/8 was adopted as a pragmatic quality threshold to retain studies demonstrating acceptable methodological adequacy while accommodating heterogeneity in IDS datasets and validation settings. The threshold was used as a minimum quality criterion rather than an indication of methodological equivalence among included studies. The Study Quality Assessment Matrix for ML-Based Intrusion Detection Studies is presented in [Table 5](#).

2.7.1 Quality-score distribution

Following application of the quality assessment matrix, the distribution of quality assessment scores among the 200 included studies is presented in [Table 6](#).

Among the 200 studies retained after quality assessment, 39 (19.5%) scored 5/8, 44 (22.0%) scored 6/8, 55 (27.5%) scored 7/8, and 62 (31.0%) achieved the maximum score of 8/8. Overall, 58.5% of the studies scored 7/8 or higher, indicating generally good methodological quality. Nevertheless, methodological variation was observed in dataset realism, validation procedures, reproducibility, and risk-of-bias considerations. Studies at the minimum inclusion threshold were therefore interpreted with appropriate caution during evidence synthesis.

TABLE 5 Study quality assessment matrix for ML-based intrusion detection studies.

Criterion	Score 0	Score 1	Score 2
Dataset realism	Dataset not described	Benchmark or simulated dataset only	Benchmark plus realistic, real-world, campus, IoT, or SDN traffic
Validation method	No validation reported	Basic train-test split only	Cross-validation, time-based validation, scenario testing, or real-time validation
Reproducibility	Method unclear	Partial dataset or model details	Dataset, preprocessing, model configuration, and evaluation procedure clearly reported
Bias risk	Not addressed	Partially addressed	Handles class imbalance, overfitting, data leakage, or fair comparison

TABLE 6 Distribution of quality assessment scores among the included studies.

Quality score	Interpretation	Number of studies (n)	Percentage (%)
5/8	Acceptable	39	19.5%
6/8	Moderate good	44	22.0%
7/8	Good	55	27.5%
8/8	High	62	31.0%
Total		200	100%

2.8 Bias and validity considerations

To minimize selection bias, studies were identified using predefined search and eligibility criteria across multiple databases. Quality assessment considered dataset realism, validation strategy, reproducibility, and bias risk. However, many studies relied on benchmark datasets and simple train-test validation, which may overestimate detection performance.

3 Characteristics of included studies

Following the PRISMA-guided screening and quality assessment process, 200 peer-reviewed studies published between 2021 and 2025 were included in this review. The studies examined ML and deep learning approaches for detecting DDoS attacks, ARP spoofing, and

related network intrusions across university, IoT, SDN, WBAN, benchmark, and simulation-based environments. The reviewed approaches included supervised, unsupervised, semi-supervised, deep learning, hybrid, and ensemble models, with performance commonly evaluated using accuracy, precision, recall, F1-score, and ROC-AUC. The temporal distribution of the included studies is presented in the section below.

3.1 Real university Network studies

Of the 200 studies included in the review, 24 (12%) were classified as involving real university-network environments. These studies provide the most direct evidence of ML-based intrusion detection under operational campus conditions, where traffic is influenced by heterogeneous users and devices, BYOD practices, IoT integration, and changing network workloads (Awad et al., 2024). However, the majority of the reviewed studies were conducted using benchmark datasets, IoT environments, SDN settings, WBANs, or simulation platforms rather than operational university networks (Chaudhry et al., 2023). Therefore, findings from these controlled or specialized environments should be interpreted as evidence of algorithmic performance under specific experimental conditions and not as direct evidence of performance in real campus deployments. This distinction is important when assessing the applicability and generalizability of ML-based DDoS and ARP-spoofing detection approaches to operational university networks.

3.2 Benchmark dataset studies

Most studies evaluated intrusion detection models using publicly available benchmark datasets such as UNSW-NB15, CICIDS2017, CICDDoS2019, and NSL-KDD. These datasets constituted the largest category in the review, accounting for 96 of the 200 included studies (48%). However, benchmark performance should not be interpreted as direct evidence of effectiveness in operational university networks. Such datasets are generated or collected under specific experimental conditions and may not fully represent the heterogeneous devices, changing traffic volumes, encrypted communications, user behavior, network policies, and infrastructure configurations found on university campuses (Blessing and Klaus, 2024). Consequently, high accuracy, precision, recall, or F1-scores obtained from benchmark datasets indicate performance under the characteristics of those datasets rather than guaranteed performance after deployment in a real campus network. This distinction limits the extent to which benchmark-based findings can be generalized to operational university environments.

3.3 IoT-based studies

IoT-based studies accounted for 34 studies (17%) and primarily examined botnet activity, DDoS attacks, and anomalous traffic generated by interconnected devices. Although these studies provide useful evidence regarding ML detection of IoT-related threats, their findings should be distinguished from evidence obtained from operational university networks. Many IoT studies relied on specialized testbeds, simulated traffic, or benchmark datasets, which may not reproduce the broader traffic characteristics and

operational constraints of a university campus (Rahman et al., 2024).

3.4 SDN-based studies

SDN-based studies accounted for 20 studies (10%) and demonstrated the potential of centralized traffic monitoring and programmable network control for detecting and mitigating DDoS and ARP-spoofing attacks. However, most evaluations were conducted within SDN-specific or simulated environments rather than production university networks (Wainwright et al., 2025). Their findings therefore provide evidence of feasibility under controlled SDN conditions but should not be interpreted as equivalent to validated performance in operational campus networks.

3.5 WBAN studies

Wireless Body Area Network (WBAN) studies accounted for 8 of the 200 included studies (4%). These studies primarily focused on lightweight intrusion detection mechanisms for resource-constrained devices. Nevertheless, their findings have limited direct applicability to university network security because WBAN environments differ from campus networks in terms of communication protocols, traffic characteristics, device constraints, and deployment scenarios. Therefore, WBAN results were considered as supporting evidence on ML-based intrusion detection rather than direct evidence of performance in operational university networks. The complete distribution of the 200 included studies across real university, benchmark, IoT, SDN, WBAN, and simulation-based evaluation environments is summarized in Table 7. This cross-reference provides the quantitative context for the category-specific discussion in Sections 3.1–3.6.

3.6 Simulation-based studies

As presented in Table 7, simulation-based studies accounted for 18 of the 200 included studies (9%). These studies evaluated

TABLE 7 Distribution of included studies by evaluation environment.

Study category	Number of studies ($n = 200$)	Percentage (%)	Typical environment
Real university network	24	12	Operational campus networks
Benchmark dataset	96	48	CICIDS2017, UNSW-NB15, CICDDoS2019, etc.
IoT network	34	17	Smart campus IoT
SDN	20	10	Software-defined campus networks
WBAN	8	4	Wireless Body Area Networks
Simulation-based	18	9	NS-3, OMNeT++, Mininet, etc.

ML-based intrusion detection approaches using simulated network environments such as NS-3, OMNeT++, and Mininet (Al-Dulaimy and Frey, 2026; Patil and Shyamala, 2025). Simulation provides a controlled and repeatable environment in which researchers can generate specific attack scenarios, vary network conditions, and evaluate detection models without exposing operational networks to security risks (Solutions et al., 2022). However, simulated environments may not fully reproduce the traffic variability, device heterogeneity, user behavior, network configurations, and operational constraints of real university networks. Consequently, findings from simulation-based studies provide useful evidence of algorithmic feasibility under controlled conditions but should not be considered equivalent to evidence obtained from operational campus deployments. Further validation using real university network traffic is therefore necessary to establish practical generalizability.

3.7 Publication trends

Figure 2 illustrates the annual distribution of the 200 studies included in this review. Publications increased from 31 studies in 2021 to 50 studies in 2025, with 35, 44, and 40 studies published in 2022, 2023, and 2024, respectively. This upward trend reflects increasing research interest in ML-based intrusion detection for university network security.

3.8 Dataset characteristics and implications for generalizability

The reviewed studies employed a combination of benchmark and real-world datasets for developing and evaluating ML-based intrusion detection systems. CICIDS2017, UNSW-NB15, CICDDoS2019, and CAIDA were frequently used because they provide labeled traffic, defined attack scenarios, and standardized conditions for comparing machine-learning models. However, the characteristics of these datasets can influence the performance reported by ML models and their ability to generalize to operational university networks.

Differences in attack composition, class distribution, traffic characteristics, feature distributions, and data generation environments can affect model learning and evaluation. For example, models trained and tested on datasets containing distinctive attack patterns may achieve high performance because the malicious and benign traffic are

relatively separable. Similarly, class imbalance can make overall accuracy appear high when minority attack classes are detected less effectively. Dataset-specific feature distributions may also allow a model to learn patterns that are specific to the source dataset rather than general characteristics of network attacks. Consequently, high accuracy, precision, recall, or F1-score on a benchmark dataset does not necessarily demonstrate equivalent performance on an unseen network environment.

This limitation is particularly important for university networks, which are characterized by heterogeneous devices, BYOD connections, IoT deployments, user mobility, encrypted traffic, and changing academic and administrative workloads. Such characteristics can produce traffic distributions that differ substantially from those represented in controlled or benchmark datasets. The reviewed evidence therefore suggests that benchmark-based results are valuable for standardized model comparison but should not be interpreted as direct evidence of deployment readiness or generalization to operational university networks. Cross-dataset validation, time-based evaluation, laboratory-generated traffic, and testing using real university network traffic can provide stronger evidence of generalizability. The Characteristics of Benchmark Datasets used is presented in Table 8.

4 Threat landscape in university networks

The growing adoption of IoT devices on university campuses faces various cybersecurity risks, with DDoS attacks and ARP spoofing being among the most persistent and disruptive (Bandara et al., 2021). These threats exploit structural weaknesses in open, high-capacity campus networks. DDoS attacks inundate critical academic services such as authentication systems, learning platforms, and data centers with malicious traffic, leading to severe performance degradation or complete outages, often masking secondary intrusions (Ouhssini et al., 2024).

Meanwhile, ARP-based threats, including ARP poisoning and spoofing, take advantage of the lack of authentication in ARP mechanisms to intercept or redirect traffic, resulting in credential theft, session hijacking, and the injection of malicious packets. A recent study (Ain et al., 2025) notes that these risks are heightened in dynamic university environments where unmanaged student devices, IoT sensors, and laboratory systems operate with minimal segmentation. Together, DDoS and ARP-based threats expose significant gaps in university network security, highlighting the limitations of static, signature-based intrusion detection systems. There is an urgent need for more adaptive, ML-driven anomaly detection approaches that can identify subtle traffic irregularities in real time and respond to evolving threats (Dulstrud and Bygstad, 2022).

4.1 DDoS attacks in university networks

DDoS attacks threaten university networks by targeting system availability, a core aspect of cybersecurity, by overwhelming servers with malicious traffic. DDoS attacks render essential services like learning platforms and online registration unreachable (Singh and Gupta, 2022). Universities are vulnerable due to their open-access design, high bandwidth, and diverse user base (Singun, 2025).

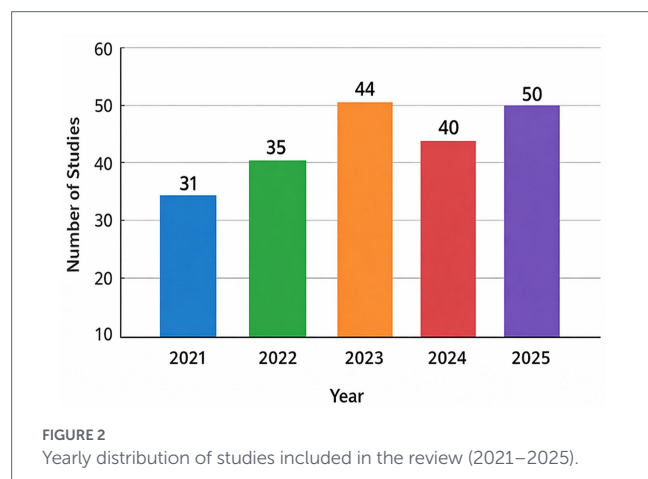


TABLE 8 Characteristics of benchmark datasets used in the reviewed literature.

Dataset	Primary focus	Typical attacks	Common use	Implication for generalizability
CICIDS2017	General IDS	DDoS, DoS, Brute Force, Botnet	ML/DL IDS evaluation	Useful for comparison, but may not represent heterogeneous campus traffic
UNSW-NB15	Modern network attacks	Exploits, DoS, Reconnaissance, Generic	General intrusion detection	Provides diverse attacks, but traffic characteristics may differ from operational university networks.
CICDDoS2019	DDoS	Reflection and amplification attacks	DDoS detection	Useful for DDoS evaluation, but focused attack coverage limits broader campus generalization.
CAIDA	Backbone traffic	Large-scale DDoS	Traffic analysis and anomaly detection	Useful for large-scale traffic analysis but differs from typical campus traffic.

Misconfigured personal devices and expanding IoT ecosystems increase risk, as compromised endpoints can be used in botnets that attack the university and contribute to global DDoS activity.

DDoS incidents in universities occur through volumetric, protocol-based, or application layer attacks, exploiting weaknesses in bandwidth, protocol handling, or service functionality. These attacks disrupt online teaching, examinations, and administrative operations, and the rise of insecure IoT devices on campus, such as surveillance systems and sensors, has intensified this threat, evidenced by large-scale IoT-driven botnets like Mirai (Hirsi and Member, 2025). Given the increasing sophistication and frequency of DDoS attacks, universities need advanced ML detection mechanisms to identify anomalous traffic patterns early and prevent them from being attacked, thus maintaining operational continuity.

4.2 ARP spoofing and Layer-2 threats

ARP-based attacks, particularly ARP poisoning and ARP spoofing, pose a significant threat to university networks by exploiting the lack of authentication within the Address Resolution Protocol (Tas, 2025). By forging ARP messages that corrupt IP-MAC associations, attackers can redirect or intercept traffic, enabling man-in-the-middle attacks within local network segments. University environments are particularly vulnerable due to their open-access design, frequent device mobility, shared broadcast domains, and extensive use of Layer-2 Ethernet switching (Wind et al., 2024). The presence of unmanaged student devices each running different operating systems creates an expanded attack surface, allowing even minimally skilled attackers to deploy ARP spoofing tools that compromise sensitive communications. Once ARP tables are poisoned, attackers can harvest credentials, hijack sessions, or inject malicious payloads into network traffic, often without detection.

4.3 Smart campus and IoT security challenges

Universities increasingly rely on smart campus technologies and IoT devices to support teaching, research, campus administration,

and security (Elbertsen et al., 2025). Smart surveillance cameras, biometric systems, intelligent lighting, digital door locks, HVAC controllers, and sensor-based laboratory equipment have improved operational efficiency but also expanded the university attack surface (Isong et al., 2024). Many IoT devices have limited processing power, outdated firmware, default credentials, and weak communication security, making them attractive targets for cyberattacks (Čekerevac et al., 2025; Ali G. et al., 2025).

Conventional signature-based intrusion detection systems primarily detect previously known attack signatures and are less effective against evolving or zero-day threats (Ahmed et al., 2025). In contrast, machine learning models learn normal and malicious traffic patterns from data, enabling adaptive detection of both known and previously unseen attacks. This capability makes ML particularly suitable for university networks characterized by heterogeneous devices, BYOD, IoT integration, and dynamic traffic patterns (Pinto et al., 2023).

Attackers frequently exploit these vulnerabilities to compromise IoT devices and recruit them into botnets capable of launching large-scale DDoS attacks or conducting ARP spoofing by manipulating MAC-IP mappings (Domínguez-Bolaño et al., 2024; Hussien et al., 2024). The open and heterogeneous nature of university networks, together with BYOD practices and limited cybersecurity resources, further complicates threat detection and mitigation (Vajrobol et al., 2025). Consequently, traditional signature-based intrusion detection systems are increasingly inadequate, highlighting the need for adaptive ML-based anomaly detection capable of identifying subtle and evolving attack patterns in smart campus environments (Zou et al., 2025; Chee et al., 2025).

4.4 Detection challenges in university networks

Universities face significant challenges in detecting and mitigating DDoS and ARP-based attacks due to the scale, openness, and heterogeneity of their network environments (Kumar M. A. et al., 2024). Large campus networks generate high traffic volumes from thousands of users and devices, making real-time monitoring difficult. Legitimate high-bandwidth activities, such as virtual learning, research computing, software updates, and large file transfers, can resemble malicious traffic, allowing DDoS and

ARP-based attacks to remain concealed within normal network operations (Ogogo, 2021). Furthermore, legacy network infrastructure often limits the deployment of advanced security mechanisms, such as dynamic ARP inspection and flow-based anomaly detection, leaving Layer 2 traffic particularly vulnerable (Morsy and Nashat, 2022).

These challenges are compounded by limited cybersecurity resources, heterogeneous devices, and open-access network architectures. Consequently, traditional intrusion detection systems often struggle to detect evolving DDoS attacks and Layer 2 ARP spoofing (Devabhakthini et al., 2023). These limitations highlight the need for adaptive, ML-driven anomaly detection frameworks capable of learning normal network behavior, detecting real-time anomalies, and improving resilience against complex cyber threats (Uddin et al., 2024).

4.5 Methodological risks affecting reported ML performance

To assess whether the performance reported across the reviewed studies may have been affected by methodological factors, the included studies were examined for three important risks: overfitting, data leakage, and class imbalance. These factors were considered during the evidence synthesis because they can produce overly optimistic estimates of model performance, particularly when evaluation procedures do not adequately separate training and testing data (Ramos et al., 2026).

Overfitting was assessed by examining whether studies used appropriate validation procedures, such as independent test sets, cross-validation, regularization, or comparison of training and testing performance. Studies reporting very high performance without clear validation procedures were treated cautiously because such results may reflect memorization of the training data rather than genuine generalization (Lopez et al., 2025).

Data leakage was assessed by examining whether information from the test set or future observations could have influenced model training or preprocessing. Particular attention was given to feature selection, normalization, resampling, and train-test splitting procedures. Studies in which preprocessing or feature selection was performed before data partitioning, or where test information was incorporated into model development, were considered at higher risk of performance inflation (Starcke et al., 2025).

Class imbalance was assessed by examining the class distribution and whether studies used appropriate measures or techniques to address unequal class representation. These included resampling, class weighting, synthetic sampling, stratified validation, and imbalance-sensitive metrics such as precision, recall, F1-score, and macro-averaged F1-score. Accuracy results were therefore interpreted cautiously where minority attack classes were substantially underrepresented (Carvalho et al., 2025).

These methodological risks were considered when interpreting the reported performance of machine-learning models. Consequently, high accuracy or F1-scores were not treated as evidence of superiority by themselves. Greater confidence was placed in studies that used independent testing, leakage-controlled preprocessing, appropriate handling of class imbalance, and

TABLE 9 Quantitative assessment of methodological risks across the included studies.

Methodological risk	Number of studies (n = 200)	Percentage (%)
Evidence of overfitting risk	36	18%
Evidence of data leakage risk	24	12%
Substantial class-imbalance risk	72	36%
Total included studies	200	100%

evaluation metrics that reflected performance across both majority and minority attack classes. The quantitative distribution of these methodological risks across the 200 included studies is presented in Table 9.

5 ML approaches for intrusion detection

DDoS attacks and ARP spoofing remain major threats to university networks because they compromise service availability and Layer-2 communication integrity, respectively (Adedeji and Abumahfouz, 2023). The dynamic nature of university environments, characterized by BYOD devices, IoT systems, user mobility, and heterogeneous traffic, limits the effectiveness of traditional signature- and rule-based intrusion detection systems (Dehkordi et al., 2025).

ML has emerged as an effective approach for intrusion detection by learning traffic patterns and identifying both known and previously unseen attacks (Majumder et al., 2025; Syahputra and Wibowo, 2023). Supervised models, including SVM, Random Forest, KNN, and Decision Trees, achieve high detection performance for known attacks using labeled datasets such as CICIDS2017 and CICDDoS2019 (Salvador-najar et al., 2025; Wang et al., 2025). In contrast, unsupervised, semi-supervised, deep learning, and hybrid models improve adaptability by detecting unknown anomalies, including ARP spoofing and evolving DDoS attacks, through behavioral and traffic pattern analysis (Agrawal et al., 2024; Yunita et al., 2025; Sinha et al., 2025). These advances highlight the need for adaptive, real-time, and deployment-aware ML-based IDS for university networks.

5.1 Traditional intrusion detection system

Traditional IDS, such as signature-based, rule-based, network-based, host-based, and early anomaly-based approaches, have long been used to protect computer networks. However, their effectiveness is limited in dynamic university environments characterized by BYOD devices, IoT systems, cloud services, and highly variable network traffic (Engineering, 2025). Signature- and rule-based IDS primarily detect known attacks using predefined patterns, making them ineffective against zero-day attacks, evolving DDoS variants, and stealthy ARP spoofing (N. Security, 2025; Mahendar and Shivakanth, 2025).

Network- and host-based IDS also face deployment challenges in heterogeneous campus environments due to unmanaged devices,

limited endpoint coverage, and resource constraints (Ghazi, 2024). Furthermore, traditional anomaly-based IDS often generate high false-positive rates because they cannot continuously adapt to changing traffic patterns (Khraisat and Alazab, 2021; Ramos et al., 2026; Ahmed et al., 2025). These limitations highlight the need for ML-based intrusion detection systems capable of learning normal network behavior, adapting to evolving threats, and detecting DDoS and ARP spoofing attacks in real time.

5.2 Limitations of conventional intrusion detection systems

Traditional IDS are ineffective in university networks because they are not designed for the dynamic, heterogeneous, and open-access nature of campus environments (Kumar M. A. et al., 2024; Ogogo, 2021). The widespread use of BYOD devices, IoT systems, diverse operating systems, and rapidly changing traffic patterns limits the effectiveness of signature-, rule-, and conventional anomaly-based IDS (Alhulayyil et al., 2024; Quffa and Abu-Naser, 2025; Alfrieht et al., 2024). Operational challenges, including limited cybersecurity resources, legacy infrastructure, encrypted traffic, and the need for continuous signature and rule updates, further reduce detection performance at scale (Singh and Gupta, 2022; Casteleijn and Franzsen, 2024; Papadogiannaki and Ioannidis, 2021). Consequently, traditional IDS struggle to detect low-rate DDoS attacks, ARP spoofing, botnet activity, and multi-stage intrusions that blend with legitimate academic traffic (Rizwan et al., 2025; Anagnostopoulos et al., 2021). These limitations highlight the need for ML-based anomaly detection capable of learning normal network behavior, adapting to evolving threats, and supporting real-time intrusion detection.

5.3 Supervised ML algorithms for intrusion detection

Supervised learning is widely used in intrusion detection because it classifies network traffic as benign or malicious using labeled datasets (Ali Z. et al., 2025). Common algorithms include Decision Trees, Random Forest, Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Naïve Bayes, each offering different trade-offs in terms of accuracy, scalability, interpretability, and computational cost (Rahman et al., 2024). These models achieve high detection performance for known attacks but depend heavily on large, accurately labeled datasets.

Despite their effectiveness, supervised models have limited adaptability to unknown or evolving attacks and require continuous data labeling, which is costly and impractical in dynamic university networks (Shyaa et al., 2024; Merkurjev et al., 2024). These limitations have encouraged the adoption of unsupervised learning techniques for detecting previously unseen anomalies (Han et al., 2025).

5.4 Unsupervised ML for anomaly detection

Unsupervised learning is well suited to university networks because it detects anomalies without requiring labeled data, making it effective for identifying unknown DDoS and ARP spoofing attacks (Gupta and Tripathy, 2024). Techniques such as K-Means, DBSCAN, Isolation Forest, and PCA detect deviations from normal traffic and are widely applied in heterogeneous environments with IoT devices,

BYOD, and dynamic network traffic (Zeinalpour and Ahmed, 2022; Wororomi et al., 2023).

However, unsupervised methods are sensitive to parameter selection, unstable in dynamic environments, and prone to false positives (Sharma A. et al., 2024). These limitations have driven the development of hybrid and adaptive frameworks that combine multiple techniques to improve detection accuracy, robustness, and real-time performance in university networks (Ennaji et al., 2025).

5.5 Semi-supervised ML

Semi-supervised learning bridges the gap between supervised and unsupervised paradigms by leveraging limited labeled datasets alongside large volumes of unlabeled network traffic. This approach is particularly well-suited for academic environments, where obtaining comprehensive attack labels is inherently challenging (Jalal and Elmaghraby, 2025). In university networks, it enables the detection of anomalous deviations without relying on exhaustive prior knowledge of attack signatures (Hu et al., 2026). However, its practical effectiveness is constrained by several factors, such as sensitivity to noisy benign data, difficulty in distinguishing subtle anomalies from legitimate traffic variations, and degraded performance in highly dynamic, multi-device campus environments (Tariq et al., 2024). These limitations reduce its reliability in large-scale, heterogeneous network infrastructures (Folarin Ogunjinmi, 2025). To address these challenges, the proposed ML-based anomaly detection framework integrates semi-supervised learning with adaptive feature selection and continuous behavioral profiling (Kornaros, 2022). This hybrid approach enhances the precise detection of threats such as ARP spoofing and early-stage DDoS attacks, while improving model robustness, minimizing false positives, and strengthening overall intrusion detection performance across complex university network ecosystems (Kandasamy and Roseline, 2025).

5.6 Deep learning techniques

Deep learning has enhanced intrusion detection by learning complex spatial and temporal traffic patterns that are difficult for traditional ML models to capture (Dhrir et al., 2025). CNNs effectively detect spatial features associated with DDoS and ARP spoofing, while LSTMs and GRUs model temporal traffic behavior to identify evolving and persistent attacks (Ahmad, 2025). Hybrid architectures, such as CNN-LSTM and CNN-GRU, further improve detection accuracy and adaptability in heterogeneous university network environments (Mohsin et al., 2025).

Despite their high detection performance, deep learning models require large labeled datasets, high computational resources, and GPU-enabled hardware, limiting their deployment in resource-constrained university networks (Mohammad et al., 2024). These limitations highlight the need for computationally efficient and deployment-aware ML frameworks that balance detection accuracy with real-time operational requirements.

5.7 Hybrid and ensemble ML approaches

Hybrid and ensemble ML approaches are increasingly applied to university intrusion detection because different algorithms can

capture different characteristics of network traffic. Ensemble models such as Random Forest, boosting-based classifiers, and Isolation Forest combine multiple decision patterns, while hybrid architectures may integrate supervised, unsupervised, and deep learning techniques to address different types of network anomalies (Wang et al., 2026).

In university networks, these approaches may be useful because DDoS attacks can generate high-volume traffic anomalies, whereas ARP spoofing may involve more subtle Layer-2 behavioral changes (Soori et al., 2023). Several reviewed studies report high detection performance using hybrid and ensemble approaches (Polat et al., 2026). However, these results should be interpreted cautiously because the studies differ in datasets, attack scenarios, validation procedures, feature sets, and experimental environments. Therefore, the existing evidence does not establish that hybrid and ensemble models are universally superior to standalone approaches. Instead, their effectiveness should be assessed under consistent experimental conditions and through validation on independent operational data.

5.8 Justification of ML algorithms

The selection of appropriate ML algorithms for anomaly detection in university networks is primarily driven by the complexity, scale, and dynamic nature of campus traffic patterns (Soori et al., 2023). University environments exhibit high user diversity, fluctuating usage behaviors, extensive BYOD integration, and a heterogeneous mix of legacy systems and IoT devices, resulting in highly non-linear and unpredictable network conditions. Traditional rule-based and signature-based intrusion detection systems are ineffective in such environments because they lack adaptability and cannot identify previously unseen attack patterns (Bzai et al., 2022).

As noted by (Chen et al., 2025), ML algorithms such as Random Forest, SVM, Isolation Forest, and deep learning architectures like CNN and LSTM provide robust capabilities for detecting both known and unknown anomalies through pattern recognition and behavioral modeling. These algorithms can capture complex feature interactions, temporal dependencies, and subtle deviations in traffic behavior that often precede or accompany malicious activities like DDoS attacks and ARP spoofing. Moreover, ensemble and unsupervised learning techniques are particularly well-suited for this context due to their resilience to noisy data, reduced reliance on labeled datasets, and high generalization ability in real-world deployments (Vetrivel et al., 2024).

Thus, the integration of these ML algorithms is strategically justified, as they offer the enhanced accuracy, scalability, and adaptability necessary to effectively detect and prevent evolving network threats within university environments.

5.9 Comparison of ML algorithms for university Network security

The reviewed studies show that supervised, deep learning, hybrid, and ensemble models achieve strong detection performance across benchmark, IoT, SDN, and simulated environments. However, most evaluations rely on benchmark datasets, with limited cross-dataset validation, real-time testing, and deployment in heterogeneous university networks (Wang et al., 2021). Models

demonstrating high offline accuracy may therefore generalize poorly to operational environments characterized by BYOD devices, IoT diversity, user mobility, and dynamic traffic (Ortiz-Ruiz et al., 2024).

The comparison also highlights trade-offs among ML approaches. Classical ML models offer practical and efficient detection but have limited adaptability to evolving attacks, whereas deep learning and hybrid models improve detection accuracy at the expense of higher computational requirements (Almuhanna and Dardouri, 2025). These findings highlight the need for adaptive, explainable, and computationally efficient IDS frameworks capable of detecting DDoS and ARP spoofing across multiple network layers (Das et al., 2019). Table 10 summarizes representative studies from the formal 2021–2026 evidence synthesis together with selected 2026 publications presented separately as post-search contextual literature.

The 2026 studies presented in Table 10 were identified after the predefined January 2021–January 2026 eligibility period. They are included solely as post-search contextual literature to reflect recent developments in ML-based DDoS and ARP spoofing detection. They were not included in the 200 studies used for the PRISMA screening counts, quantitative distributions, or formal evidence synthesis.

6 Security frameworks for smart university networks

University networks require comprehensive security frameworks to protect heterogeneous infrastructures comprising BYOD devices, IoT systems, cloud services, and legacy network resources. Frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, ISO/IEC 30141, ETSI EN 303645, and ENISA provide guidance for risk management, access control, incident response, continuous monitoring, and IoT security governance (Mishra et al., 2025; Paper, 2022). These frameworks strengthen the overall security posture of smart university networks but primarily define governance and baseline security controls rather than intelligent threat detection.

6.1 Security standards and frameworks

Standard security frameworks establish policies and best practices for protecting university networks, but they do not independently detect evolving cyber threats such as DDoS attacks and ARP spoofing (ENISA, 2024). Consequently, these frameworks should be complemented by ML-based intrusion detection systems, which provide adaptive, real-time detection of abnormal network behavior and improve cyber resilience in dynamic university environments (Shuiling et al., 2025; Syahputra and Wibowo, 2023; Aziz Al Kabir et al., 2023).

6.2 Integration with ML-based intrusion detection systems

Machine learning-based intrusion detection systems enhance existing security frameworks by providing adaptive and real-time threat detection. While frameworks such as NIST, ISO/IEC 27001,

TABLE 10 Comparative analysis of included studies and selected post-search contextual literature on DDoS and ARP spoofing detection.

Year	Approach	Dataset type	Dataset/ environment	Attack scenario	Validation method	Evaluation metrics	Actual reported performance
2021	RF, KNN, SVM, DT, NB, ANN, LR (Churcher et al., 2021)	Benchmark	BoT-IoT	HTTP DDoS	Experimental evaluation	Accuracy, Precision, Recall, F1, Log Loss	RF: 99% accuracy for HTTP DDoS; KNN: 99% in multiclass classification
2021	LR, NB, SVM, KNN, DT, RF, LSTM, CNN-SVM (Maseer et al., 2021)	Benchmark	CICIDS2017	DDoS and other attacks	Experimental evaluation	Precision, Recall, F1	RF F1: 98.59% for Botnet; 98.62% for DDoS; LSTM F1: 98.93% for DDoS
2023	CNN-LSTM hybrid (Ahuja et al., 2022)	Experimental/SDN	SDN/ARP traffic environment	ARP spoofing	Experimental evaluation	Accuracy, Precision, Recall, F1	99.73% accuracy
2023	LSTM/adversarial neural network (Mustapha et al., 2023)	Experimental	Regular and adversarial DDoS traffic	DDoS	Adversarial testing	Detection ratio	91.75–100% detection ratio
2024	RF, KNN, SVM, DT, LSTM, MLP, GRU (Putra et al., 2024)	Benchmark	UNSW-NB15	DDoS	Experimental evaluation	Accuracy, Precision, Recall, F1	RF: 97.68% accuracy
2024	Feature selection + ML/RF (Han et al., 2024)	Benchmark	CICIDS2017, CICIDS2018, InSDN	DDoS	Experimental evaluation	Accuracy, Precision, Recall, F1	RF: 99.98% on CICIDS2017; 100% on CICIDS2018
2024	Neural Network (24–106-5) (Tymoshchuk et al., 2024)	Benchmark + laboratory	Normal and DDoS traffic	SYN, ACK, HTTP, and UDP flooding	Dataset evaluation + laboratory validation	Accuracy, Precision, Recall, F1	99.35% accuracy on dataset; 95.05% accuracy in laboratory validation; Precision 99.32%, Recall 99.54%, F1 99%
2024	RF, LSTM, CNN, SVM, Isolation Forest (Kumar and Dash, 2024)	Experimental/real-time	ARP traffic environment	ARP spoofing	Experimental evaluation	Accuracy, Precision, Recall, F1, FPR, FNR	RF $\approx$ 94% accuracy
2025	Random Forest, Logistic Regression, Naïve Bayes (Nawaz et al., 2025)	Benchmark	NSL-KDD	DDoS	10-fold cross-validation	Accuracy, Precision, Recall, F1	RF: 99.88% accuracy; 99.93% precision; 99.81% recall; 99.87% F1
2025	DT, RF, Gradient Boosting, XGBoost, RNN, Isolation Forest (Alturki and Alsulami, 2025)	Benchmark/IoMT	CICIoMT2024	ARP spoofing	Experimental evaluation	Accuracy, Precision, Recall, F1	RF: 97% accuracy
2025	Hybrid DT + ensemble + DL (Ali A. et al., 2025)	IoT + benchmark	Simulated IoT traffic + CICIDS2017	ARP spoofing	Simulation + dataset validation	Detection accuracy, FPR	>97% detection accuracy

(Continued)

TABLE 10 (Continued)

Year	Approach	Dataset type	Dataset/ environment	Attack scenario	Validation method	Evaluation metrics	Actual reported performance
2025	Multi-layer ML + ensemble/ DT (El-Sayed et al., 2025)	IoT/benchmark	CICIDS2017 + simulated IoT traffic	ARP spoofing	Simulation + dataset validation	Detection accuracy	>97% detection accuracy
2026	LightGBM, XGBoost, RF, and other ML classifiers (Almomani et al., 2026)	IoT benchmark	IoTID20	ARP spoofing/ MITM	Train-test split	Accuracy, Precision, Recall, F1	LightGBM: 99.7% across all four metrics
2026	P4 + ML ensemble (DiMCA) (Sharma and Rani, 2025)	IoT/SDN	CICIoMT2024 + IoT datasets	ARP spoofing/ DDoS/hybrid attacks	Experimental evaluation	Accuracy, F1	99.22% accuracy; 99.76% F1
2026	Cost-sensitive Random Forest (Singhal and Kumar, 2026)	IoMT benchmark	CICIoMT2024	ARP spoofing	Three-way train/ validation/test	Accuracy, Precision, Recall, F1	99.90% accuracy; 99.95% precision; 99.83% recall; 99.89% F1

and ENISA establish security governance and incident response guidelines, ML-based IDS enable continuous traffic monitoring, anomaly detection, and automated attack identification. This integration is particularly important in university networks, where BYOD, IoT devices, and dynamic traffic patterns increase exposure to DDoS and ARP spoofing attacks. Consequently, combining established security frameworks with ML-based IDS strengthens network resilience and improves the detection of both known and emerging cyber threats.

7 Evidence synthesis and comparative review findings

The reviewed studies consistently identify DDoS and ARP spoofing as major security threats in university networks because of their scalability, stealth, and potential to disrupt service availability and communication integrity. Among the 200 studies included in this review, the majority focused on DDoS and ARP spoofing detection, highlighting their prominence in university network security research. Reported detection accuracies generally exceeded 90% across benchmark and real-world datasets, although these results should be interpreted cautiously because many studies relied on benchmark datasets and limited validation strategies (Hirsi et al., 2025).

Evaluations of supervised ML using benchmark datasets like CIC-IDS2017 and CIC-DDoS2019 show high detection performance. However, these results should be interpreted with caution because most studies relied on benchmark datasets, and the reported high accuracy may be influenced by overfitting, data leakage, class

imbalance, or limited validation (Diro et al., 2024). Consequently, cross-dataset evaluation, cross-validation, and real-world testing are needed to improve model generalizability. In contrast, ARP spoofing operates at Layer 2, producing low-volume but high-impact anomalies that often bypass traditional intrusion detection systems. Nevertheless, CNN-LSTM and ensemble models consistently demonstrate strong behavior-based detection capabilities.

The open-access architecture of university networks, along with extensive BYOD practices and accelerated IoT integration, expands the institutional attack surface. Many connected endpoints on campuses remain unmanaged and often lack baseline security controls. IoT-driven botnet propagation significantly amplifies DDoS traffic intensity; these factors increase susceptibility to ARP attacks, as shared broadcast domains, high device mobility, and dynamic IP allocation contribute to irregular MAC–IP binding patterns and increased ARP request frequencies. Such anomalies are more effectively captured through unsupervised and semi-supervised ML than through signature-based detection, highlighting the limitations of conventional intrusion detection systems (Paes et al., 2025).

Experimental investigations show that traditional intrusion detection frameworks have limited adaptability in dynamic academic environments, often producing high false-positive and false-negative rates with low-rate DDoS and ARP spoofing. Host-based IDS solutions face scalability and deployment issues in heterogeneous BYOD and IoT ecosystems, making widespread implementation impractical (Hnamte and Hussain, 2024).

ML-driven IDS architectures, especially hybrid and ensemble configurations, demonstrate high detection performance, lower false alarm rates, and near real-time inference with minimal latency. These systems are validated using robust evaluation

metrics, such as F1-score, MCC, AUC, and the Receiver Operating Characteristic. Despite these strengths, empirical evidence indicates a gap in integrated, adaptive detection models capable of simultaneously addressing Layer 2 and higher-layer attacks in real-world campus environments, reinforcing the need for a context-aware ML-driven anomaly detection framework tailored to university networks (Villegas-Ch et al., 2024).

7.1 Evidence on DDoS detection performance

The reviewed studies show that DDoS detection has received substantial attention in ML-based intrusion detection research because of its direct impact on service availability, network performance, and institutional continuity (Ahmed et al., 2025). DDoS attacks are commonly identified through flow-level and packet-level indicators such as abnormal packet rates, traffic-volume deviations, flow-duration changes, connection-frequency spikes, protocol irregularities, source-destination distribution anomalies, and sudden throughput degradation. These indicators allow ML models to distinguish between legitimate high-volume traffic and malicious traffic floods.

Supervised and ensemble models are frequently reported as effective for DDoS detection, particularly when trained on labeled benchmark datasets such as CIC-IDS2017, CIC-DDoS2019, CAIDA, and related IoT traffic datasets (Vermesan and Friess, 2022). Random Forest, Decision Tree variants, SVM, KNN, and boosting-based classifiers often demonstrate strong performance in known attack classification because they can learn structured traffic patterns and separate malicious flows from benign communication. Deep learning models, including CNN, LSTM, GRU, and CNN-LSTM architectures, extend this capability by learning spatial and temporal traffic representations, making them relevant for detecting high-rate, low-rate, and evolving DDoS behaviors (Abiramasundari and Ramaswamy, 2025).

Despite these promising results, DDoS detection performance remains strongly influenced by dataset realism and validation design. In university networks, legitimate activities such as online examinations, virtual lectures, software updates, cloud-service access, research data transfers, and peak registration periods may generate traffic bursts that resemble DDoS behavior. Models evaluated only under static benchmark conditions may therefore overestimate operational effectiveness (Rose et al., 2021). A reliable DDoS detection framework for university networks should be assessed using classification metrics such as precision, recall, F1-score, MCC, and ROC-AUC, together with operational metrics such as false positive rate, false negative rate, detection latency, throughput, and computational overhead (Mahar et al., 2026).

7.2 Evidence on ARP spoofing detection performance

The reviewed evidence shows that ARP spoofing detection remains less extensively developed than DDoS detection, although it is highly relevant to university network security. ARP spoofing operates at Layer 2 by manipulating MAC-IP address mappings within local network segments. Unlike DDoS attacks, which often produce

visible traffic surges, ARP spoofing may generate low-volume but high-impact anomalies that support man-in-the-middle attacks, credential interception, session hijacking, traffic redirection, and lateral movement (El-Sayed et al., 2025).

The evidence also shows that many ARP spoofing studies treat the attack as an isolated Layer-2 problem rather than integrating it into broader multi-layer IDS architectures. This creates a limitation for university networks, where shared broadcast domains, unmanaged student devices, IoT endpoints, mobile users, and weak segmentation increase exposure to local network manipulation (Ali A. et al., 2025). A stronger research direction is to integrate ARP spoofing detection with higher-layer anomaly detection so that university IDS architectures can provide cross-layer situational awareness.

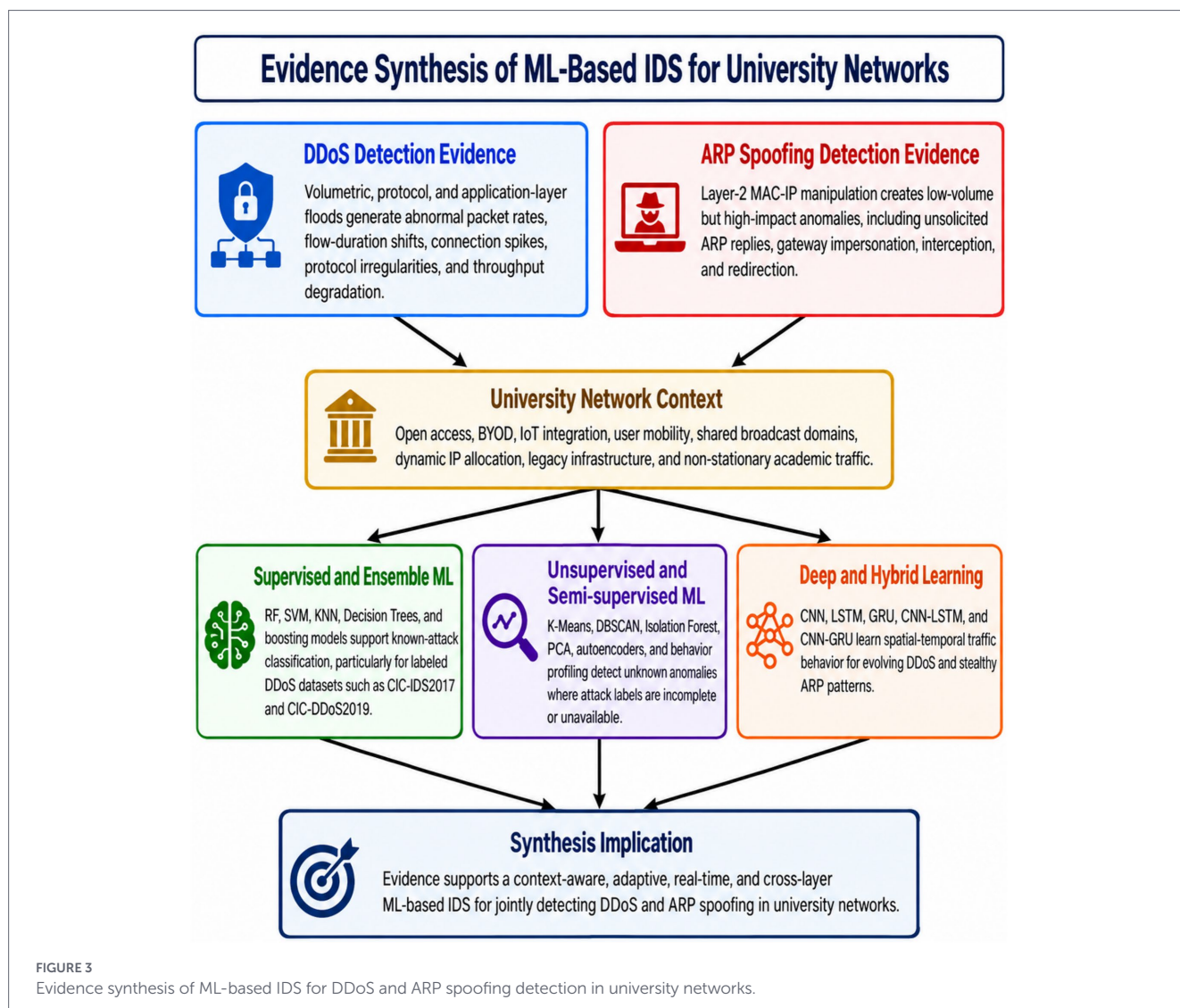
7.3 Comparative insights across ML and DL models

The reviewed studies demonstrate that supervised ML, deep learning, hybrid, and ensemble approaches can achieve high detection performance across different network security datasets and environments. However, direct comparison of the reported results is difficult because the studies use different datasets, attack scenarios, feature representations, validation procedures, and evaluation metrics. Consequently, a higher reported accuracy in one study does not necessarily indicate that the corresponding model would perform better under another experimental or operational environment (Sebestyen et al., 2025).

Hybrid and ensemble approaches therefore appear promising for addressing the complexity of heterogeneous network traffic, but their reported advantages should not be interpreted as universal superiority. Further empirical evaluation under a common experimental framework, followed by testing on independent operational data, is necessary to determine whether combining models provides consistent improvements in detection performance and generalization (Rueda-Rueda and Portocarrero, 2021).

Deep learning models provide stronger feature-learning capacity by modeling complex spatial, temporal, and sequential traffic patterns. CNN-based models are useful for extracting spatial relationships from packet-level and flow-level features, while LSTM and GRU architectures are more suitable for temporal traffic analysis. Hybrid CNN-LSTM and CNN-GRU architectures are particularly relevant where DDoS traffic bursts and stealthy ARP spoofing patterns must be analyzed across time. Their deployment, however, may be constrained by training-data requirements, computational cost, hardware dependency, energy consumption, and model maintenance demands (Alsulami et al., 2023).

The comparative evidence supports hybrid and ensemble-based IDS architectures rather than reliance on a single algorithmic family. Supervised models strengthen known attack classification, unsupervised and semi-supervised models support unknown anomaly detection, deep learning captures spatial-temporal traffic behavior, and ensemble methods improve robustness through model diversity. This combination is more suitable for dynamic university networks than isolated single-model approaches, as depicted in Figure 3.



8 Discussion

The reviewed evidence confirms that ML-based IDS offer stronger adaptability than traditional signature- and rule-based systems in university networks, where BYOD, IoT, cloud services, and user mobility create highly variable traffic patterns. However, most existing studies are fragmented, often treating DDoS and ARP spoofing as separate problems despite their shared relevance in the campus threat environment (Parmar and Miles, 2024; Eric and Juncut, 2022).

A major implication is that university IDS design should move toward cross-layer detection. DDoS attacks generate high-volume anomalies across network, transport, and application layers, while ARP spoofing produces low-volume Layer-2 behavioral deviations. A unified IDS framework is therefore required to correlate flow-level, packet-level, and MAC-IP mapping anomalies (Vemuri et al., 2024).

Although supervised, deep learning, ensemble, and hybrid models report high detection accuracy, their practical validity remains limited by dependence on benchmark datasets. Datasets such as CIC-IDS2017, CIC-DDoS2019, and CAIDA support reproducibility but do not fully capture campus-specific traffic variability,

BYOD behavior, IoT density, encrypted traffic, and academic workload changes. Consequently, high offline accuracy may not indicate real-time deployment readiness (Vetrivel et al., 2024). Therefore, the very high detection accuracies reported in several studies should be interpreted as evidence of strong benchmark performance rather than guaranteed real-world effectiveness, particularly where independent datasets or operational university network traffic were not used for validation (Ajax, 2025).

The findings further suggest that hybrid and ensemble approaches appear promising relative to single-model IDS because they combine known attack classification, unknown anomaly detection, temporal learning, and model diversity. Nevertheless, real-world adoption requires stronger evaluation of latency, throughput, computational overhead, scalability, and integration with existing campus infrastructure.

Explainability also remains essential. Without interpretable outputs, advanced ML models may be difficult for network administrators to trust or act upon. Future IDS frameworks should therefore integrate explainable AI, adaptive learning, feature selection, and decision fusion to support accurate, lightweight, and deployable intrusion detection in university networks (Alblehai, 2025).

9 Research gaps

Although several studies report high detection performance using ensemble and hybrid models, these findings cannot be considered directly comparable because of differences in datasets, attack scenarios, validation methods, evaluation metrics, and experimental environments (Rustam et al., 2025). Many studies rely on benchmark or simulated datasets, with relatively limited validation using independent operational network traffic. This creates uncertainty regarding whether the reported performance of ensemble and hybrid approaches can be maintained in heterogeneous and dynamic university network environments (Albalwy, 2025). Therefore, there is a need for empirical comparison of standalone and ensemble models under a consistent evaluation framework, together with independent external validation using operational university network data. This highlights the need for adaptive and context-aware intrusion detection systems specifically designed to detect both ARP spoofing and DDoS attacks within real-world university network environments.

9.1 Benchmark dataset dependency

A major finding across the reviewed literature is that reported detection performance is strongly shaped by dataset choice. Benchmark datasets such as CIC-IDS2017, CIC-DDoS2019, CAIDA, and related IoT datasets support reproducibility and model comparison, but they may not fully capture the heterogeneity, mobility, encrypted traffic, IoT density, academic workload variation, and administrative traffic patterns of real university networks. Consequently, high offline accuracy may not directly translate into reliable real-time detection performance in operational campus environments (Hafiz et al., 2022).

9.2 Limited cross-layer detection

The reviewed studies reveal that most ML-based intrusion detection systems address DDoS attacks and ARP spoofing independently, with DDoS detection focusing on network, transport, or application layers and ARP spoofing treated as an isolated Layer-2 threat (Katuri et al., 2025). This fragmented approach limits cross-layer visibility and reduces the ability to detect coordinated or multi-stage attacks in dynamic university networks. Future research should therefore develop adaptive multi-layer IDS frameworks capable of jointly detecting DDoS and ARP-related anomalies while supporting scalable,

low-latency, and real-time deployment in university environments (Laurens et al., 2023).

9.3 Real-time deployment constraints

The reviewed literature is dominated by benchmark-based studies (48%), while only 12% evaluated intrusion detection in real university network environments. This imbalance highlights a gap in operational validation and supports the need for frameworks tailored to university network conditions. Real-time deployment also remains a major limitation in ML-based DDoS and ARP spoofing detection. Although many studies report high offline accuracy, fewer evaluate detection latency, throughput, computational overhead, scalability, online learning, concept drift, model retraining, and integration with existing campus infrastructure. This gap is particularly important in university networks, where BYOD access, IoT devices, cloud services, legacy systems, and high user mobility create rapidly changing traffic conditions (Shyryn et al., 2026). Therefore, deployable IDS models should balance detection accuracy with low latency, resource efficiency, scalability, adaptability, and administrator interpretability. The distribution of these characteristics across the reviewed studies is presented in Table 11.

9.4 Limited explainability

Explainability is also essential for real-world adoption. Network administrators require interpretable outputs showing why traffic was classified as malicious, which features influenced the decision, and what response action is appropriate. Techniques such as SHAP, LIME, feature importance, and rule extraction can improve trust, reduce alert fatigue, and support forensic analysis (Khan et al., 2025).

Despite the high detection performance reported by many ML-based intrusion detection systems, model explainability remains a significant research gap. Most deep learning and ensemble models, including CNNs, LSTMs, deep neural networks, and hybrid architectures, operate as black-box systems, providing limited insight into the features driving anomaly detection (Ahanger et al., 2025). This lack of transparency reduces administrator trust, limits forensic analysis, and hinders practical deployment in university networks.

Although recent studies have incorporated Explainable Artificial Intelligence (XAI) techniques, such as SHAP and LIME, their adoption remains limited and may introduce additional computational overhead. Future research should focus on developing lightweight, explainable, and computationally efficient IDS frameworks that balance detection accuracy, transparency, and real-time deployment requirements for university network environments (Zubairu and Gide, 2025).

9.5 High computational cost

Computational cost remains a major barrier to the practical deployment of ML-based intrusion detection systems in university networks, particularly in resource-constrained institutions. Many high-performing deep learning, ensemble, and hybrid models require large labeled datasets, GPU-enabled computing resources, continuous model maintenance, and frequent retraining, which are often unavailable in universities with limited IT infrastructure and cybersecurity resources (Venturi et al., 2022).

TABLE 11 Distribution of real-time deployment and adaptation characteristics across reviewed studies ($n = 200$).

Evidence category	Studies ($n = 200$)	Percentage
Real-time detection evaluated	80	40%
Continuous/online learning evaluated	40	20%
Concept-drift detection	30	15%
Model retraining/adaptation	50	25%

Furthermore, real-time intrusion detection demands low latency, high throughput, and minimal computational overhead, making many offline models unsuitable for operational deployment. Future research should therefore focus on lightweight, scalable, and resource-efficient IDS frameworks that leverage techniques such as feature selection, model compression, incremental learning, edge-based detection, and hybrid architectures to balance detection accuracy with computational efficiency (Schummer et al., 2024).

9.6 Concept drift

University network traffic changes over time due to semester schedules, examinations, registration periods, research activity, software updates, new devices, and changing user behavior. These fluctuations introduce concept drift, causing models trained on previous traffic to become less effective as normal and malicious patterns evolve. Attackers also continually modify DDoS and ARP spoofing techniques to evade detection.

Future IDS frameworks should therefore support adaptive learning, periodic retraining, drift detection, and continuous performance monitoring to maintain reliable detection in dynamic campus environments (Prasad and Chandra, 2022).

10 Review-derived taxonomy of ML-based intrusion detection systems

The reviewed studies reveal fragmented ML-based intrusion detection approaches across learning paradigms, attack layers, deployment environments, operational modes, datasets, evaluation methods, and explainability. Existing IDS classifications typically emphasize one or a small number of these characteristics (Suleman et al., 2025). Therefore, this review develops a multidimensional, review-derived taxonomy that integrates seven complementary dimensions: learning paradigm, attack layer, deployment architecture, operational mode, dataset source, evaluation metrics, and explainability to provide a more comprehensive basis for comparing ML-based IDS approaches and identifying gaps relevant to university network environments.

The taxonomy integrates supervised, unsupervised, semi-supervised, deep learning, hybrid, and ensemble models with cross-layer attack detection, deployment architectures, dataset types, and evaluation criteria. It highlights key research gaps, including limited cross-layer detection, real-time deployment, and explainable ML, and provides a foundation for developing adaptive IDS for university networks (Razzaq and Shah, 2025; Ozdem, 2025).

10.1 Taxonomy by learning paradigm

Existing IDS classification frameworks commonly classify IDS according to a limited number of characteristics, including detection method, monitoring location, and system architecture. Traditional classifications distinguish IDS as signature-based, anomaly-based, or hybrid systems, while other frameworks classify systems as host-based IDS (HIDS), network-based IDS (NIDS), or distributed IDS according to their monitoring location and architecture (Alsaaidah et al., 2024). ML-oriented classifications further distinguish systems according to

supervised, unsupervised, semi-supervised, deep learning, and hybrid learning approaches.

Although these classifications provide useful descriptions of IDS technologies, they generally emphasize one primary characteristic at a time. They provide less systematic attention to the relationship between the learning approach, attack layer, deployment architecture, operational mode, dataset realism, evaluation methodology, and explainability of ML-based IDS (Firdhaust et al., 2025). This limitation is important for university networks because an IDS that performs well on a benchmark dataset may not necessarily be suitable for real-time deployment, cross-layer attack detection, or operational decision-making.

Therefore, this review extends conventional IDS classification by organizing the reviewed ML-based IDS studies across multiple complementary dimensions. The proposed taxonomy is intended not to replace established IDS classifications, but to provide a broader analytical structure for comparing modern ML-based detection approaches within the specific context of university network security.

10.2 Rationale for the proposed taxonomy dimensions

The seven dimensions of the proposed taxonomy were selected based on the recurring characteristics, limitations, and research gaps identified across the reviewed studies. Together, the dimensions capture the major factors that determine how an ML-based IDS learns, what it detects, where and when it operates, what evidence supports its performance, and whether its decisions can be interpreted.

The learning paradigm was selected because the learning strategy determines how an IDS learns patterns of normal and malicious traffic. Supervised, unsupervised, semi-supervised, deep learning, hybrid, and ensemble approaches provide different capabilities for known and previously unseen attacks.

The attack layer was selected because DDoS and ARP spoofing occur at different network layers and produce different observable behaviors. ARP spoofing is primarily a Layer-2 threat, whereas DDoS attacks may involve network, transport, and application layers. Including this dimension therefore supports analysis of whether an IDS provides single-layer or cross-layer detection.

Deployment architecture was selected because the practical effectiveness of an IDS depends on where monitoring and analysis occur. Centralized, distributed, edge-based, SDN-enabled, and cloud-assisted architectures have different implications for scalability, latency, coverage, and resource requirements.

Operational mode was selected to distinguish systems that operate offline from those capable of near-real-time, real-time, or adaptive/online detection. This dimension is particularly relevant to university networks because security monitoring must respond to rapidly changing traffic and active attacks.

Dataset source was selected because the realism and representativeness of training and evaluation data strongly influence reported IDS performance. Benchmark, simulated, and real-world datasets provide different levels of reproducibility and operational realism. This dimension also supports identification of benchmark-dataset dependency and generalization limitations.

Evaluation metrics were selected because accuracy alone may provide an incomplete assessment of IDS effectiveness, particularly where attack classes are imbalanced. Precision, recall, F1-score, ROC-AUC, false-positive rate, false-negative rate, detection rate, and latency

provide complementary information about detection quality and operational performance.

Explainability was selected because practical IDS deployment requires security administrators to understand and investigate model decisions. The inclusion of explainability distinguishes models that provide interpretable decisions from black-box approaches and captures the growing relevance of XAI techniques such as SHAP, LIME, feature importance, and rule extraction.

Thus, the seven dimensions collectively provide a technical, operational, data-oriented, performance-oriented, and interpretability-oriented perspective for analyzing ML-based IDS research in university network environments.

10.3 Taxonomy by attack layer

The taxonomy classifies ML-based intrusion detection systems according to the network layer targeted by the attack, recognizing that different attack types require distinct detection strategies. Layer 2 detection focuses on ARP spoofing, where ML models identify anomalies such as abnormal ARP requests, duplicate MAC–IP bindings, unsolicited ARP replies, and irregular gateway associations. In contrast, detection at the network, transport, and application layers primarily targets DDoS attacks using traffic volume, packet rates, flow duration, protocol behavior, connection frequency, and throughput patterns.

The taxonomy also incorporates cross-layer attacks, where multiple attack vectors, such as ARP spoofing combined with DDoS or session hijacking, are correlated across different network layers. This classification highlights the importance of multi-layer ML-based IDS frameworks capable of detecting coordinated attacks in dynamic university network environments.

10.4 Taxonomy by deployment architecture

The taxonomy classifies ML-based intrusion detection systems according to deployment architecture, reflecting where traffic monitoring and analysis occur within the network. The reviewed studies identify centralized, distributed, edge-based, SDN-enabled, and cloud-assisted deployment models, each addressing different operational requirements in university networks.

Centralized architectures provide unified monitoring but may face scalability and single-point-of-failure limitations. Distributed architectures improve coverage by deploying detection across multiple network segments. Edge-based architectures enable low-latency detection near traffic sources, making them suitable for IoT-enabled campuses. SDN-enabled architectures support dynamic traffic monitoring and automated response through programmable network controllers, while cloud-assisted architectures provide scalable storage and analytics for large-scale intrusion detection. Together, these deployment models highlight the need for flexible IDS architectures that balance scalability, response time, and operational efficiency in university networks.

10.5 Taxonomy by operational mode

The taxonomy by operational mode classifies ML-based IDS according to the speed of detection and the model’s ability to update its knowledge over time. This classification is crucial for university networks, which require both historical analysis and timely responses to active threats.

In offline mode, detection occurs after traffic data has been collected and stored. This mode is beneficial for model training, testing, forensic analysis, and algorithm comparison, but it is not suitable for immediate attack response.

In near-real-time mode, traffic is analyzed with minimal delay. This approach enables faster detection than offline analysis and is useful for monitoring suspicious traffic trends before they escalate. In real-time mode, traffic is analyzed continuously as it flows through the network. This mode is essential for detecting active DDoS attacks, ARP spoofing, and other intrusions before they cause significant disruption to university services.

In adaptive or online learning mode, the IDS updates its model as new traffic patterns and attack behaviors emerge. This is particularly useful in university networks, where traffic often changes due to BYOD use, IoT devices, online learning, examinations, and cloud services. Thus, the operational mode taxonomy aids in assessing the responsiveness of an ML-based IDS. Offline mode supports evaluation and training, near-real-time mode provides early warnings, real-time mode enables immediate detection, and adaptive learning facilitates continuous improvement against evolving threats.

TABLE 12 Multi-dimensional review-derived taxonomy of ML-based intrusion detection systems for university networks.

Learning paradigm	Attack layer	Deployment architecture	Operational mode	Dataset source	Evaluation metrics	Explainability
Supervised	Layer 2 (ARP)	Centralized	Real-time	Benchmark	Accuracy, Precision, Recall, F1-score	High
Unsupervised	Layer 2/Network	Distributed	Offline	Benchmark/ Simulated	Precision, Recall, FPR	Moderate
Semi-supervised	Cross-layer	Edge-based	Real-time	Mixed	F1-score, AUC	Moderate
Deep learning	Network/ Transport/ Application	SDN-enabled	Real-time	Benchmark/ Real-world	Accuracy, AUC, Latency	Low (Black-box)
Hybrid/ensemble	Cross-layer	Cloud-assisted	Real-time and offline	Mixed	Accuracy, F1-score, AUC, Latency	Moderate to High (XAI-supported)

10.6 Taxonomy by dataset source

The taxonomy classifies ML-based intrusion detection systems according to the source of training and evaluation data. The reviewed studies utilize benchmark datasets, simulated traffic, and real-world network traffic. Benchmark datasets, such as UNSW-NB15, CICIDS2017, CIC-DDoS2019, and CAIDA, are widely used because they support reproducibility and comparative evaluation. Simulated datasets enable controlled experimentation but may not fully represent operational environments. In contrast, real-world university network traffic provides greater realism but is less frequently used because of privacy, security, and data collection challenges. This classification highlights the need for more realistic datasets to improve the generalizability of ML-based IDS.

10.7 Taxonomy by evaluation metrics

The taxonomy also classifies IDS based on evaluation metrics. The reviewed studies commonly report accuracy, precision, recall, F1-score, ROC-AUC, false positive rate, detection rate, and latency. These metrics provide complementary measures of classification performance, reliability, and real-time deployment capability.

10.8 Taxonomy by explainability

Explainability is increasingly important in ML-based IDS because security analysts need to understand and justify detection decisions. Although models such as Decision Trees and Random Forests are relatively interpretable, more complex models may operate as black boxes. XAI techniques such as SHAP, LIME, feature importance, and rule extraction can therefore provide evidence for predictions, improve analyst trust, support forensic investigation, and strengthen practical IDS deployment. Table 12 summarizes the review-derived taxonomy by learning paradigm, attack layer, deployment architecture, operational mode, dataset source, evaluation metrics, and explainability.

11 Proposed review-derived ML-based intrusion detection framework

This systematic review synthesized evidence from 200 peer-reviewed studies to develop a review-derived conceptual framework for ML-based intrusion detection in university networks. The framework is synthesized from recurring architectural and methodological components identified across the reviewed literature and is intended to provide a structured blueprint for integrating ML into dynamic university network environments. It links six interdependent stages: traffic acquisition, preprocessing and feature extraction, ML-based detection, decision fusion, explainability, and response. These components collectively provide a conceptual pathway for supporting adaptive, scalable, explainable, and near-real-time detection of DDoS and ARP spoofing attacks.

The proposed framework is conceptual rather than empirically validated in this systematic review. Its purpose is to organize and integrate findings from existing studies into a unified architecture that can guide researchers and practitioners in the design, evaluation, and implementation of ML-based intrusion detection pipelines. The framework therefore does not claim demonstrated effectiveness or superiority over existing approaches. Future research should operationalize and empirically validate the framework through controlled experiments, quantitative performance benchmarking, and evaluation using diverse benchmark and real-world university network datasets.

11.1 Design rationale

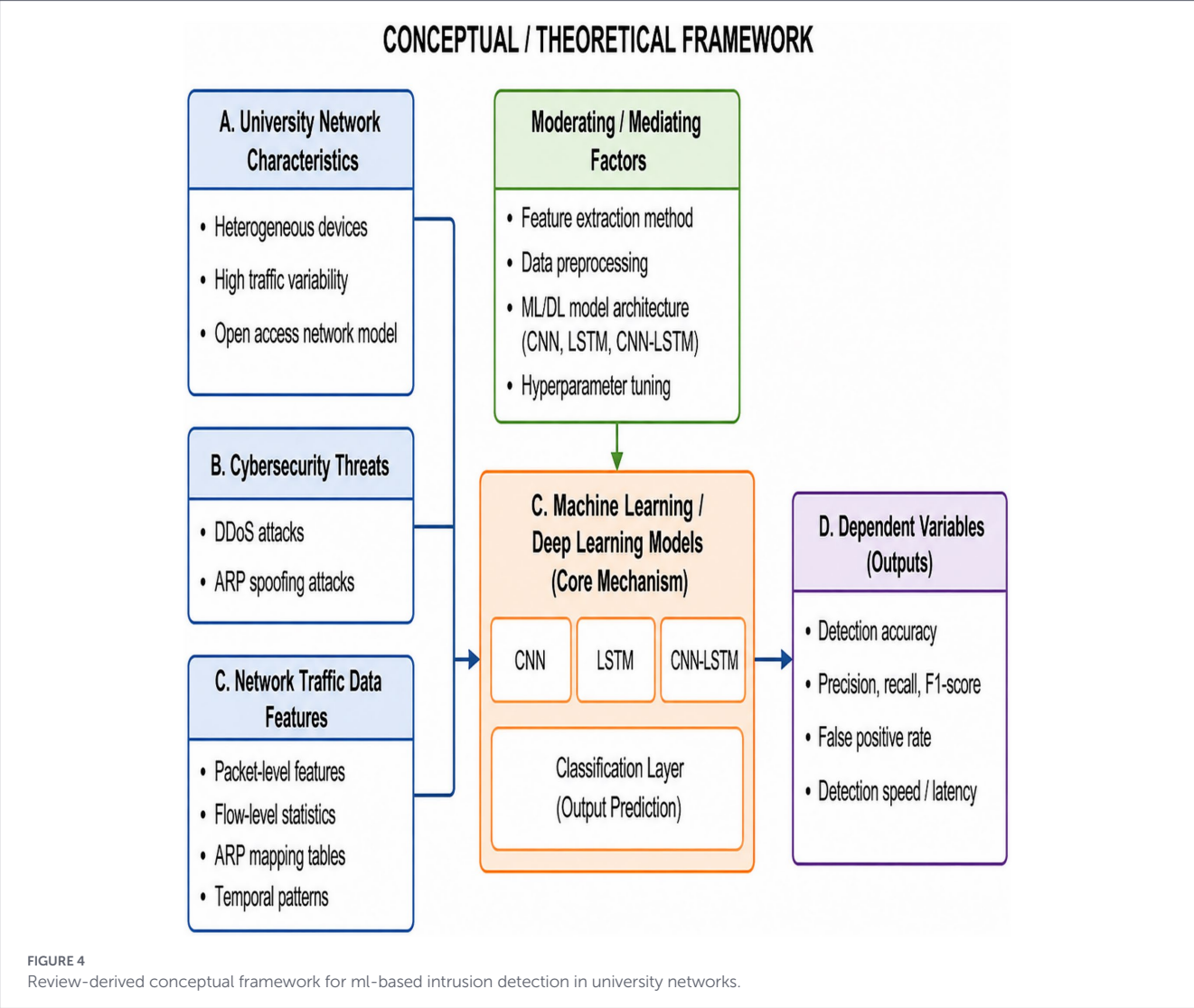
University network traffic is highly heterogeneous, dynamic, and non-stationary; therefore, relying on a single ML model is insufficient for robust intrusion detection. Classical supervised models, such as RF, SVM, and KNN, are effective for known attack patterns but depend on labeled data and may generalize poorly to evolving threats. Unsupervised and semi-supervised models can detect unknown anomalies but are often sensitive to threshold selection and prone to false positives.

Deep learning models capture complex spatial-temporal traffic behavior, but they require large datasets and higher computational resources. Since DDoS attacks generate high-volume flow anomalies while ARP spoofing produces low-volume Layer-2 behavioral deviations, an effective university IDS requires a hybrid and adaptive design that combines complementary models across multiple network layers. This rationale supports a unified framework that balances detection accuracy, scalability, computational efficiency, explainability, and real-time deployment feasibility.

11.2 Review-derived conceptual architecture

University networks face significant cybersecurity challenges due to their heterogeneous architecture, large scale, and resource-constrained devices, which create vulnerabilities across multiple layers, including devices, networks, services, and applications (Rueda-Rueda and Portocarrero, 2021). Although established frameworks like the NIST Cybersecurity Framework offer structured, risk-based guidance through the functions of Identify, Protect, Detect, Respond, and Recover, their effectiveness is often limited by the complexity, openness, and dynamic nature of university environments.

In this context, emerging threats such as DDoS and ARP-based attacks manifest as distinct anomaly patterns in network traffic. Conceptually, ML and DL models, when trained on these patterns and enhanced through targeted feature extraction and hyperparameter optimization, can detect and classify anomalies with high accuracy, thereby strengthening IDS and overall network security. The interplay between input data, model architecture, and detection outcomes provides a foundational basis for evaluating and optimizing IDS performance, underscoring the potential of intelligent, adaptive approaches to mitigating cybersecurity risks in university networks, as presented in Figure 4.



11.3 Review-derived ML-based anomaly detection framework

The reviewed studies demonstrate that no single ML algorithm effectively addresses the diverse and evolving threats in university networks (Mallick and Nath, 2024; Hirsi et al., 2024). Ensemble methods provide robust detection of known attacks, deep learning models capture complex traffic patterns, while autoencoders and other anomaly detection techniques identify previously unseen attacks (Jacobs et al., 2024). These findings informed the development of a review-derived ML-based anomaly detection framework that integrates traffic acquisition, preprocessing, feature extraction, multi-model detection, decision fusion, and real-time response to support adaptive, scalable, and accurate detection of DDoS and ARP spoofing attacks in university network environments (Chicco and Jurman, 2023). The proposed framework is illustrated in Figure 5.

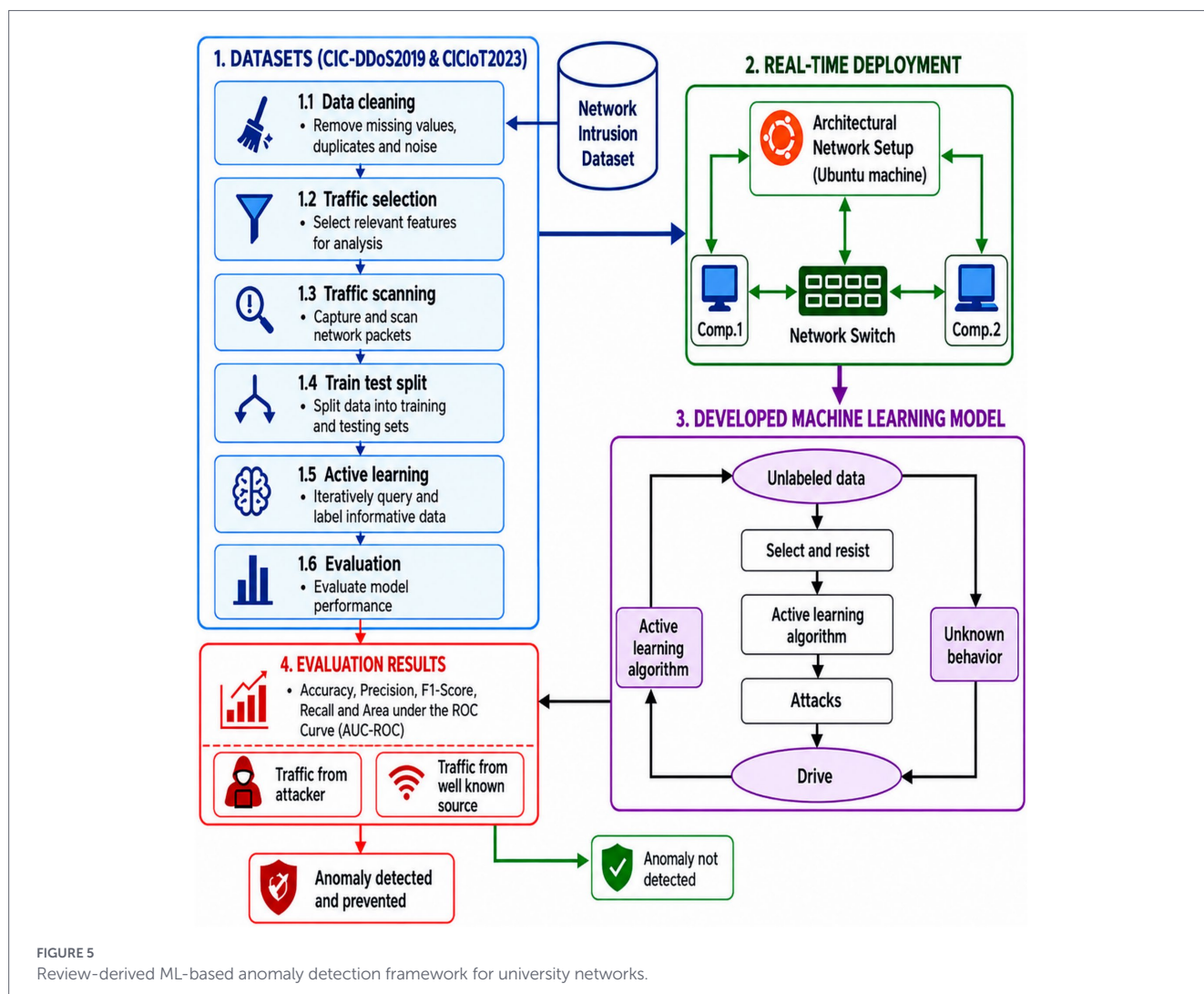
11.4 Data acquisition layer

The data acquisition layer captures diverse traffic essential for detecting DDoS attacks and ARP spoofing in university networks. It gathers packet-level, flow-level, and Layer-2 traffic attributes from switches, routers, wireless access points, IoT gateways, SDN

controllers, and network monitoring tools. Features include packet rate, flow duration, protocol type, source-destination distribution, throughput variation, ARP request frequency, MAC-IP binding changes, duplicate address mappings, and unsolicited ARP replies. This layer enables multi-source visibility across BYOD devices, IoT endpoints, cloud services, learning platforms, and legacy systems, establishing a foundation for cross-layer anomaly detection.

11.5 Preprocessing and feature engineering layer

The preprocessing and feature engineering layer transforms raw network traffic into reliable inputs for machine learning-based detection. It includes data cleaning, duplicate removal, handling of missing values, encoding of categorical features, normalization, traffic aggregation, and management of class imbalance. Feature engineering extracts DDoS-related indicators, such as packet bursts, flow-rate deviations, connection frequency, and abnormal throughput. Additionally, ARP-related features capture MAC-IP inconsistencies, repeated ARP replies, gateway impersonation, and local traffic redirection. Dimensionality reduction and feature selection are applied to minimize computational overhead and enhance real-time detection efficiency in resource-constrained university environments.



11.6 Hybrid detection layer

Based on the reviewed literature, the hybrid detection layer conceptually integrates complementary ML and deep learning models to improve detection robustness across diverse attack patterns. Supervised models support the detection of known DDoS and ARP spoofing attacks, while unsupervised and semi-supervised models facilitate the identification of unknown or evolving anomalies when labeled data are limited. Deep learning models capture complex spatial and temporal traffic patterns, particularly in high-volume DDoS flows and stealthy Layer-2 ARP deviations. This review-derived design highlights the potential benefits of combining multiple learning paradigms for adaptive intrusion detection in university networks.

11.7 Decision fusion and alert layer

The decision fusion and alert layer integrates outputs from multiple detection models to produce a final intrusion decision. Model outputs can be combined using techniques such as voting, weighted scoring, confidence thresholds, anomaly scores, or

meta-classification. This layer correlates flow-level DDoS indicators with Layer-2 ARP anomalies to enhance cross-layer situational awareness and reduce isolated false alerts. When malicious behavior is detected, the system generates prioritized alerts that include the attack type, affected device, confidence score, detected features, severity level, and recommended response action. This facilitates faster decision-making by administrators and improves operational readiness.

11.8 Explainability and response layer

The explainability and response layer improves trust, auditability, and practical deployment of ML-based IDS in university networks. Explainable AI techniques such as SHAP, LIME, feature importance, and rule extraction can be used to show why specific traffic was classified as malicious. Interpretable outputs help administrators verify alerts, reduce alert fatigue, and support forensic analysis. The response component may trigger mitigation actions such as rate limiting, VLAN isolation, MAC blocking, ARP inspection, SDN rule updates, traffic redirection, or administrator notification. This layer ensures that the framework moves beyond detection to actionable, explainable, and real-time intrusion prevention.

12 Model evaluation and performance metrics

Classification metrics are used to evaluate the framework's ability to distinguish benign traffic from DDoS and ARP spoofing attacks (Hirsi et al., 2024). The main metrics include accuracy, precision, recall, F1-score, MCC, ROC-AUC, and PR-AUC. Accuracy measures overall correctness, while precision and recall assess false alarms and missed attacks (Jacobs et al., 2024; Chicco and Jurman, 2023). F1-score balances precision and recall, MCC provides a robust measure under class imbalance, and ROC-AUC and PR-AUC evaluate discrimination across decision thresholds (Akwaronwu et al., 2025).

In Equations 11–14, TP and TN denote true positives and true negatives, while FP and FN denote false positives and false negatives. For DDoS or ARP spoofing detection, the positive class represents the attack being evaluated.

Equation 11 defines accuracy as the proportion of correct classifications:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (11)$$

Equation 12 defines precision among predicted positives:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (12)$$

Equation 13 defines recall among actual positives:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (13)$$

The F1-score is the harmonic mean of precision and recall.

Equation 14 expresses the F1-score in terms of the confusion-matrix counts:

$$\text{F1-score} = \frac{2\text{TP}}{2\text{TP} + \text{FP} + \text{FN}} \quad (14)$$

Equation 15 defines ROC-AUC as the area under the receiver operating characteristic curve, where TPR and FPR denote the true-positive and false-positive rates:

$$\text{AUC} = \int_0^1 \text{TPR}(\text{FPR}) d(\text{FPR}) \quad (15)$$

ROC-AUC summarizes discrimination between positive and negative classes across classification thresholds. When attacks are rare, PR-AUC is also informative because it emphasizes precision and recall for the positive class. Figure 6 shows schematic ROC curves for illustration only; it does not report a measured result from the included studies.

The performance of intrusion detection models must be evaluated using real-time metrics, especially in resource-constrained network scenarios where quick response times and little computational overhead are critical. Metrics such as detection latency (the time it takes to detect an anomaly), throughput (the number of packets processed per second), and resource consumption are critical for establishing the operational efficiency of an IDS in real-time networks (Kumar G. S. C. et al., 2024).

12.1 Operational metrics

Operational metrics are used to assess the real-time deployment feasibility of the proposed framework in university networks. These metrics include detection latency, throughput, CPU and memory overhead, and scalability (Graf et al., 2024). Detection latency measures the time required to identify an attack after it occurs, while throughput assesses the number of packets or flows processed within a specific timeframe. CPU and memory overhead indicate the computational cost of the detection model, and scalability evaluates whether performance remains stable as traffic volume, user count, BYOD devices, and IoT endpoints increase (Nawaz et al., 2025). Table 13 shows a summary of model validation and performance evaluation metrics for ML-based anomaly detection in university networks.

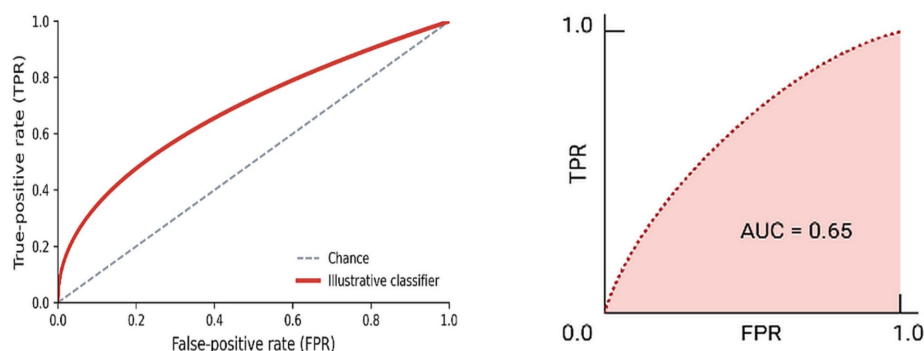


FIGURE 6
Receiver operating characteristic (ROC) curve illustrating IDS classification performance.

TABLE 13 Summary of model validation and performance evaluation metrics for ML-based anomaly detection in university networks.

Category	Technique/ metric	Description	Relevance to university network anomaly detection
Model validation (Security and Privacy, 2025)	Train-test split	Dataset is divided into training and testing subsets (e.g., 70/30 or 80/20).	Simple and efficient for evaluating ML models on campus traffic datasets.
	k-fold cross-validation	The dataset is split into k folds; each fold is used once for testing while the others train the model.	Reduces overfitting and improves generalization in diverse university traffic patterns.
	Stratified k-fold	Ensures each fold maintains the same class distribution as the full dataset.	Important for imbalanced attack datasets common in anomaly detection.
	Time-based validation	Training on historical data and testing on future data.	Suitable for real-time university networks with temporal traffic behavior.
Classification metrics (United Nations Conference on Trade and Development, 2021; Kumar G. S. C. et al., 2024; Syahputra and Wibowo, 2023)	Accuracy	Ratio of correctly predicted instances to total instances.	Useful for balanced datasets but limited for rare attack detection.
	Precision	Proportion of correctly detected attacks among all detected attacks.	Critical to reduce false alarms in university SOC environments.
	Recall (detection rate)	Proportion of actual attacks correctly identified.	Essential for detecting stealthy DDoS or ARP attacks in campus networks.
	F1-score	Harmonic mean of precision and recall.	Provides balanced performance evaluation under class imbalance.
Error metric (Kasumu, 2024; Shafiq et al., 2022)	False positive rate (FPR)	Ratio of normal traffic misclassified as attacks.	Important to avoid unnecessary disruption of academic services.
	False negative rate (FNR)	Ratio of attacks misclassified as normal traffic.	Critical since undetected attacks can compromise university systems.
Threshold and curve metrics (Kalyani and Vydeki, 2026; Karthickkumar et al., 2025)	ROC curve	Plots True Positive Rate against False Positive Rate.	Evaluates detection capability across different thresholds.
	AUC (area under curve)	Measures overall model discrimination ability.	Robust comparison metric for IDS models across datasets.
Anomaly-specific (Thakur et al., 2025)	Detection latency	Time taken to detect an anomaly after occurrence.	Important for real-time intrusion response in university networks.
	Throughput impact	Effect of detection model on network performance.	Ensures ML-based IDS does not degrade campus network services.
Operational evaluation (Al Sukkar et al., 2016; Monton et al., 2024; Alluraiah et al., 2024)	Computational overhead	CPU, memory, and processing cost of the model.	Relevant for deployment on limited university IT infrastructure.
	Scalability testing	Model performance under increasing traffic volume.	Ensures effectiveness in large, multi-user campus environments.

12.2 Validation strategies

Validation strategies assess the reliability and generalizability of ML-based IDS models. The train-test split offers a fundamental evaluation method, while stratified k-fold cross-validation enhances robustness by maintaining class distribution across folds. Time-based validation is particularly important for university networks, as traffic patterns fluctuate throughout semesters, registration periods, examinations, holidays, and peak usage times. Cross-dataset validation further evaluates whether a model trained on one dataset can perform reliably on another dataset or in a different environment. This is essential for minimizing overfitting and evaluating real-world

transferability beyond benchmark datasets (Allgaier and Pryss, 2024).

12.3 Simulation-based evaluation

Simulation-based evaluation provides a controlled environment for testing ML-based IDS models before real deployment. Platforms such as Mininet and SDN testbeds can emulate university network topologies, traffic flows, device mobility, and attack scenarios. Synthetic DDoS floods can be generated to assess detection under high-volume traffic conditions, while ARP spoofing scenarios can be

used to test Layer-2 anomaly detection (Yasarathna and Le-Khac, 2026). This approach supports controlled measurement of latency, throughput, packet loss, scalability, and response effectiveness under repeatable attack conditions.

12.4 Real-world deployment validation

Real-world deployment validation is necessary to determine whether ML-based IDS models remain effective in operational university environments. Campus traffic includes BYOD devices, IoT endpoints, cloud services, authentication systems, learning management platforms, research traffic, and administrative applications (Perumath, 2024). These conditions produce heterogeneous and non-stationary traffic patterns that are difficult to reproduce fully in benchmark datasets. Therefore, deployment validation should assess detection accuracy, false alarms, latency, resource consumption, administrator interpretability, and integration with existing network infrastructure under live or privacy-preserving campus traffic conditions (Deng, 2025).

12.5 Offline validation

For future empirical validation, the review-derived framework should be evaluated through a rigorous multi-level strategy combining offline testing, cross-validation, scenario-based analysis, and operational university-network validation (Shanmugam et al., 2025). Offline evaluation should be conducted on benchmark datasets, such as CIC-IDS2017 and CIC-DDoS2019, using stratified training, validation, and testing partitions to assess accuracy, precision, recall, F1-score, detection rate, false-positive rate, MCC, ROC-AUC, and PR-AUC. These evaluations would establish predictive reliability before subsequent testing under realistic university-network conditions.

12.6 Cross-validation and generalization

To assess generalizability and reduce overfitting during future empirical evaluation, k-fold or stratified k-fold cross-validation should be applied so that each data subset is used iteratively for training and testing under varying conditions (Churcher et al., 2021; Hnamte and Hussain, 2024). Scenario-based validation should additionally simulate realistic DDoS and ARP spoofing attacks in a controlled environment (Rose et al., 2021). Such testing would complement, rather than replace, independent validation using operational university-network traffic. Together, these validation stages would provide evidence about accuracy, stability, scalability, computational efficiency, and deployment suitability; they should not be interpreted as demonstrated performance until the review-derived framework has been implemented and empirically tested.

13 Limitations of the review

This review has several limitations. First, only English-language studies published between January 2021 and January 2026 were included, which may have excluded relevant studies published in other languages or outside the selected period. Second, most reviewed

studies relied on benchmark datasets such as CIC-IDS2017, CIC-DDoS2019, and CAIDA, while relatively few used real university network traffic. Finally, a quantitative meta-analysis was not performed because of the heterogeneity of datasets, ML models, validation strategies, and reported performance metrics.

Consequently, models that achieve high accuracy, precision, recall, or F1-score under offline experimental conditions may experience reduced generalization when exposed to live university traffic. This problem is intensified by the scarcity of high-quality labeled data in operational environments, where traffic is often noisy, imbalanced, encrypted, incomplete, or outdated. The lack of representative datasets also increases the risk of overfitting, where models perform well on curated benchmark data but fail to detect emerging or context-specific attacks in real campus networks. Future research should therefore prioritize the development of privacy-preserving, representative, and context-specific university network datasets that capture real DDoS behavior, ARP spoofing patterns, BYOD activity, IoT traffic, and normal academic operations (Padariya, 2025).

13.1 Limited integration of cross-layer attack detection

A further limitation in the reviewed literature is the limited integration of DDoS and ARP spoofing detection within unified, multi-layer ML-based intrusion detection architectures. Most existing studies examine these attacks separately, with DDoS detection commonly evaluated at the network, transport, or application layers, whereas ARP spoofing is treated mainly as a Layer-2 local network threat (Ali A. et al., 2025). This separation limits cross-layer visibility and constrains the development of integrated detection architectures capable of identifying both volumetric and stealthy attacks within the same operational environment.

This limitation is particularly critical in university networks, where shared broadcast domains, high device mobility, weak segmentation, IoT deployment, legacy infrastructure, and open-access connectivity increase exposure to both large-scale DDoS attacks and low-volume ARP manipulation. DDoS attacks may disrupt learning management systems, online registration platforms, authentication servers, and research services, while ARP spoofing may support man-in-the-middle attacks, credential interception, session hijacking, and traffic redirection within local network segments. Treating these threats independently reduces the ability of IDS architectures to support cross-layer situational awareness. Future studies should therefore develop unified and multi-layer ML-based frameworks that jointly analyze DDoS and ARP-related anomalies using flow-level, packet-level, temporal, and Layer-2 behavioral features (TilaPatil, 2025).

13.2 Class imbalance and false alarms

Class imbalance remains a major challenge in IDS evaluation because benign traffic usually dominates while attack traffic is relatively rare. Models trained on imbalanced datasets may achieve high accuracy but fail to detect low-frequency attacks such as ARP spoofing or low-rate DDoS. False positives can also overwhelm university IT teams and disrupt legitimate academic

services, while false negatives allow attacks to remain undetected. Therefore, IDS evaluation should prioritize precision, recall, F1-score, MCC, PR-AUC, FPR, and FNR rather than relying on accuracy alone (Shanmugam et al., 2025).

14 Future research directions

The reviewed literature demonstrates significant progress in applying ML and deep learning to DDoS and ARP spoofing detection. However, several research gaps remain. Future studies should focus on developing unified multi-layer intrusion detection frameworks that can simultaneously detect Layer-2 ARP spoofing and higher-layer DDoS attacks within a single architecture. Emphasis should also be placed on using realistic university network datasets that capture the heterogeneity of BYOD devices, IoT systems, cloud services, and dynamic user behavior.

More research is needed on adaptive and online learning approaches that can address concept drift and evolving attack strategies in university environments. Integrating explainable AI techniques should also be explored to improve model transparency, administrator trust, and forensic analysis. Furthermore, lightweight and edge-based detection models that can operate efficiently in resource-constrained campus infrastructures warrant investigation.

Finally, more real-world deployment studies are required to evaluate IDS performance using operational metrics such as latency, throughput, scalability, computational overhead, and response effectiveness. Such investigations would provide stronger evidence regarding the practical feasibility of ML-based intrusion detection systems in university network environments.

15 Conclusion

This systematic review synthesized evidence from 200 peer-reviewed studies on ML-based intrusion detection for DDoS and ARP spoofing attacks in university networks. The findings indicate that ML and deep learning approaches generally improve detection performance compared with traditional intrusion detection systems. However, their practical deployment remains limited by benchmark dataset dependency, limited real university network datasets, class imbalance, computational overhead, limited explainability, and concept drift (Vermesan and Friess, 2022; Ahanger et al., 2025)–(Schummer et al., 2024).

A major contribution of this review is the proposed review-derived taxonomy, which classifies existing IDS approaches according to learning paradigm, attack layer, deployment architecture, operational mode, dataset source, evaluation metrics, and explainability (Prasad and Chandra, 2022; Alsaaidah et al., 2024). The taxonomy provides a structured basis for comparing existing studies, identifying methodological trends, and highlighting research gaps. In addition, the proposed review-derived conceptual framework synthesizes key architectural components reported in the literature into a unified reference architecture for ML-based intrusion detection in university networks.

The reviewed evidence further suggests that hybrid and ensemble approaches, which combine supervised, unsupervised, and deep

learning models, may provide more robust detection across diverse attack patterns by leveraging complementary learning capabilities. Nevertheless, many reported detection accuracies above 99% are based on benchmark datasets and limited validation strategies, highlighting the need for more realistic evaluations using operational university network traffic before practical deployment.

These findings indicate that ML-based intrusion detection has considerable potential for university network security, but the strength of the evidence depends on the evaluation environment. Results obtained from operational campus networks provide the most relevant evidence of practical applicability, whereas results from benchmark datasets and controlled IoT, SDN, WBAN, and simulation environments primarily demonstrate algorithmic capability under specific experimental conditions. Therefore, the reported performance should not be assumed to represent real-world campus performance without further validation using representative university traffic and operational network deployments.

Future research should prioritize realistic university network datasets, adaptive and explainable ML models, lightweight edge-assisted deployment, and comprehensive real-world validation. Overall, this review provides a structured synthesis of current evidence together with a review-derived taxonomy and conceptual framework that support researchers, practitioners, and university network administrators in developing scalable, explainable, and deployable ML-based intrusion detection systems for modern university network environments.

Author contributions

KR: Supervision, Methodology, Conceptualization, Writing – review & editing, Investigation, Software, Writing – original draft, Funding acquisition, Project administration, Formal analysis, Visualization, Validation, Resources, Data curation. BS: Writing – original draft, Investigation, Supervision, Methodology, Writing – review & editing, Conceptualization. VM: Investigation, Supervision, Writing – review & editing, Visualization, Formal analysis, Methodology, Writing – original draft.

Funding

The author(s) declared that financial support was not received for this work and/or its publication.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated

organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary material for this article can be found online at: <https://www.frontiersin.org/articles/10.3389/fcomp.2026.1900515/full#supplementary-material>

References

- Abiramasundari, S., and Ramaswamy, V. (2025). Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms. *Sci. Rep.* 15. doi: 10.1038/s41598-024-84879-y
- Adejebi, K. B., and Abu-mahfouz, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: concept, research perspectives, and challenges. *J. Sens. Actuator Netw.* 12:51. doi: 10.3390/jsan12040051
- Agrawal, S., Gupta, G. K., Gopalakrishna, P. K., Balasubramaniam, V. S., Goel, L., and Mahadik, S. (2024). *Hybrid Machine Learning Models: Combining Strengths of Supervised and Unsupervised Learning Approaches*. 2024 7th International Conference on Contemporary Computing and Informatics (IC3I), pp. 1056–1061.
- Ahanger, T. A., Ullah, I., Algamdi, S. A., and Tariq, U. (2025). Machine learning-inspired intrusion detection system for IoT: security issues and future challenges. *Comput. Electr. Eng.* 123:110265. doi: 10.1016/j.compeleceng.2025.110265
- Ahmad, A. (2025). Telematics and informatics reports DDoS attack detection using CNN-BiLSTM with attention mechanism. *Telemat. Inform. Rep.* 18:100211. doi: 10.1016/j.teler.2025.100211
- Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E. H. M., Shahzad, T., et al. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Sci. Rep.* 15:1726. doi: 10.1038/s41598-025-85866-7
- Ahuja, N., Singal, G., Mukhopadhyay, D., and Nehra, A. (2022). Ascertain the efficient machine learning approach to detect different ARP attacks. *Comput. Electr. Eng.* 99:107757. doi: 10.1016/j.compeleceng.2022.107757
- Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., and Alourani, A. (2025). Securing IoT networks against DDoS attacks: a hybrid deep learning approach. *Sensors* 25, 1–23. doi: 10.3390/s25051346
- Ajax, R. (2025). *Comparison of Traditional vs. AI-Based Intrusion Detection and Prevention Systems: Efficiency and Accuracy*.
- Akwaronwu, B. G., Akwaronwu, I., and Adeniyi, O. J. (2025). Machine learning for detecting DoS attack: a comparative approach. *Br. J. Comput. Netw. Inf. Technol.* 1, 51–70. doi: 10.52589/BJCNIIT-10V0HK0Y
- Al Sukkar, G., Saifan, R., Khwaldeh, S., Maqableh, M., and Jafar, I. (2016). Address resolution protocol (ARP): spoofing attack and proposed defense. *Commun. Netw.* 08, 118–130. doi: 10.4236/cn.2016.83012
- Albalwy, F. (2025). *Advancing Artificial Intelligence of Things Security: Integrating Feature Selection and Deep Learning for Real-Time Intrusion Detection*, pp. 1–17.
- Alblehai, F. (2025). *Artificial Intelligence-Driven Cybersecurity System for Internet of Things Using Self-Attention Deep Learning and Metaheuristic Algorithms*.
- Al-Dulaimy, A. N., and Frey, H. (2026). A systematic review of machine learning-driven software-defined wireless sensor networks: architectures, security, and routing trends. *Electronics* 15. doi: 10.3390/electronics15163733
- Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., and Mahgoub, I. (2025). Machine learning-based security solutions for IoT networks: a comprehensive survey. *Sensors* 25, 1–48. doi: 10.3390/s25113341
- Alfriehat, N., Anbar, M., Aladaileh, M., and Hasbullah, I. (2024). RPL - based attack detection approaches in IoT networks: review and taxonomy. *Artif. Intell. Rev.* 57:10907. doi: 10.1007/s10462-024-10907-y
- Alhulayyil, H., Alzahrani, T., and Alsagri, H. (2024, 2025). Intrusion detection system framework for cyber-physical systems. *Egypt. Informatics J.* 30:100600. doi: 10.1016/j.eij.2024.100600
- Ali, Z., Akram, A., and Aslam, N. (2025). Supervised learning approach for intrusion detection in unbalanced network traffic. *VFAST Trans. Softw. Eng.* 1–12. doi: 10.21015/vtse.v13i2.2116
- Ali, A., Husain, M., and Hans, P. (2025). Intelligent ARP spoofing detection using multi-layered machine learning (ML) techniques for IoT networks. *arXiv*, 1–5. doi: 10.48550/arXiv.2507.21087
- Ali, G., Samuel, A., Mijwil, M. M., Al-Mahzoum, K., Sallam, M., Adamopoulos, I., et al. (2025). Enhancing cybersecurity in smart education with deep learning and computer vision: a survey. *Mesopotamian J. Comput. Sci.* 2025, 115–158. doi: 10.58496/MJCSC/2025/008
- Allgaier, J., and Pryss, R. (2024). Practical approaches in evaluating validation and biases of machine learning applied to mobile health studies. *Commun. Med.* 4. doi: 10.1038/s43856-024-00468-0
- Alluraiah, K., Sheela, M., and Chetty, R. (2024). 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* 2024, 743–753.
- Almomani, O., Alwada'n, T., and Al-Tarawneh, O. H. (2026). ML-based detection of ARP spoofing attacks in internet-of-things environments: comparative study. *Procedia Comput. Sci.* 275, 523–531. doi: 10.1016/j.procs.2026.01.061
- Almuhanna, R., and Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Front. Artif. Intell.* 8, 1–12. doi: 10.3389/frai.2025.1625891
- Alsaaidah, A., Almomani, O., Abu-Shareha, A. A., Abualhaj, M. M., and Achuthan, A. (2024). ARP spoofing attack detection model in IoT networks using machine learning: complexity vs. accuracy. *J. Appl. Data Sci.* 5, 1850–1860. doi: 10.47738/jads.v5i4.374
- Alsulami, R., Alqarni, B., Alshomrani, R., Mashat, F., and Gazdar, T. (2023). IoT protocol-enabled IDS based on machine learning. *Eng. Technol. Appl. Sci. Res* 13, 12373–12380. doi: 10.48084/etasr.6421
- Alturki, B., and Alsulami, A. A. (2025). Semi-supervised learning with entropy filtering for intrusion detection in asymmetrical IoT systems. *Symmetry (Basel)* 17, 1–25. doi: 10.3390/sym17060973
- Anagnostopoulos, T., Kostakos, P., Tsotsolas, N., Salmon, I., Morley, J., and Harle, R. (2021). Challenges and solutions of surveillance systems in IoT-enabled smart campus: a survey. *J. Mag.* 9, 1–29. doi: 10.1109/ACCESS.2021.3114447
- Awad, A. I., Babu, A., Barka, E., and Shuaib, K. (2024). AI-powered biometrics for internet of things security: a review and future vision. *J. Inf. Secur. Appl.* 82:103748. doi: 10.1016/j.jisa.2024.103748
- Aziz Al Kabir, M., Elmedany, W., and Sharif, M. S. (2023). Securing IoT devices against emerging security threats: challenges and mitigation techniques. *J. Cyber Secur. Technol.* 7, 199–223. doi: 10.1080/23742917.2023.2228053
- Bandara, I., Balakrishna, C., and Ioras, F. (2021). The need for cyber threat intelligence for distance learning providers and online learning systems. *INTED2021 Proc*, 9312–9321. doi: 10.21125/inted.2021.1947
- Blessing, E., and Klaus, H. (2024). *Anomaly Detection: Techniques to Identify Outliers or Anomalies in Datasets*, which Could be Indicative of Errors or Noteworthy Events.
- Bzai, J., Alam, F., Dhafer, A., Bojović, M., Altowajiri, S., Niazi, I. K., et al. (2022). Machine learning-enabled internet of things (IoT): data, applications, and industry perspective. *Des. Electron.* 11, 1–33. doi: 10.3390/electronics11172676
- Carvalho, M., Pinho, A. J., and Brás, S. (2025). Resampling approaches to handle class imbalance: a review from a data perspective. *J. Big Data* 12. doi: 10.1186/s40537-025-01119-4
- Casteleijn, D., and Franzsen, D. (2024). Heliyon personalized adaptive learning in higher education: a scoping review of key characteristics and impact on academic performance and engagement. *Heliyon* 10:e39630. doi: 10.1016/j.heliyon.2024.e39630
- Čekerevac, Z., Cekerevac, P., Prigoda, L., and Al-Naima, F. (2025). Security risks from the modern man-in-the-middle attacks. *MEST J* 13, 34–51. doi: 10.12709/mest.13.13.01.04

- Chaudhry, M., Shafi, I., Mahnoor, M., Vargas, D. L. R., Thompson, E. B., and Ashraf, I. (2023). A systematic literature review on identifying patterns using unsupervised clustering algorithms: a data mining perspective. *Symmetry (Basel)*. 15, 1–44. doi: 10.3390/sym15091679
- Chee, K. O., Ge, M., Bai, G., and Kim, D. D. (2025). Unveiling the evolution of IoT threats: trends, tactics, and simulation analysis. *Comput. Secur.* 157:104537. doi: 10.1016/j.cose.2025.104537
- Chen, S. R., Chen, S. J., and Hsieh, W. B. (2025). Enhancing machine learning-based DDoS detection through hyperparameter optimization. *Des. Electron.* 14, 1–19. doi: 10.3390/electronics14163319
- Chicco, D., and Jurman, G. (2023). The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. *BioData Min.* 16. doi: 10.1186/s13040-023-00322-4
- Chukwuani, E. N., Odunsi, O. R., and Ikemefuna, C. D. *Machine Learning Techniques for Real-Time Malware Classification and Threat Detection in Distributed Systems*. (2025).
- Churcher, A., Ullah, R., Ahmad, J., Rehman, S., Masood, F., Gogate, M., et al. (2021). An experimental analysis of attack classification using machine learning in IoT networks. *Sensors (Switzerland)* 21, 1–32. doi: 10.3390/s21020446
- Das, S., Mahfouz, A., Venugopal, D., and Shiva, S. (2019). *DDoS Intrusion Detection through Machine Learning Ensemble*.
- Dehkordi, S. B., Nasri, S., and Dami, S. (2025). Advances in network security and new anomaly detection techniques. *Majlesi J. Electr. Eng.* 19, 1–12. doi: 10.57647/j.mjee.2025.1902.26
- Deng, Z. (2025). Developing machine learning-based intrusion detection systems for IoT environments. *CEUR Workshop Proc.* 4034, 246–255.
- Devabhakthini, P., Parida, S., Shukla, R. M., and Nayak, S. C. (2023). Analyzing the impact of adversarial examples on explainable machine learning. *arXiv* 2023:327. doi: 10.48550/arXiv.2307.08327
- Dhrir, H., Charfeddine, M., Tarhouni, N., and Kammoun, H. M. (2025). Machine learning- and deep learning-based anomaly detection in firewalls: a survey. *J. Supercomput.* 81:761. doi: 10.1007/s11227-025-07212-y
- Diro, A., Kaiser, S., Vasilakos, A. V., Anwar, A., Nasirian, A., and Olani, G. (2024). Anomaly detection for space information networks: a survey of challenges, techniques, and future directions. *Comput. Secur.* 139:103705. doi: 10.1016/j.cose.2024.103705
- Domínguez-Bolaño, T., Barral, V., Escudero, C. J., and García-Naya, J. A. (2024). An IoT system for a smart campus: challenges and solutions illustrated over several real-world use cases. *Internet Things (Netherlands)* 25:101099. doi: 10.1016/j.iot.2024.101099
- Dong, H., and Kutenko, I. (2025). Cybersecurity in the AI era: analyzing the impact of machine learning on intrusion detection. *Knowl. Inf. Syst.* 67, 3915–3966. doi: 10.1007/s10115-025-02366-w
- Dulsrud, A., and Bygstad, B. (2022). Digital ecosystems as social institutions: exploring the role of consumption through four research streams of digital ecosystems. *Consum. Soc.* 1, 99–119. doi: 10.1332/QUPH6141
- Elbertsen, M., Kok, H., and Salimi, N. (2025). Designing the future smart campus: integrating key elements to enhance user experience. *J. Sci. Technol. Policy Manag* 16, 117–137. doi: 10.1108/JSTPM-10-2024-0414
- El-Sayed, A., Ramadan, H., Mohamed, E. R., and Elkomy, O. M. (2025). SFARP: a multi-layered real-time security framework for hybrid ARP and DDoS attack defense in SD-IoT networks. *Sci. Rep.* 15, 1–32. doi: 10.1038/s41598-025-28830-9
- Engineering. (2025). *(IoT) Network Intrusion Detection System Using Optimization Algorithms*, pp. 1–19.
- ENISA. (2024). *IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 Laying down rules for the Application of Directive (EU) 2022/2555 as Regards Technical and Methodological Requirements of Cybersecurity risk-Management Measures*.
- Ennaji, S., Gaspari, F. D. E., and Hitaj, D. (2025). Adversarial challenges in network intrusion detection systems: research insights and future prospects. *IEEE Access* 13, 148613–148645. doi: 10.1109/ACCESS.2025.3600984
- Eric, G., and Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge. *Sensors* 22, 1–33. doi: 10.3390/s22103744
- Firdhaust, R. S., Wati, K. M., Tsabitah, A. Z., and Wijayanto, I. (2025). *Comparative Analysis of Malicious Traffic Detection in IoT Network Using Machine Learning and Deep Learning Approaches* 2025. 4th International Electronic Conference Algorithm, pp. 18–23.
- Folarin Ogunjinmi, O. (2025). Optimizing network reliability: strategies for resilient telecommunications infrastructure in emerging economies. *Glob. J. Eng. Technol. Adv.* 22, 236–258. doi: 10.30574/gjeta.2025.22.3.0065
- Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *J. Cyber Pol.* 8871. doi: 10.1080/23738871.2021.1973526
- Ghazi, D. S. (2024). Snort versus suricata in intrusion detection. *Iraqi J. Inf. Commun. Technol.* 7, 73–88. doi: 10.31987/ijict.7.2.290
- Graf, F., Watteyne, T., and Villnow, M. (2024). Monitoring performance metrics in low-power wireless systems. *ICT Express* 10, 989–1018. doi: 10.1016/j.ict.2024.08.004
- Gupta, P., and Tripathy, P. (2024). Unsupervised learning for real-time data anomaly detection: a comprehensive approach. *Int. J. Comput. Sci. Eng.* 11, 1–11. doi: 10.14445/23488387/IJCSE-V11I10P101
- Hafiz, M., Yusuf, M., and Almohammed, A. A. (2022). Visualizing realistic benchmarked IDS dataset. *IEEE Access* 10, 94624–94642. doi: 10.1109/ACCESS.2022.3204690
- Han, D., Li, H., Fu, X., and Zhou, S. (2024). Traffic feature selection and distributed denial of service attack detection in software-defined networks based on machine learning. *Sensors* 24:4344. doi: 10.3390/s24134344
- Han, S., Li, F., Han, X., and Zhang, S. (2025). A novel feature engineering method for network anomaly detection. *Comput. Electr. Eng.* 127:110627. doi: 10.1016/j.compeleceng.2025.110627
- Hasan, M. K., Habib, A. K. M., Islam, S., Safie, N., Abdullah, S. N. H., and Pandey, B. (2023). DDoS: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Rep.* 9, 1318–1326. doi: 10.1016/j.egy.2023.05.184
- Hirsi, A., Alhartomi, M. A., Audah, L., Salh, A., Sahar, N. M., Ahmed, S., et al. (2025). Comprehensive analysis of DDoS anomaly detection in software-defined networks. *IEEE Access* 13, 23013–23071. doi: 10.1109/ACCESS.2025.3535943
- Hirsi, A., Audah, L., Salh, A., Alhartomi, M. A., and Ahmed, S. (2024). Detecting DDoS threats using supervised machine learning for traffic classification in software defined networking. *IEEE Access* 12, 166675–166702. doi: 10.1109/ACCESS.2024.3486034
- Hirsi, A., and Member, G. S. *Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks*. pp. 23013–23071. (2025).
- Hnamte, V., and Hussain, J. (2024). Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation. *Telemat. Inform. Rep.* 14:100129. doi: 10.1016/j.teler.2024.100129
- Hu, T., Zhang, Z., He, J., Shen, Y., Ma, J., Yin, H., et al. (2026). Protocol-agnostic network traffic anomaly detection via structural-temporal decoupling and adaptive fusion. *Inf. Fusion* 1:104398. doi: 10.1016/j.inffus.2026.104398
- Hussain, K., Rahmatyar, A. R., Riskhan, B., Sheikh, M. A. U., and Sindiramutty, S. R. (2024). *Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT) 2024*. IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), pp. 1–8.
- Hussien, S. H. T., Farhana, H. A. R. N., Vinukumar, L., Alexander, C. H. C., and Sivakumar, S. (2024). Smart campus attendance and security systems: leveraging IoT for enhanced efficiency. *AIP Conf. Proc.* 3161:386. doi: 10.1063/5.0229386
- Isong, B., Kgote, O., and Abu-Mahfouz, A. (2024). Insights into modern intrusion detection strategies for internet of things ecosystems. *Des. Electron.* 13:2370. doi: 10.3390/electronics13122370
- Jacobs, P. G., Herrero, P., Facchinetti, A., Vehi, J., Kovatchev, B., Breton, M. D., et al. (2024). Artificial intelligence and machine learning for improving glycemic control in diabetes: best. *IEEE Rev. Biomed. Eng.* 17, 19–41. doi: 10.1109/RBME.2023.3331297
- Jalal, M. E., and Elmaghraby, A. (2025). Toward deep semi-supervised continual learning: a unified survey for scalable and adaptive AI. *IEEE Access* 13, 60903–60929. doi: 10.1109/ACCESS.2025.3556569
- Kalyani, S., and Vydeki, D. (2026). Detecting rank attacks in RPL-based IoT networks. *J. Econ. Technol.* 4, 171–185. doi: 10.1016/j.ject.2025.06.003
- Kandasamy, V., and Roseline, A. A. (2025). Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. *Sci. Rep.* 15, 1697–1626. doi: 10.1038/s41598-025-85547-5
- Karthickkumar, A., Rathnamala, S., Parameswari, C., and Prabhananthakumar, M. (2025). 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 3, 1–6. doi: 10.1109/IATMSI64286.2025.10985456
- Kasumu, R. Y. (2024). The role and applications of internet of things (IoT) in higher education: uses and ways IoT affects students' learning. *Artic. Int. J. Multidiscip. Res. Growth Eval.* 5, 243–249.
- Katuri, K., Nguyen, H. T., and Anagnostou, E. (2025). Real-time detection and identification of ARP spoofing attacks in microgrids. *IEEE Access* 13, 72427–72441. doi: 10.1109/ACCESS.2025.3563721
- Kaur, S., and Singh, M. (2020). Hybrid intrusion detection and signature generation using deep recurrent neural networks. *Neural Comput. Applic.* 32, 7859–7877. doi: 10.1007/s00521-019-04187-9
- Khan, N., Ahmad, K., Al Tamimi, A., Alani, M. M., Bermak, A., and Khalil, I. (2025). Explainable AI-Based intrusion detection systems for industry 5.0 and adversarial XAI: a systematic review. *Information* 16, 1–45. doi: 10.3390/info16121036
- Khraisat, A., and Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* 4. doi: 10.1186/s42400-021-00077-7
- Kornaros, G. (2022). Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective. *IEEE Access* 10, 58603–58622. doi: 10.1109/ACCESS.2022.3179047
- Kumar, M., and Dash, C. S. (2024). Detecting and preventing ARP spoofing attacks using real-time data analysis and machine learning. *Int. J. Innov. Res. Comput. Sci. Technol.* 12, 47–55. doi: 10.55524/ijrcst.2024.12.5.7

- Kumar, G. S. C., Kumar, R. K., Kumar, K. P. V., Raghavendra Sai, N., and Brahmaiah, M. (2024). Deep residual convolutional neural network: an efficient technique for intrusion detection system. *Expert Syst. Appl.* 238:121912. doi: 10.1016/j.eswa.2023.121912
- Kumar, M. A., Purohit, K. C., Bhatt, J., and Semuwal, G. S. (2024). *Advanced ARP Attack Protection in SDNs Using Deep Learning Approach*. In: 2024 IEEE International Conferences Blockchain Distrib. Syst. Secur. ICBDS 2024, pp. 1–6.
- Laurens, D., Verkerken, M., Wauters, T., De Turck, F., and Volckaert, B. (2023). *Investigating Generalized Performance of Data-Constrained Supervised Machine Learning Models on Novel, Related Samples in Intrusion Detection*.
- Liu, Q., Hagenmeyer, V., and Keller, H. B. (2021). A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access* 9, 57542–57564. doi: 10.1109/ACCESS.2021.3071263
- Lopez, E., Gorla, G., Etxebarria-Elezgarai, J., Amigo, J. M., and Seifert, A. (2025). The importance of choosing a proper validation strategy in predictive models. Part 2: recipes for (avoiding) overfitting—a tutorial. *Anal. Chim. Acta* 1384:344838. doi: 10.1016/j.aca.2025.344838
- Mahar, I. A., Aziz, K., Chakrabarti, P., Ahmed, N., Ladan, M., and Javed, Y. (2026). *OPEN A hybrid Machine Learning Approach for Detecting DDoS Attacks in Software-Defined Networks*, pp. 1–16.
- Mahendar, K., and Shivakanth, G. (2025). *AI-SCAN_A Scalable AI-Driven IDS for Cyber Threat Detection in Cloud Environments*.
- Majumder, S., Deb Barma, M. K., and Saha, A. (2025). ARP spoofing detection using machine learning classifiers: an experimental study. *Knowl. Inf. Syst.* 67, 727–766. doi: 10.1007/s10115-024-02219-y
- Mallick, A. I., and Nath, R. (2024). Navigating the cybersecurity landscape: a comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Sci. News An Int. Sci. J.* 190, 1–69.
- Maseer, Z. K., Yusof, R., Bahaman, N., Mostafa, S. A., and Foozy, C. F. M. (2021). Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset. *IEEE Access* 9, 22351–22370. doi: 10.1109/ACCESS.2021.3056614
- Merkurjev, E., Ke, L., and Chen, L. (2024). Machine learning methods for small data challenges in molecular science 123, 8736–8780. doi: 10.1021/acs.chemrev.3c00189
- Mishra, S. R., Shanmugam, B., and Yeo, K. C. (2025). *SDN-Enabled IoT Security Frameworks — A Review of Existing Challenges*, pp. 1–38.
- Mohammad, R., Saeed, F., Almazroi, A. A., and Alsubaei, F. S. (2024). Enhancing intrusion detection systems using a deep learning and data augmentation approach. *Systems* 12, 1–18. doi: 10.3390/systems12030079
- Mohsin, D., Ali, A., and Lloret, J. (2025). *An Integrated Hybrid Deep Learning Framework for Intrusion Detection in IoT and IIoT Networks Using CNN-LSTM-GRU Architecture*, pp. 1–28.
- Monton, J. E. B., Dellosa, J. T., and Mendoza, R. N. (2024). *IoT-Based Energy Monitoring System (IBEMS) for Optimizing Power Consumption in University Facilities*. 8th International Artificial Intelligence and Data Processing Symposium IDAP.
- Morsy, S. M., and Nashat, D. (2022). D-ARP: an efficient scheme to detect and prevent ARP spoofing. *IEEE Access* 10, 49142–49153. doi: 10.1109/ACCESS.2022.3172329
- Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W., et al. (2023). Detecting DDoS attacks using adversarial neural network. *Comput. Secur.* 127:103117. doi: 10.1016/j.cose.2023.103117
- Nabi, N., Rahman, M. M., Ghosh, S. K., Alam, S., and Barua, R. (2024). Machine learning-based anomaly detection for cyber threat prevention. *J. Primeasia* 6, 1–8. doi: 10.25163/primeasia.6110172
- Nawaz, M., Tahira, S., Shah, D., Ali, S., and Tahir, M. (2025). Lightweight machine learning framework for efficient DDoS attack detection in IoT networks. *Sci. Rep.* 15. doi: 10.1038/s41598-025-10092-0
- Ngoie, I. (2022). The Potential Role of Cisco Networking Technologies in Advancing Smart Education Systems at the University of Lubumbashi, DRC. *J. Biomed. Res. Environ. Sci.* 6, 1302–1308. doi: 10.37871/jbres2185
- Ogogo, W. L. (2021). Real-time monitoring of network devices: its effectiveness in enhancing network security. *East Afr. J. Inf. Technol.* 3, 1–6. doi: 10.37284/eajit.3.1.153
- Ortiz-Ruiz, E., Bermejo, J. R., Sicilia, J. A., and Bermejo, J. (2024). Machine learning techniques for cyberattack prevention in IoT systems: a comparative perspective of cybersecurity and cyberdefense in Colombia. *Electronics* 13. doi: 10.3390/electronics13050824
- Ouhssini, M., Afdel, K., Akouhar, M., Agherrabi, E., and Abarda, A. (2024). Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: a comprehensive systematic review of state-of-the-art approaches. *Egypt. Informatics J.* 27:517. doi: 10.1016/j.eij.2024.100517
- Ozdem, M. (2025). A novel approach for real-time anomaly detection in dynamic computer networks using temporal graph networks and explainable artificial intelligence. *Alex. Eng. J.* 132, 369–382. doi: 10.1016/j.aej.2025.11.001
- Padariya, D. R. (2025). A privacy-preserving framework for generative model-driven synthetic datasets. *Proc. AAAI Conf. Artif. Intell.* 39, 29289–29290. doi: 10.1609/aaai.v39i28.35222
- Paes, D. S. F., de Moraes, C. H. V., and Batista, B. G. (2025). Analysis of supervised machine-learning techniques in computer networks attack detection. *Comput. Commun.* 240:108203. doi: 10.1016/j.comcom.2025.108203
- Papadogiannaki, E., and Ioannidis, S. (2021). Acceleration of Intrusion Detection in Encrypted Network. *Sensors (Basel)* 21:1140. doi: 10.3390/s21041140
- Paper, W. (2022). *Secure IoT Platforms for Consumer Internet of Things*.
- Parmar, M., and Miles, A. (2024). *Cyber Security Frameworks (CSFs): An Assessment between the NIST CSF v2.0 and EU Standards*. 2024 Security for Space Systems (3S), pp. 1–7.
- Patil, D. A., and Shyamala, G. (2025). A comprehensive survey on securing the social internet of things: protocols, threat mitigation, technological integrations, tools, and performance metrics. *Sci. Rep.* 15, 1–66. doi: 10.1038/s41598-025-23865-4
- Perumath, N. (2024). *Implementing Zero Trust Management in IoT Environment-Challenges and Solutions*. Scoping Review, pp. 1–134.
- Pham, T. V., Nguyen, A. T., Ngo, T. D., Le, D. H., Le, K. C., and Nguyen, T. H. (2020). *Proposed Smart University Model as a Sustainable Living Lab for University Digital Transformation 2020 5th International Conference on Green Technology and Sustainable Development (GTSD)*, pp. 472–479.
- Pinto, A., Herrera, L. C., Donoso, Y., and Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors* 23, 1–42. doi: 10.3390/s23052415
- Polat, O., Durmuş, O., Doğan, F., Türkoğlu, M., Şeker, H., Atasoy, F., et al. (2026). Supervised and deep learning techniques for DDoS detection in software-defined network architectures: a systematic review. *Eng. Sci. Technol. Int. J.* 75:102290. doi: 10.1016/j.jestch.2026.102290
- Prasad, A., and Chandra, S. (2022). *Defending ARP Spoofing-based MitM Attack using Machine Learning and Device Profiling*. 3rd International Conference On Computational Intelligence, ICCICIS 2022, pp. 978–982.
- Putra, R., Dyah, I., and Rachmawati, A. (2024). ScienceDirect ScienceDirect DDoS detection using machine learning approach DDoS detection using machine learning approach. *Proc. Comput. Sci* 245, 1157–1164. doi: 10.1016/j.procs.2024.10.345
- Quffa, A., and Abu-Naser, S. S. (2025). *A Rule-Based Expert System for Cybersecurity Threat Detection: Evolution, Applications, and the Hybrid AI Paradigm*. No. 9, pp. 44–62.
- Rahman, M. M., AlShakil, S., and Mustakim, M. R. (2024). A survey on intrusion detection system in IoT networks. *Cyber Secur. Appl.* 3:100082. doi: 10.1016/j.csa.2024.100082
- Ramos, J., Pais-Vieira, M., and Brás, S. (2026). Small, imbalanced, and noisy datasets in healthcare research: a systematic review. *Eng. Appl. Artif. Intell.* 181:115472. doi: 10.1016/j.engappai.2026.115472
- Razzaq, K., and Shah, M. (2025). Machine learning and deep learning paradigms: from techniques to practical applications and research frontiers. *Computers* 14. doi: 10.3390/computers14030093
- Rizwan, S., Usama, M., and Prajapat, S. (2025). A comprehensive survey on intrusion detection in internet of medical things: datasets, federated learning, blockchain, and future research directions. *ICT Express* 11:5. doi: 10.1016/j.ict.2025.11.005
- Rojas, M. P., and Chiappe, A. (2024). Artificial intelligence and digital ecosystems in education: a review. *Technol. Knowl. Learn.* 29, 2153–2170. doi: 10.1007/s10758-024-09732-7
- Rose, J. R., Swann, M., Bendiab, G., Shiales, S., and Kolokotronis, N. (2021). *Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT*. Proceeding 2021 IEEE Conference Netw. Softwarization Accel. Netw. Softwarization Cogn. Age, NetSoft 2021, pp. 409–415.
- Rueda-Rueda, J. S., and Portocarrero, J. M. T. (2021). Framework-based security measures for internet of things: a literature review. *Open Comput. Sci.* 11, 346–354. doi: 10.1515/comp-2020-0220
- Rustam, F., Obaidat, I., and Jurcut, A. D. (2025). MULTI-LF: a unified continuous learning framework for real-time DDoS detection in multi-environment networks 14, 1–18.
- Sadiqzade, Z., and Alisoy, H. (2025). Cybersecurity and online education – risks and solutions. *Luminis Appl. Sci. Eng* 2, 4–12. doi: 10.69760/lumin.20250001001
- Salvador-Najar, C., Julián, L., and Pérez, D. (2025). *Cross-Domain Adversarial Alignment for Network Anomaly Detection through Behavioral Embedding Enrichment*.
- Schiefer, T., Mahr, D., van Fenema, P. C., and Mennens, K. (2023). A collaborative approach to manage continuous service innovation. *Technovation* 134:103029. doi: 10.1016/j.technovation.2024.103029
- Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., and Llorente, Á. (2024). Machine learning-based network anomaly detection: design, implementation, and evaluation. *AI F.* 2967–2983. doi: 10.3390/ai5040143
- Sebestyen, H., Popescu, D. E., and Zmaranda, R. D. (2025). A literature review on security in the internet of things: identifying and analysing critical categories. *Computers* 14. doi: 10.3390/computers14020061
- Security. (2025). *Networking Security*, pp. 1–44.
- Security and Privacy. (2025). *Fereidouni - IoT and Man-in-the-Middle Attacks.Pdf*.

- Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., and Hamam, H. (2022). The rise of 'internet of things': review and open research issues related to detection and prevention of IoT-based security attacks. *Wirel. Commun. Mob. Comput.* 2022. doi: 10.1155/2022/8669348
- Shanmugam, V., Razavi-Far, R., and Hallaji, E. (2025). Addressing class imbalance in intrusion detection: a comprehensive evaluation of machine learning approaches. *Des. Electron.* 14, 1–19. doi: 10.3390/electronics14010069
- Sharma, A., Id, S. R., and Driss, M. (2024). Hybrid evolutionary machine learning model for advanced intrusion detection architecture for cyber threat identification. *PLoS One* 1, 1–22. doi: 10.1371/journal.pone.0308206
- Sharma, A., and Rani, S. (2025). An RF-DNN-based approach for detecting cyber attacks in IoT network. *J. Transform. Technol. Sustain. Dev* 9. doi: 10.1007/s41314-025-00077-2
- Sharma, K. V., Sarada, C., Vasavi, M., and Ambika, K. (2024). Securing IoT devices from DDoS attacks through blockchain and multi-code trust framework. *E3S Web Conf.* 472. doi: 10.1051/e3sconf/202447203001
- Shuilong, Z., Bee, H., and Ali, Y. (2025). A robust big data analytics framework for secure Network communication enhancing trust and integrity. *Int. J. Acad. Res. Bus. Soc.* 15, 1169–1186. doi: 10.6007/IJARBS/v15-i10/26821
- Shyaa, M. A., Ibrahim, N. F., Zainol, Z., Abdullah, R., Anbar, M., and Alzubaidi, L. (2024). Evolving cybersecurity frontiers: a comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. *Eng. Appl. Artif. Intell.* 137:109143. doi: 10.1016/j.engappai.2024.109143
- Shyryn, B., Ahamed, T., and Ainur, A. (2026). Enhancing software-defined network security with deep learning: a comprehensive review. *Int. J. Inf. Secur.* 25, 1–37. doi: 10.1007/s12027-026-01232-2
- Singh, N., Buyya, R., and Kim, H. (2025). Securing cloud-based internet of things: challenges and mitigations. *Sensors* 25, 1–45. doi: 10.3390/s25010079
- Singh, A., and Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. *Int. J. Semant. Web Inf. Syst.* 18, 1–43. doi: 10.4018/IJWSIS.297143
- Singhal, S., and Kumar, K. A. (2026). A cost-sensitive random forest framework for ARP spoofing detection in internet of medical things networks. *Front. Big Data* 9, 1–15. doi: 10.3389/fdata.2026.1878242
- Singun, A. J. (2025). Unveiling the barriers to digital transformation in higher education institutions: a systematic literature review. *Discov Educ* 4:37. doi: 10.1007/s44217-025-00430-9
- Sinha, P., Sahu, D., Prakash, S., Yang, T., Rathore, R. S., and Pandey, V. K. (2025). *OPEN A high Performance hybrid LSTM CNN Secure Architecture for IoT Environments Using Deep Learning*, pp. 1–26.
- Solutions, S., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., and Ullah, S. S. (2022). Network threat detection using machine/deep learning in sdn-based platforms: a comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction. *Sensors (Basel)* 22:7896. doi: 10.3390/s22207896
- Soori, M., Arezoo, B., and Dastres, R. (2023). Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cogn. Robot.* 3, 54–70. doi: 10.1016/j.cogr.2023.04.001
- Starcke, J., Spadafora, J., Spadafora, J., Spadafora, P., and Toma, M. (2025). The effect of data leakage and feature selection on machine learning performance for early Parkinson's disease detection. *Bioengineering* 12. doi: 10.3390/bioengineering12080845
- Suleman, D., Shibl, R., Ansari, K., and Yakoi, P. S. (2025). A taxonomy proposal of information assurance and data quality solutions in smart cities. *Franklin Open* 13:100436. doi: 10.1016/j.fraope.2025.100436
- Syahputra, H., and Wibowo, A. (2023). Comparison of support vector machine (SVM) and random forest algorithm for detection of negative content on websites. *J. Ilm. Tek. Elektro Komput. Inform.* 9, 165–173. doi: 10.26555/jiteki.v9i1.25861
- Tariq, U., Ahmed, I., Bashir, A. K., and Khan, M. A. (2024). Securing the evolving iot with deep learning: a comprehensive review 12, 3426–3454. doi: 10.58262/ks.v12i1.242
- Tas, O. (2025). An examination of the role of the address resolution protocol in computer networks and the ARP spoofing threat. *Eurasia Proc. Sci. Technol. Eng. Math* 35, 1–9. doi: 10.55549/epstem.1802618
- Thakur, D. S., Tiwari, D. V. K., and Agrawal, D. J. (2025). Performance analysis of linear kernel support vector machine models on real-world datasets. *Int. J. Adv. Netw. Appl* 17, 6753–6760. doi: 10.35444/ijana.2025.17106
- TilaPatil, V. (2025). Deep learning-driven IoT defence: comparative analysis of CNN and LSTM for DDoS detection and mitigation. *J. Inf. Syst. Eng. Manag.* 10, 8–21. doi: 10.52783/jisem.v10i8s.951
- Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., and Tymoshchuk, V. (2024). Detection and classification of DDoS flooding attacks by machine learning method. *CEUR Workshop Proc* 3842, 184–195. doi: 10.48550/arXiv.2412.18990
- Uddin, R., Kumar, S. A. P., and Chamola, V. (2024). Denial of service attacks in edge computing layers: taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Netw.* 152:3322. doi: 10.1016/j.adhoc.2023.103322
- Ulven, J. B., and Wangen, G. (2021). A systematic review of cybersecurity risks in higher education-Una revisión sistemática de los riesgos de ciberseguridad en Educación más Alta. *Futur. Internet* 13, 1–40. doi: 10.3390/fi13020039
- Umoke, C. C., Nwango, S. O., Onwe, O. A., and Oloko, K. (2025). Cybersecurity and governance in online education: addressing policy gaps in protecting students' digital identities. *Int. J. Soc. Sci. Manag. Res.* 11:2025. doi: 10.56201/ijssmr.vol.11no4.2025.pg499.515
- United Nations Conference on Trade and Development. (2021). *And Innovation 2021*.
- Vajrobol, V., Saxena, G. J., Pundir, A., Singh, S., Gupta, B., Gaurav, A., et al. (2025). Identify spoofing attacks in internet of things (IoT) environments using machine learning algorithms. *J. High Speed Netw.* 31, 61–70. doi: 10.1177/09266801241295886
- Vemuri, N., Thaneeru, N., and Tatikonda, V. M. (2024). Adaptive generative AI for dynamic cybersecurity threat detection in enterprises. *Int. J. Sci. Res. Arch.* 11, 2259–2265. doi: 10.30574/ijrsra.2024.11.1.0313
- Venturi, A., Stabili, D., Pollicino, F., Bianchi, E., and Marchetti, M. (2022). "Comparison of machine learning-based anomaly detectors for controller area Network," NCA 2022 - 2022 IEEE 21st int. Symp. Netw. Comput. Appl 21, 81–88. doi: 10.1109/NCA57778.2022.10013527
- Vermesan, O., and Friess, P. (2022). *Internet of Things-Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT*. Boca Raton, FL: CRC Press.
- Vetrivel, S. C., Maheswari, R., and Saravanan, T. P. (2024). *Industrial IOT: Security Threats and Counter Measures BT - Communication Technologies and Security Challenges in IoT: Present and Future*. Singapore: Springer Nature Singapore, 403–425.
- Villegas-Ch, W., Govea, J., Gutierrez, R., Maldonado Navarro, A., and Mera-Navarrete, A. (2024). Effectiveness of an adaptive deep learning-based intrusion detection system. *IEEE Access* 12, 184010–184027. doi: 10.1109/ACCESS.2024.3512363
- Wainwright, R., Bagheri, M., Salama, A., and Saatchi, R. (2025). Software-defined networking security detection strategies and their limitations with a focus on distributed denial-of-service for small to medium-sized enterprises. *Appl. Sci.* 15, 1–19. doi: 10.3390/app152312389
- Wang, S., Balarezo, J. F., and Member, G. S. (2021). Machine learning in network anomaly detection: a survey. *IEEE Access* 9, 152379–152396. doi: 10.1109/ACCESS.2021.3126834
- Wang, C. H., Kang, H., Lam, U., Seo, J. T., and Kim, D. (2026). A hybrid ensemble framework for unknown attack detection in IoT networks. *Futur. Gener. Comput. Syst.* 181:108447. doi: 10.1016/j.future.2026.108447
- Wang, J., Yu, L., Lui, J. C. S., and Luo, X. (2025). *Modern DDoS Threats and Countermeasures: Insights into Emerging Attacks and Detection Strategies*, pp. 1–35.
- Wind, N. O., State, F., Network, S., and Management, S. (2024). Towards a software-defined industrial IoT-edge network for next-generation offshore wind farms: state of the art, resilience, and self-X network and service management. *Energies* 17, 1–31. doi: 10.3390/en17122897
- Wororomi, J. K., Bintang, C., Allo, G., and Paranoan, N. R. (2023). Performance of K-means and DBSCAN algorithm in clustering gross regional domestic product. *J. Int. Conf. Proc.* 6, 179–193. doi: 10.32535/jicp.v6i5.2710
- Xu, C. (2022). Optimization of innovation and entrepreneurship education and training system in colleges and universities based on OpenStack cloud computing. *Sci. Prog.* 2022. doi: 10.1155/2022/2868499
- Yasarathna, T. L., and Le-Khac, N.-A. (2026). ASEADOS-SDN-IoT: a novel SDN-IoT network intrusion detection dataset and framework. *Internet Things* 36:101891. doi: 10.1016/j.iot.2026.101891
- Yunita, A., Pratama, M. I., Almuzakki, M. Z., Ramadhan, H., EAP, A., Firdausiah Mansur, A. B., et al. (2025). MethodsX performance analysis of neural network architectures for time series forecasting: a comparative study of RNN, LSTM, GRU, and hybrid models. *MethodsX* 15:103462. doi: 10.1016/j.mex.2025.103462
- Zeinalpour, A., and Ahmed, H. A. (2022). Addressing the effectiveness of DDoS-attack detection methods based on the clustering method using an ensemble method. *Electronics* 11. doi: 10.3390/electronics11172736
- Zou, Y., Kuek, F., Feng, W., and Cheng, X. (2025). Digital learning in the 21st century: trends, challenges, and innovations in technology integration. *Front. Educ.* 10:391. doi: 10.3389/feduc.2025.1562391
- Zubairu, B., and Gide, A. I. (2025). Machine learning-based framework for detecting and mitigating DoS attacks in Mobile ad-hoc networks (MANETs) 10, 151–160.