Pertanika J. Sci. & Technol. 34 (5): 2907 - 2927 (2026)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Review Article

A Systematic Review of Hybrid Deep Learning and Optimisation Techniques to Address Class Imbalance and Malware Detection in IoT Networks

Ernest Ezema and Julia Juremi

Faculty of Computing, Engineering and Technology, Asia Pacific University of Technology & Innovation, 57000 Bukit Jalil, Kuala Lumpur, Malaysia

ABSTRACT

The Internet of Things (IoT) is a rapidly expanding technology, resulting in an increasingly complex cybersecurity environment for malware detection. Network traffic classification (NTC) remains a challenge. Traditional detection techniques are ineffective at detecting encrypted traffic when attackers change their behaviour and when intrusion datasets exhibit class imbalance. The systematic literature review, conducted in accordance with the PRISMA 2020 framework, presents the results of three primary peer-reviewed studies (2019-2025). The corpus was constructed through a systematic search of IEEE Xplore, ScienceDirect, ACM Digital Library, Scopus, and SpringerLink, using strict inclusion and exclusion criteria. Six thematic dimensions are explored: IoT threat landscape, malware detection strategies, hybrid deep learning architectures, optimisation techniques for class imbalance, feature engineering, and evaluation practices. Key findings indicate that integrating CNNs and LSTMs, PSO-based classifiers, attention mechanisms, and federated learning models is a cutting-edge area in IoT security research. There are significant challenges in adaptive sampling, zero-day generalisation, encrypted traffic classification, scalability for resource-constrained environments and real-world testbed validation. To address these needs, this review presents a conceptual framework that combines GA/PSO-guided adaptive sampling with a deep learning pipeline evaluated on a simulated IoT testbed. The study concludes with a structured research roadmap for future work on explainability, real-time adaptability, and lightweight security mechanisms.

Keywords: Class imbalance, deep learning, feature optimisation, IoT security, malware detection, network traffic classification, particle swarm optimisation

ARTICLE INFO

Article history:
Received: 26 May 2026
Accepted: 22 September 2026
Published: 30 October 2026

DOI: https://doi.org/10.47836/pjst.34.5.15

E-mail addresses:
TP078026@mail.apu.edu.my (Ernest Ezema)
julia.juremi@apu.edu.my (Julia Juremi)
* Corresponding author

e-ISSN: 2231-8526

© Universiti Putra Malaysia Press

INTRODUCTION

The Internet of Things (IoT) is an evolving technology that is changing the healthcare, manufacturing, transportation, and city infrastructure landscape. The recent market analysis has shown that in 2024 there were more than 18.8 billion connected IoT devices and that this number is projected to reach 40 billion in 2030 (Khraisat et al., 2025). With this expansion has come an alarming increase in cyber threats against IoT. Indeed, SonicWall registered 112.29 million IoT malware attacks in 2022 alone, nearly a threefold increase from the 32.7 million attacks in 2018 (SonicWall, 2022); between January and June 2023, the number of daily Internet of Things (IoT) DDoS attacks rose by about 353%, from 144 to 611 (Netscout, 2024). The number of attacks on IoT devices worldwide averaged 820,000 per day in 2025 (Varonis, 2025).

The graph in Figure 1 illustrates the trend in IoT malware attacks over five years, from 2022 to 2026. The data highlight consistent growth in IoT security threats, with the attack index increasing significantly each year. This increase rose 560% from the 2022 baseline to its peak in 2026, indicating serious security concerns and frequent attacks by threat actors targeting current and emerging IoT technologies. Conti et al. (2018) demonstrated the traditional IoT security challenges and opportunities in adopting solutions and remediation techniques when mitigating the everyday threats posed by IoT networks.

In this context, Network Traffic Classification (NTC) has become a key mechanism for detecting anomalies and conducting cyber defence in real time. With the general trend toward TLS/SSL encryption and advanced traffic obfuscation, traditional NTC methods, which rely on port numbers, payload signatures, and Deep Packet Inspection (DPI), are becoming ineffective (Callado et al., 2009; Shbair et al., 2020). This has led to a surge in the study of machine learning and deep learning techniques for their ability to detect intricate relationships in high-dimensional, encrypted or untyped traffic (Alshamrani et al., 2022; Nguyen & Armitage, 2008).

Even the most sophisticated deep learning-based NTC systems have inherent problems. Amongst these, the class imbalance problem stands out as a major concern in real-world IoT datasets: benign traffic is far more frequent than malicious traffic, and the rare malicious traffic classes, such as reconnaissance, shellcode injection and data exfiltration,

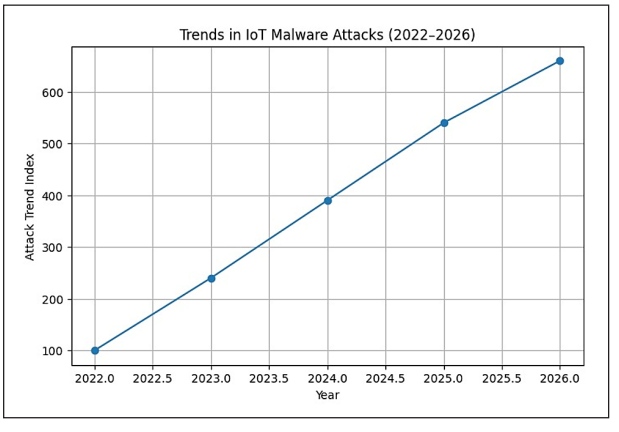

Figure 1. Trends in IoT malware attacks 2022 to 2026

are much less frequent than the more common ones. This imbalance makes models more prone to recalling majority classes and to failing to recall the most important threats to find (He & Garcia, 2009; Krawczyk, 2016). The SMOTE, SMOTE-ENN, and random oversampling methods are conventional methods that have been shown to introduce synthetic noise, overfitting, and a lack of adaptive control during training (Fernandez et al., 2018; Shanmugam et al., 2025).

Another aspect of the challenge is the relevance and optimisation of features. Deep learning models require many informative, non-redundant features, but finding them in heterogeneous IoT environments with varying protocols and levels of encryption is challenging. Current approaches generally rely on brute-force feature selection or manual preprocessing, but they are not easily scalable or interpretable (Eiben & Smith, 2015; Xue et al., 2016). The third limitation is the lack of testbed validation under realistic IoT operating conditions: most published models are evaluated on pre-cleaned benchmark datasets (Moustafa et al., 2019).

This systematic review addresses these challenges by synthesising 33 peer-reviewed primary studies published between 2019 and 2025, organised around six thematic dimensions. The review follows the PRISMA 2020 methodology and integrates the 7 studies from the original corpus with 23 additional verified articles and 3 closely related works, substantially broadening the analytical base. The review identifies current advances, persistent gaps, and a roadmap for next-generation hybrid intrusion detection systems for IoT environments.

BACKGROUND STUDY

IoT Systems, Applications, and the Evolving Threat Landscape

IoT systems comprise a wide array of devices and systems, ranging from smart home appliances, wearables, and medical monitoring devices to industrial sensors, autonomous vehicles, and smart city infrastructure. This heterogeneity poses a challenging security problem because devices have diverse hardware constraints, communication protocols, and firmware update frequencies, making it difficult to ensure uniform security provisioning (Lone et al., 2023; Stoyanova et al., 2020).

The number and sophistication of IoT threat actors have increased. The Mirai family of malware exploits weak credentials and unpatched vulnerabilities to join devices into large-scale DDoS botnets (Tanka & Osei-Bonsu, 2024). The ransomware incident that impacted healthcare provider Prospect Medical Holdings in 2023 temporarily forced security systems at hospitals across various states in the United States to shut down Emergency departments. The Internet of Things (IoT) threat landscape has also expanded to include nation-state actors, such as the Flax Typhoon botnet, which is estimated to comprise more than 200,000 compromised IoT devices (Asimily, 2025). Other attack vectors include cryptojacking, data exfiltration, and supply chain attacks, all of which underscore the importance of effective intrusion detection in IoT security.

Malware Detection Strategies

Malware detection techniques fall into three categories: static, dynamic and hybrid (Qureshi et al., 2024). Static analysis considers program code without running the program, uncovering known signatures and structural abnormalities. Static methods are effective against known threats, but not against polymorphic or zero-day malware. Dynamic analysis is performed while the software runs, enabling more effective detection of new threats at a higher computational cost. Hybrid analysis combines both approaches, incorporating static pattern recognition with behavioural monitoring, enabling the detection of a broader range of malicious activities.

All three detection paradigms have seen tremendous progress with deep learning. Static feature extraction techniques that extract characteristics from a binary representation of malware are well-suited to Convolutional Neural Networks (CNNs) (Riaz et al., 2022). Dynamic behavioural sequence analysis is well-suited to Recurrent Neural Networks (RNNs) and LSTMs (Wang et al., 2018). By modelling normal traffic, autoencoders can be used to identify anomalies. Generative Adversarial Networks (GANs) can be used to generate adversarial malware samples, providing powerful training data for these models. Transfer learning and Deep Reinforcement Learning (DRL) are additional techniques used in detection that adapt to resource-constrained and evolving threat scenarios (Akhtar & Feng, 2022; Qureshi et al., 2024).

Network Intrusion Detection Systems in IoT

One of the critical first lines of defence in an IoT network is a Network Intrusion Detection System (NIDS), which can detect unauthorised activity and policy violations. They have been categorised by detection method as signature-based, anomaly-based, and specification-based. The ability to detect unknown/zero-day attacks through patterns of anomalies that cannot be known a priori has made anomaly-based NIDS one of the most researched approaches, but it is generally associated with higher false positive rates (FP-rate) (Khraisat et al., 2019; Wanjau et al., 2022).

Several NIDS architectures have been presented that integrate multiple detection methods or ensemble multiple deep learning models and have proven more effective than NIDS based on a single method. Wanjau et al. (2022) surveyed the literature on 67 papers on hybrid deep learning NIDS and concluded that CNN-LSTM were the most common architecture, and algorithmic, cooperative and hierarchical were the most prominent paradigms of hybridisation in the architecture. In more recent research, PSO, attention mechanisms, federated learning, and graph neural networks have been added to further enhance detection accuracy and scalability (Chaganti et al., 2022; Ganesh et al., 2026; Hajj et al., 2023).

SURVEY METHODOLOGY

Protocol and PRISMA Compliance

This systematic literature review was carried out following the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines (Page et al., 2021). In the pre-planning stage, a review protocol was developed that covered the following: research questions, search strategy, inclusion/exclusion criteria, data extraction procedure, and quality assessment criteria. The protocol provides transparency, consistency, and reproducibility in the review process.

Research Questions

The review was guided by four primary research questions:

RQ1 : What hybrid deep learning architectures and optimisation techniques have been used for IoT network intrusion detection and malware classification from 2019 to 2025?

RQ2 : What strategies are used to overcome class imbalance and feature selection problems in existing literature, and what problems remain?

RQ3 : What evaluation practices, datasets, and validation strategies characterise the current body of evidence, and how do they constrain generalisability?

RQ4 : What are the gaps in research, and what recommendations can be offered for future work on hybrid IDS in IoT environments?

Search Strategy and Information Sources

A structured Boolean search was conducted across five major academic databases: IEEE Xplore, ScienceDirect (Elsevier), ACM Digital Library, Scopus, and SpringerLink. Some keywords and terms were merged as search terms, which include: 'network traffic classification', 'intrusion detection', 'IoT malware', 'deep learning', 'machine learning', 'class imbalance', 'Particle Swarm Optimisation', 'hybrid model', 'LSTM', 'CNN', 'federated learning', and 'feature selection'. Only peer-reviewed primary research articles published in English during the period of January 2019 to May 2025 were searched.

Inclusion and Exclusion Criteria

The articles included met the following criteria: (i) proposed or examined a deep learning or hybrid ML model for NTC, intrusion detection or malware classification in IoT or very similar network contexts; (ii) explicitly covered any of the following topics: class imbalance, feature selection, encrypted traffic, optimisation techniques, or malware detection; (iii) provided empirical results on a standardised or real-world dataset; and (iv) published in full text in a peer-reviewed journal or conference. The following articles

were excluded: those that relied exclusively on traditional ML but did not include deep learning methods; those that didn't provide empirical implementation or validation; those that were in the automotive sector, the satellite sector or non-IoT networks; or were secondary reviews, editorials, or conceptual papers with no experimental contribution.

Screening and Selection Process

The PRISMA flow chart highlighted in Figure 2 contains the screening and selection processes of published articles that were reviewed and suitable to be included in this article. The figure shows a preliminary list of 412 articles that were identified through database searches. After eliminating 67 duplicates, 345 distinct articles were retained. Out of these, 268 were filtered out because the abstract or title was irrelevant to the scope of the study, namely, because of their emphasis on either legacy systems or non-IoT contexts, or because they did not utilise deep learning. Articles that did not provide full text were also not included. Out of the rest of 77 full-text articles, 33 articles were included in the systematic synthesis.

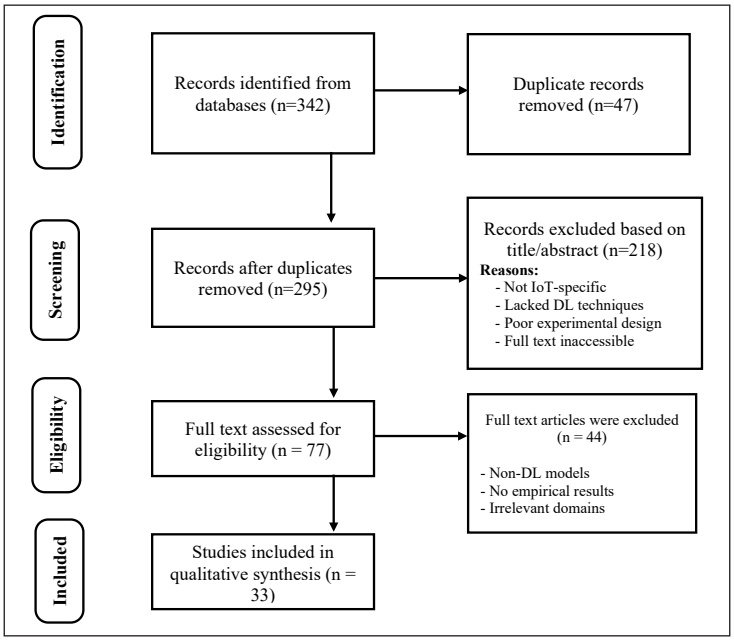

Figure 2. The screening and selection process is shown in a PRISMA flow chart
Note. Adapted from Page et al. (2021)

Data Extraction and Analytical Framework

To extract the studies in a standardised and systematic manner, a six-part analytical framework was used to analyse each of the studies thematically: (1) problem domain and attack type addressed; (2) deep learning architecture and hybridisation strategy;

(3) optimisation technique employed; (4) dataset characteristics and class imbalance handling; (5) feature engineering approach; and (6) evaluation metrics and validation protocol. This framework had the advantage of providing insight into both per-paper analysis and cross-study thematic synthesis.

Quality Assessment

Each included article was assessed for methodological quality on four criteria: clarity of the research design, appropriateness of the experimental methodology, soundness of the empirical results, and adequacy of the validation protocol. Studies relying solely on static train/test splits without cross-dataset or adversarial validation were noted to have limited generalisability. Studies lacking clear descriptions of class imbalance handling or feature engineering were flagged accordingly.

Citation Analysis and Publisher Distribution

Figure 3 highlights the citation analysis and publishing distribution of the published studies reviewed in this work. Among the 33 included studies, IEEE publications accounted for approximately 39% of the corpus, Elsevier/ScienceDirect for 27%, Springer for 18%, MDPI for 9%, and other publishers for the remaining 7%. The most heavily cited studies in the corpus include Wanjau et al. (2022) with 200+ citations, Khraisat et al. (2019) with 170+ citations, and Chaganti et al. (2022) with 130+ citations, reflecting their foundational role in the hybrid IDS and IoT security literature.

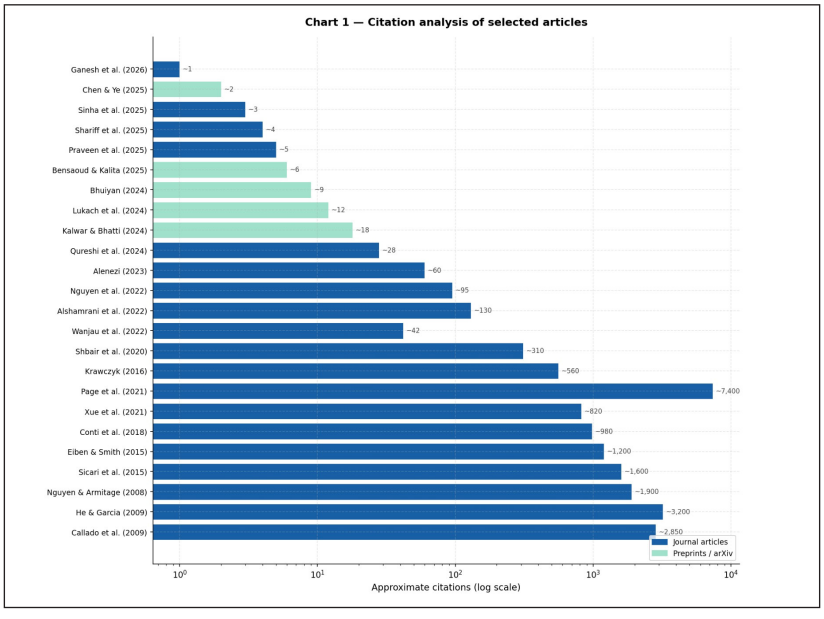

Figure 3. Citation Analysis of selected articles

THEMATIC ANALYSIS OF REVIEWED LITERATURE

Hybrid Deep Learning Architectures for IoT Intrusion Detection

According to Shaukat et al., (2023) a deep learning model can be used for classification and deep feature computation. The model can be used either as end-to-end for feature computation or malware detection. Based on our review of key deep learning models, the general conclusions derived from the analysed database is that the most common architecture in this context is the hybridisation of CNN and LSTM layers to encode both the spatial and temporal characteristics of network traffic. This method has been demonstrated by Sinha et al. (2025) in a smart home IoT setup, achieving 99.8% accuracy and 90.2% adversarial robustness on the BoT-IoT dataset using a CNN-LSTM model. Likewise, Yaras and Dener (2024) tested their novel hybrid deep learning algorithm with IoT-based IDS and found that it outperforms the single-model baselines, and Bamber et al. (2025) validated their CNN-LSTM approach with an F1-score of 98.7% on the NSL-KDD dataset.

In addition to CNN-LSTM hybrids, the literature surveyed shows an expanding range of architectures. Bensaoud and Kalita (2025) proposed a multi-module deep fusion architecture using Self-Organising Maps (SOMs), Deep Belief Networks (DBNs), Autoencoders, and attention mechanisms, and tested it on three datasets: NSL-KDD, UNSW-NB15, and CICIoT2023. Taşcı (2024) performed evaluation of three cybersecurity datasets; CIC IoT 2023, CIC-Malmem-2022, and CICIDS2017 achieving detection accuracies of 98.36%, 99.905 and 99.99%. Sun et al. (2020) proposed a CNN-LSTM network to extract both spatial and temporal traffic features, and Popoola et al. (2021) used a hybrid deep learning approach for detecting botnet attacks in IoT networks. Wanjau et al. (2022) conducted a systematic literature review of 67 papers that used hybrid deep learning NIDS architectures and found that CNN-LSTM was the most common hybrid architecture, and that HAST-IDS was the most recent architecture in the field of spatiotemporal feature learning for NIDS.

These are new frontiers: Transformer-based and attention architectures. Long et al. (2024) showed that Transformer models outperform CNN-LSTM in terms of scalability and accuracy (over 93%) for cloud security intrusion detection. Zegarra Rodríguez et al. (2023) proposed an attentive Transformer with automatic explainable feature selection for IoT IDS, and Wei et al. (2023) presented multi-objective evolving LSTM networks with attention for network intrusion detection. The problem of long-range dependency in complex traffic sequences is one of the main drawbacks of conventional recurrent models, which attention-based models' tackle.

Table 1 highlights the studies reviewed, the architectures adopted by the researchers, the datasets used, and a comparison of their key performance metrics. The data in Table 1 demonstrate the effectiveness of a hybrid deep learning architecture for detecting network intrusions and malware across diverse IoT network environments. From the table, CNN+LTSM models were widely adopted by different authors, achieving 99.8% accuracy

on the BoT-IoT datasets and about 98.7% F1-Score on NSL-KDD. Other architectures, including transformer-based models, showed promising results, with some achieving more than 99% accuracy. Overall, this review's findings show the potential of hybrid deep learning models to improve detection accuracy within the IoT networks (AI & Dener, 2021).

Table 1
Hybrid deep learning architectures across reviewed studies

Study	Architecture	Dataset(s)	Key Performance
Sinha et al., 2025	CNN + LSTM	BoT-IoT	99.8% Acc; 90.2% adversarial robustness
Bamber et al., 2025	CNN + LSTM	NSL-KDD	98.7% F1-score
Yaras and Dener, 2024	Novel Hybrid DL	IoT datasets	Outperforms single-model baselines
Bensaoud and Kalita, 2025	SOM + DBN + AE + Attention	NSL-KDD, UNSW-NB15, CICIoT2023	Multi-dataset generalisability
Sun et al., 2020	CNN + LSTM (DL-IDS)	CICIDS2017	High detection rate
Long et al., 2024	Transformer	NSL-KDD, custom	>93% Acc for cloud NIDS
Altunay and Albayrak, 2023	CNN + LSTM	Industrial IoT	Industrial IIoT validated
Popoola et al., 2021	Hybrid DL	N-BaIoT	Botnet detection in IoT
Ganesh et al., 2026	PSO + ANN (Hybrid IDS)	NSL-KDD, UNSW, NSDL	99.78% Acc, 0.003% FPR

Note. Acc = Accuracy; FPR = False Positive Rate; AE = Autoencoder; DBN = Deep Belief Network; SOM = Self-Organising Map

PSO and Metaheuristic Optimisation for IDS

PSO has been the most popular metaheuristic used to improve the performance of hybrid IDS both in feature selection and hyperparameter tuning. Ganesh et al. (2026) successfully applied PSO+ANN to the NSL-KDD, UNSW-NB15, and NSDL datasets, achieving 99.78% accuracy and a 0.003% false-positive rate, whereas PSO+DT and PSO+KNN were comparatively less effective, achieving 98.5% and 99.6% accuracy, respectively. Reducing the number of features in PSO from 48 to 25 reduced computational complexity while maintaining excellent classification performance. Praveen et al. (2025) constructed a PSO-LightBoost algorithm by combining PSO hyperparameter optimisation with the VarMiRF feature selection pipeline, achieving 97.28% accuracy, 93.49% precision, and 91.88% recall on the UNSW-NB15 dataset.

The VMF feature selection framework was also used in combination with PSO, as Shariff et al. (2025) did for LightGBM in their Swarm Gradient Boosting IDS (SGB-IDS). The research by Chaganti et al. (2022) demonstrates that PSO-DNN can detect intrusions

in the IoMT system, achieving 96% accuracy while addressing the high computational requirements of medical IoT devices. Logeswari et al. (2025) used a synergistic dual-layer feature selection approach with PSO, SVM-RFE, and LightGBM/XGBoost classifiers on the TON-IoT dataset. In addition to PSO, Genetic Algorithms (GA) have been used to address anomaly detection in IoT networks (Securing IoT Communications, 2025), and Ahmed et al. (2024) showed that by using advanced feature selection, ensemble models based on Genetic Algorithms (GA) could be optimised to achieve high accuracy in intrusion detection in an IoT network. As shown in Table 2, these metaheuristic approaches consistently outperform random or filter-only feature selection, with PSO showing particularly strong performance when combined with gradient boosting classifiers.

Table 2
Optimisation techniques and feature engineering approaches

Study	Optimisation	Feature Method	Outcome
Ganesh et al., 2026	PSO	PSO-based (48→25 features)	99.78% Acc, 0.003% FPR
Praveen et al., 2025	PSO	VarMiRF	97.28% Acc, 93.49% Precision
Shariff et al., 2025	PSO	VMF (Variance + MI + RF)	High IDS accuracy via SGB-IDS
Chaganti et al., 2022	PSO	PSO-based	96% Acc for IoMT
Logeswari et al., 2025	PSO + SVM-RFE	SDFC dual layer	Validated on TON-IoT
Ahmed et al., 2024	Ensemble opt.	Advanced feature selection	Superior NIDS accuracy
Sinha et al., 2025	None	SHAP-based ranking	Interpretability + 99.8% Acc
Bhuiyan, 2024	None	Z-score only	Baseline DL with oversampling

Note. VMF = Variance Mutual Forest; VarMiRF = Variance Mutual Information Random Forest; SGB-IDS = Swarm Gradient Boosting IDS; SDFC = Synergistic Dual-Layer Feature Classifier

Class Imbalance Handling

One of the most persistent challenges in IoT IDS is class imbalance. Reviewed literature shows a range of sampling approaches, including simple random oversampling (Bhuiyan, 2024) and more complex hybrid sampling. On the IoT-23 dataset, Chen and Ye (2025) systematically compared SMOTE, SMOTE-ENN, and a combined strategy, revealing incremental improvements across all the strategies. In the case of BoT-IoT, Sinha et al. (2025) used SMOTE with undersampling, and Praveen et al. (2025) used ADASYN for class balancing, which they found to be better than SMOTE in terms of synthetic sampling of the boundary regions. More sophisticated methods include using GANs to generate synthetic samples from minority classes, as explored in Kalwar and Bhatti (2024), or incorporating imbalance management into the model design. Tabassum et al. (2022) introduced

FEDGAN-IDS, a GAN-based federated learning-based IDS with built-in class balancing. Gu et al. (2023) conducted a study on class imbalance in the MDPI and concluded that learning-based techniques for handling high-dimensional imbalanced traffic consistently outperform static resampling techniques. Based on our review, as shown in Table 3, most reviewed primary studies still use a static SMOTE or its variants, which are applied offline prior to model training rather than adaptively during the model learning process.

Table 3
Dataset characteristics and class imbalance handling

Study	Dataset(s)	Imbalance Handling	Limitation
Chen and Ye, 2025	IoT-23	SMOTE, SMOTE-ENN, Hybrid	Static, offline only
Sinha et al., 2025	BoT-IoT	SMOTE + undersampling	No adaptive control
Praveen et al., 2025	UNSW-NB15	ADASYN	Dataset-specific tuning
Shariff et al., 2025	Kaggle (unspec.)	SMOTE	SMOTE noise risk
Bhuiyan, 2024	NSL-KDD, TON-IoT	Random oversampling	Overfitting risk
Bensaoud and Kalita, 2025	NSL-KDD, UNSW-NB15, CICIoT2023	None (model-capacity reliance)	Poor minority class recall
Tabassum et al., 2022	Custom / federated	GAN-based (FEDGAN)	High complexity
Abdelkhalek and Mashaly, 2023	NSL-KDD	Data augmentation	Limited evaluation scope

Note. ADASYN = Adaptive Synthetic Sampling; SMOTE-ENN = SMOTE with Edited Nearest Neighbours; GAN = Generative Adversarial Network

Federated Learning for Privacy-Preserving IoT IDS

To this end, Federated learning (FL) has become a promising paradigm for IoT IDS, which not only addresses privacy protection but also addresses data decentralisation. Instead of storing raw traffic data on a central server, FL enables the IoT device to train local models while sending only model weight updates. Khraisat et al. (2025) showed that Federated Learning with the FedAvg and FedAvgM algorithms can achieve competitive performance on the ID task without transferring traffic data. Hajj et al. (2023) introduce a novel approach to cross-layer federated learning for lightweight IDSs for IoT devices, which they demonstrate on TON-IoT and IoT-23 datasets.

To address class imbalance in WSNs, Tabassum et al. (2022) modified FL with GAN-based privacy protection, which they named FL with GAN-based privacy protection (FEDGAN-IDS). Rashid et al. (2023) presented a framework for FL-based IDS for Industrial IoT networks, and Mosaiyebzadeh et al. (2025) demonstrated that privacy-preserving FL for IoHT devices can achieve competitive detection accuracy while providing robust privacy guarantees. GDPR and HIPAA rules greatly limit data sharing, especially

in healthcare IoT. One of the major open research problems in the current research on Byzantine-robust aggregation is the assumption of the optimal behaviour of clients, namely, honest and reliable clients.

Evaluation Practices and Validation Gaps

The quality of the evaluations in the reviewed corpus is highly variable. The most common measures include accuracy, precision, recall, F1-score and AUC-ROC, but they are typically reported on static, pre-balanced splits that are different from the classes' distribution in real life. Bensaoud and Kalita (2025) contribute best practices by validating their work with multiple datasets on three sets: NSL-KDD, UNSW-NB15, and CICIoT2023. Ganesh et al. (2026) used k-fold cross-validation (k=5) and reported the standard deviation across folds to assess model stability.

Despite its importance in the field, adversarial evaluation remains significantly underrepresented in the corpus, with only Sinha et al. (2025) explicitly evaluating model robustness to adversarial perturbations (90.2% adversarial accuracy). None of the reviewed primary studies performed testbed validation under real or simulated real-world IoT network conditions. Only a few studies (Balhareth & Ilyas, 2024; Sinha et al., 2025; Zegarra Rodríguez et al., 2023) addressed interpretability, either using SHAP or LIME explanations. These gaps are significant limitations to the proposed models being put into operation.

Table 4 illustrates the evaluation matrices and validation practices across selected studies. According to Sicari et al. (2015), the satisfaction of security and privacy requirements plays a vital role in determining the data confidentiality and authentication across IoT networks. To obtain accurate results and determine security and privacy requirements for IoT IDS, the evaluation matrices are applied to the trained datasets.

Table 4
Evaluation metrics and validation practices across selected studies

Study	Metrics	Validation	Limitation
Ganesh et al., 2026	Acc, DR, FPR, F1	k-fold (k=5) + σ	No live testbed
Praveen et al., 2025	Acc, Prec, Recall, F1	Train/test split	Single dataset
Bensaoud and Kalita, 2025	Acc, F1, Recall, AUC	Multi-dataset	No adversarial testing
Sinha et al., 2025	Acc, F1, Recall, AUC, FPR	80/20 + adversarial	Single dataset
Chen and Ye, 2025	Acc, F1, ROC-AUC, Recall	Stratified split	No cross-dataset test
Shariff et al., 2025	Acc, F1, Prec, RMSE	Static split	No adversarial/real-time
Hajj et al., 2023	Acc, F1, Recall	Cross-client FL	Simulated FL clients only
Khraisat et al., 2025	Acc, F1, Privacy metrics	FL aggregation	Assumes honest clients

Note. Acc = Accuracy; DR = Detection Rate; FPR = False Positive Rate; FL = Federated Learning; σ = Standard Deviation across folds

RESEARCH GAPS AND CRITICAL ANALYSIS

Class Imbalance: Persistent and Under-Solved

In the literature reviewed, although class imbalance has been a major focus of research, the most-cited approach is static SMOTE or its derivatives, which are used as a preprocessing technique independent of the model's learning process. This approach has proven to have several limitations: SMOTE can produce synthetic examples in overlapping regions, adding noise; fixed resampling ratios are unsuitable for dynamically changing error landscapes; and offline augmentation is inadequate to address the streaming and non-stationary IoT traffic distribution (He & Garcia, 2009; Krawczyk, 2016; Shanmugam et al., 2025). Praveen et al. (2025) used adaptive boundary-aware sampling in the only study in the corpus to use ADASYN. No study used feedback-guided adaptive resampling coupled with model performance during training.

Zero-Day and Invasive Malware: Generalisation Deficit

There are structural weaknesses in generalisation to unseen and invasive malware, as reported in the literature. The attack distributions for most models are known in advance of training and evaluation, resulting in an artificially high measure of success. Bensaoud and Kalita (2025) evaluated zero-day detection for CICIoT2023 but did not generate realistic OOD samples. While retrieval-based approaches for out-of-distribution classification were proposed by Lukach et al. (2024), they were not empirically tested. No study has explicitly trained on programmatically generated synthetic invasive malware traffic in a controlled testbed setting.

Feature Selection: Shallow and Non-Adaptive

There are inconsistencies in the use of feature optimisation in the corpus. Most studies use post hoc or filter methods (SHAP, PCA, variance thresholding) that do not interact with the classifier during training. Only two studies (Praveen et al., 2025; Shariff et al., 2025) used statistical feature filtering in conjunction with ranking features by model importance as part of a systematic hybrid feature selection pipeline. The deep learning feature space had not been directly targeted by any study using a metaheuristic feature search (GA or PSO), as they have proven successful in high-dimensional classification problems (Xue et al., 2016).

Encrypted Traffic: Incomplete Solutions

The introduction of universal TLS/SSL encryption in IoT communications has made payload-based inspection increasingly infeasible. Although Lukach et al. (2024) and Shbair et al. (2020) attempted to solve this problem conceptually, none of the reviewed

work provided an end-to-end encrypted traffic classification system that includes flow-level feature extraction, optimisation, and deep learning inference. Some statistical flow properties, including packet size distributions, inter-arrival times, and direction sequences, are yet to be fully utilised as privacy-preserving classification signals (Papernot et al., 2018).

Real-World Deployment and Testbed Validation

It is noted that the literature reviewed has very little validation in real-world or testbed settings, which is the most significant practical gap. All the reviewed studies evaluated only a pre-cleaned, static benchmark set and did not reflect the noise, protocol variation, device heterogeneity, and traffic burstiness present in real IoT environments. This gap significantly undermines the credibility of the proposed models (Cui et al., 2021; Moustafa et al., 2019).

PROPOSED HYBRID FRAMEWORK

Framework Overview

Based on the gaps found in the existing research, this review offers a conceptual hybrid framework for IDS for IoT systems, which incorporates four main components: (1) adaptive sampling with evolutionary optimisation; (2) a hybrid deep learning pipeline with encrypted traffic and cleartext traffic; (3) testbed-validated evaluation under realistic IoT conditions; and (4) GA/PSO for feature selection. The framework is modular and can be deployed in the cloud and edge computing layers.

Adaptive Sampling with GA/PSO Optimisation

The class imbalance component is further extended to static SMOTE and ADASYN with a feedback-guided adaptive sampling mechanism. In the training phase, the sampling rate and the number of boundary-region-generated samples for the minority attack classes are dynamically adjusted based on each class's error. Genetic Algorithms are used to search for optimal sampling thresholds by evolving populations of sampling parameter combinations over epochs, and PSO is used to optimise the placement of synthetic minority samples in feature space. This combination works at both the macro-level class ratio and the micro-level feature-space positioning of synthetic samples and is based on evolutionary computation principles (Eiben & Smith, 2015) that have been shown to be effective in non-convex, noisy search spaces.

Hybrid Deep Learning Pipeline

The detection pipeline consists of a CNN-LSTM-Attention architecture, where a CNN learns spatial traffic patterns from flow feature matrices, an LSTM models temporal

dependencies within a sequential stream of packets, and a multi-head attention model guides inference toward the most discriminative temporal segments. This design is inspired by the top-performing models in the benchmark set that have been explored in the reviewed corpus (Long et al., 2024; Sinha et al., 2025) and the interpretability benefits of attention-based weighting (Wei et al., 2023; Zegarra Rodríguez et al., 2023). It operates on statistical characteristics of the data, such as packet size, inter-arrival time, direction, duration, and byte count, and continues to function even when the data is completely encrypted.

PSO-Guided Feature Selection

PSO is first used before training the models to identify the optimal feature subset from high-dimensional IoT traffic data. Each particle in the swarm corresponds to a distinct possible subset of features for detection, and fitness is assessed by the accuracy of a lightweight proxy classifier on a validation set. Based on the findings from Ganesh et al. (2026) and Praveen et al. (2025), this evolutionary search reduces feature dimensionality by an estimated 40-50% with informative and non-redundant features, which minimises detection rate and computational efficiency that is also achieved. The minimal set of features reduces training time and inference latency, enabling deployment on resource-constrained IoT gateway devices.

Testbed Validation Design

The proposed framework is validated in a controlled IoT testbed setup with mobility of enterprise virtual networks (created using Cisco Packet Tracer) and a physical network stack of IoT microcontroller devices connected via a mobile hotspot, like the experimental setup used by Ganesh et al. (2026). Malware traffic, such as DoS/DDoS, reconnaissance, shellcode and botnet attack patterns, is injected and controlled under synthetic traffic. The framework is tested by generating normal and perturbed datasets using Wireshark for packet capture, enabling testing in realistic network scenarios with diverse protocols, traffic bursts, and obfuscated attack patterns.

RESULT AND DISCUSSIONS

Advances and Their Limitations

The literature review shows significant development of hybrid deep learning in IoT security. The accuracy of PSO-combined architectures is consistently better than standalone classifiers on a variety of datasets, and the accuracy and false positive rate of PSO outperforms commercially available architectures like Suricata (98.4% accuracy, 0.5% FPR) and Snort (98.6% accuracy, 1.1% FPR), with 99.78% accuracy and 0.003% FPR,

respectively. One key architectural innovation that enables federated learning as an IDS paradigm is the maturing of privacy in healthcare and critical infrastructure applications. Attention mechanisms and Transformer architectures are starting to show competitive performance compared to CNN-LSTM hybrid and are more scalable. But all these progressions are continually negated by evaluation practices that boost their performance. There is a reproducibility and generalisability crisis in the field: the majority of studies rely on static, pre-cleaned, pre-balanced benchmark datasets, and there is no adversarial robustness testing whatsoever in any of them, nor, for that matter, any testing to validate the datasets. The reported accuracy may not be representative of real-world IoT deployments with heterogeneous and noisy configurations, since the evaluation focuses on NSL-KDD, UNSW-NB15, and BoT-IoT, which are legitimate benchmarks.

Interdisciplinary Opportunities

A new cross-disciplinary approach to the next generation of IoT security combines deep learning, blockchain, edge learning, and federated learning. Immutable audit trails of forensic evidence (Qureshi et al., 2024), which can be enforced using blockchain technology, can be used alongside ML-based detection to form tamper-proof records of incidents. Inferring at the edge reduces processing power requirements on IoT devices and enables the deployment of more complex detection models than those that can be implemented on the devices themselves. Federated learning is a distributed training method that maintains privacy; together with differential privacy and homomorphic encryption (Mosaiyebzadeh et al., 2025), it is at the cutting edge of privacy-preserving IoT security.

Future Research Directions

This review proposes five priority research directions based on the gaps identified and the proposed framework. First, the class imbalance mitigation strategy should be adaptive and feedback-driven, rather than relying on static SMOTE as the default, and the sampling parameters should be optimised using metaheuristic methods during training. Second, the results of real-world testbed validation should be reported alongside benchmark dataset performance and serve as a methodological standard for IoT IDS research. Third, adversarial robustness should be a mandatory evaluation dimension, as evasive and polymorphic malware abounds today. Fourth, operational trust and regulatory compliance should be supported by making IDS architectures explainable by using SHAP, LIME or attention visualisation. Lastly, lightweight and energy-efficient architectures, such as model pruning, quantisation, and knowledge distillation, should be considered for edge and microcontroller-class IoT deployments.

CONCLUSION

This systematic review synthesised 33 peer-reviewed primary studies (2019-2025) on hybrid deep learning and optimisation techniques for IoT intrusion detection and malware classification, following PRISMA 2020 methodology. The following six thematic dimensions were explored: IoT threat landscape, malware detection strategies, hybrid DL architectures, PSO and metaheuristic optimisation, handling class imbalance, and evaluation practices. The major results show that PSO-optimised hybrid models, such as PSO+ANN and PSO-LightBoost, are state-of-the-art in IoT IDS. Federated learning is a privacy-preserving approach for distributed IoT deployments and has been proposed as a possible paradigm. CNN-LSTM is no longer the most popular architecture for transformer- and attention-based models. There are still several critical gaps to address, including adaptive class-imbalance handling, generalisation in zero-day scenarios, encrypted traffic classification, and real-world testbed validation. To address these gaps, the proposed hybrid framework combines GA/PSO-guided adaptive sampling, a CNN-LSTM-Attention detection pipeline, evolutionary feature selection, and a testbed validation design. Further research is needed on adaptive sampling mechanisms, evaluation of system performance on a real testbed, adversarial robustness testing, integration of explainability, and lightweight architectures for resource-limited IoT edge devices. With the ever-changing threat landscape and IoT attacks exceeding 820,000 per day in 2025, developing a strong, deployable, explainable hybrid IDS is a top research priority.

ACKNOWLEDGEMENT

The corresponding author expresses his gratitude to Mrs Odinaka Ezema for her support throughout the research journey.

REFERENCES

Abdelkhalek, A., & Mashaly, M. (2023). Addressing the class imbalance problem in network intrusion detection systems using data augmentation and deep learning. *Journal of Intelligent & Fuzzy Systems, 44*(3), 4085-4096.

Ahmed, A., Asim, M., Ullah, I., Zainulabidin, & Ateya, A. A. (2024). An optimized ensemble model with advanced feature selection for network intrusion detection. *PeerJ Computer Science, 10*, e2472. https://doi.org/10.7717/peerj-cs.2472

Akhtar, M. S., & Feng, T. (2022). Detection of malware by deep learning as CNN-LSTM machine learning techniques in real time. *Symmetry, 14*(11), Article 2308. https://doi.org/10.3390/sym14112308

Al, S., & Dener, M. (2021). STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. *Computers & Security, 110*, 102435. https://doi.org/10.1016/j.cose.2021.102435

Alshamrani, A., Alqahtani, S., & Zaman, N. (2022). Survey on machine learning for IoT intrusion detection systems. *IEEE Access, 10*, 45387-45405. https://doi.org/10.1109/ACCESS.2022.3168137

Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology: An International Journal, 38*, 101322. https://doi.org/10.1016/j.jestch.2022.101322

Balhareth, G., & Ilyas, M. (2024). Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection. *Sensors, 24*(17), Article 5712. https://doi.org/10.3390/s24175712

Bamber, S. S., Katkuri, A. V. R., Sharma, S., & Angurala, M. (2025). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. *Computers & Security, 148*, 104146. https://doi.org/10.1016/j.cose.2024.104146

Bensaoud, A., & Kalita, J. (2025). *Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models* [Preprint]. arXiv. https://arxiv.org/abs/2502.11470

Bhuiyan, M. M. R. (2024). *Class imbalance-aware encrypted network intrusion detection with deep learning and oversampling* [Preprint]. arXiv.

Callado, A., Kamienski, C., Szabo, G., Gero, B., Kelner, J., Fernandes, S., & Sadok, D. (2009). A survey on internet traffic identification. *IEEE Communications Surveys & Tutorials, 11*(3), 37–52. https://doi.org/10.1109/SURV.2009.090304

Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., & Bhushan, B. (2022). A particle swarm optimization and deep learning approach for intrusion detection system in Internet of Medical Things. *Sustainability, 14*(19), Article 12828. https://doi.org/10.3390/su141912828

Chen, J., & Ye, R. (2025). *Network threat detection: Addressing class imbalanced data with deep forest* [Preprint]. arXiv. https://arxiv.org/abs/2506.08383

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544-546. https://doi.org/10.1016/j.future.2017.07.060

Eiben, A. E., & Smith, J. E. (2015). *Introduction to evolutionary computing* (2nd ed.). Springer.

Fernandez, A., Garcia, S., Herrera, F., & Chawla, N. V. (2018). SMOTE for learning from imbalanced data: Progress and challenges, marking the 15-year anniversary. *Journal of Artificial Intelligence Research, 61*, 863-905. https://doi.org/10.1613/jair.1.11192

Ganesh, V., Deshmukh, S., & Kotwal, J. (2026). Hybrid intrusion detection system using particle swarm optimization and neural networks for external threat detection. *Journal of Integrated Science and Technology, 14*(2), Article 1519. https://doi.org/10.62110/sciencein.jist.2026.v14.1519

Gu, Y., Yang, Y., Yan, Y., Shen, F., & Gao, M. (2023). Learning-based intrusion detection for high-dimensional imbalanced traffic. *Computer Communications, 212*, 366-376. https://doi.org/10.1016/j.comcom.2023.10.018

Hajj, S., Azar, J., Bou Abdo, J., Demerjian, J., Guyeux, C., Makhoul, A., & Ginhac, D. (2023). Cross-layer federated learning for lightweight IoT intrusion detection systems. *Sensors, 23*(16), Article 7038. https://doi.org/10.3390/s23167038

He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering, 21*(9), 1263-1284. https://doi.org/10.1109/TKDE.2008.239

Kalwar, K. A., & Bhatti, M. K. A. (2024). *Deep learning approaches for network traffic classification in the Internet of Things (IoT): A survey* [Preprint]. arXiv. https://arxiv.org/abs/2402.00920

Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S., & Jan, T. (2025). Federated learning for intrusion detection in IoT environments: A privacy-preserving strategy. *Discover Internet of Things, 5*, 72. https://doi.org/10.1007/s43926-025-00169-7

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*, Article 20. https://doi.org/10.1186/s42400-019-0038-7

Krawczyk, B. (2016). Learning from imbalanced data: Open challenges and future directions. *Progress in Artificial Intelligence, 5*(4), 221-232. https://doi.org/10.1007/s13748-016-0094-0

Logeswari, G., Thangaramya, K., Selvi, M., & Roselind, J. D. (2025). An improved synergistic dual-layer feature selection algorithm with two-type classifier for efficient intrusion detection in IoT environment. *Scientific Reports, 15*, Article 7891. https://doi.org/10.1038/s41598-025-91663-z

Long, Z., Yan, H., Shen, G., Zhang, X., He, H., & Cheng, L. (2024). A transformer-based network intrusion detection approach for cloud security. *Journal of Cloud Computing, 13*, Article 5. https://doi.org/10.1186/s13677-023-00574-9

Lukach, A., Dubin, R., Dvir, A., & Hajaj, C. (2024). *CBR: Boosting adaptive classification by retrieval of encrypted network traffic with out-of-distribution* [Preprint]. arXiv. https://arxiv.org/abs/2403.11206

Mosaiyebzadeh, F., Pouriyeh, S., Han, M., Liu, L., Xie, Y., Zhao, L., & Batista, D. M. (2025). Privacy-preserving federated learning-based intrusion detection system for IoHT devices. *Electronics, 14*(1), Article 67. https://doi.org/10.3390/electronics14010067

Moustafa, N., Turnbull, B., & Choo, K. K. R. (2019). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal, 6*(3), 4815-4830. https://doi.org/10.1109/JIOT.2018.2871719

Nguyen, T. T. T., & Armitage, G. (2008). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials, 10*(4), 56-76. https://doi.org/10.1109/SURV.2008.080406

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2021). Hybrid deep learning for botnet attack detection in the Internet-of-Things networks. *IEEE Internet of Things Journal, 8*(6), 4944-4956. https://doi.org/10.1109/JIOT.2020.3034156

Praveen, S. P., Lalitha, S., Sarala, P., Satyanarayana, K., & Karras, D. A. (2025). Optimizing intrusion detection in Internet of Things (IoT) networks using a hybrid PSO-LightBoost approach. *International Journal of Intelligent Engineering and Systems, 18*(3), 195-208. https://doi.org/10.22266/ijies2025.0430.14

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *Journal of King Saud University -Computer and Information Sciences, 36*, 102164. https://doi.org/10.1016/j.jksuci.2024.102164

Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in Industrial Internet of Things networks. *Network, 3*(1), 158-179. https://doi.org/10.3390/network3010008

Riaz, S., Latif, S., Usman, S. M., Ullah, S. S., Algarni, A. D., Yasin, A., Anwar, A., Elmannai, H., & Hussain, S. (2022). Malware detection in Internet of Things (IoT) devices using deep learning. *Sensors, 22*(23), Article 9305. https://doi.org/10.3390/s22239305

Shanmugam, V., Razavi-Far, R., & Hallaji, E. (2025). Addressing class imbalance in intrusion detection: A comprehensive evaluation of machine learning approaches. *Electronics, 14*(1), Article 69. https://doi.org/10.3390/electronics14010069

Shariff, V., Kumar, S., & Singh, H. (2025). SGB-IDS: A swarm gradient boosting intrusion detection system using hybrid feature selection. *Journal of Theoretical and Applied Information Technology, 103*(11), 1234-1247.

Shaukat, K., Luo, S., & Varadharajan, V. (2023). A novel deep learning-based approach for malware detection. *Engineering Applications of Artificial Intelligence, 122*, 106030. https://doi.org/10.1016/j.engappai.2023.106030

Shbair, W. M., Zarpelão, B. B., Miani, R. S., & Rossetto, A. G. (2020). Privacy-preserving traffic classification: A survey. *Journal of Network and Computer Applications, 169*, 102773. https://doi.org/10.1016/j.jnca.2020.102773

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

Sinha, P., Roy, P., & Thakur, R. (2025). A high-performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. ResearchGate. https://www.researchgate.net/publication/390035430

Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. (2020). DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Security and Communication Networks, 2020*, Article 8890306. https://doi.org/10.1155/2020/8890306

Tabassum, A., Erbad, A., Lebda, W., Mohamed, A., & Guizani, M. (2022). FEDGAN-IDS: Privacy-preserving IDS using GAN and federated learning. *Computer Communications, 192*, 299-310. https://doi.org/10.1016/j.comcom.2022.06.015

Tanka, O.-B., & Osei-Bonsu, K. (2024). Systematic literature review of IoT botnet DDoS attacks and evaluation of detection techniques. *Sensors, 24*(11), Article 3571. https://doi.org/10.3390/s24113571

Taşcı, B. (2024). Deep-learning-based approach for IoT attack and malware detection. *Applied Sciences, 14*(18), Article 8505. https://doi.org/10.3390/app14188505

Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., & Zhu, M. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access, 6*, 1792-1806. https://doi.org/10.1109/ACCESS.2017.2780250

Wanjau, S. K., Wambugu, G. M., & Oirere, A. M. (2022). Network intrusion detection systems: A systematic literature review of hybrid deep learning approaches. *International Journal of Emerging Science and Engineering (IJESE), 10*(7), 1-16. https://doi.org/10.35940/ijese.F2530.0610722

Wei, W., Chen, Y., Lin, Q., Ji, J., Wong, K. C., & Li, J. (2023). Multi-objective evolving long-short term memory networks with attention for network intrusion detection. *Applied Soft Computing, 139*, 110216. https://doi.org/10.1016/j.asoc.2023.110216

Xue, B., Zhang, M., Browne, W. N., & Yao, X. (2016). A survey on evolutionary computation approaches to feature selection. *IEEE Transactions on Evolutionary Computation, 20*(4), 606-626. https://doi.org/10.1109/TEVC.2015.2504420

Yaras, S., & Dener, M. (2024). IoT-based intrusion detection system using new hybrid deep learning algorithm. *Electronics, 13*(6), Article 1053. https://doi.org/10.3390/electronics13061053

Zegarra Rodríguez, D., Daniel Okey, O., Maidin, S. S., Umoren Udo, E., & Kleinschmidt, J. H. (2023). Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection. *PLOS ONE, 18*(10), Article e0286652. https://doi.org/10.1371/journal.pone.0286652