Peer-to-Peer Networking and Applications (2026) 19:32
https://doi.org/10.1007/s12083-025-02177-4

RESEARCH

IA-IDS: an intelligent adaptive intrusion detection system for IoT security using CNN, BiLSTM, and attention mechanism

Logeswari G[1] · Rudraksh Purbia[1] · Tamilarasi K[1] · Bose S[2]

Received: 22 May 2025 / Accepted: 19 November 2025

Abstract

The exponential growth of Internet of Things (IoT) ecosystems has introduced unprecedented cybersecurity challenges, making traditional Intrusion Detection Systems (IDS) increasingly ineffective in addressing sophisticated and evolving threats. Existing IDS frameworks often encounter issues such as high false positive rates, limited adaptability to new types of attacks, and poor efficiency in dynamic network environments. This paper presents an Intelligent Adaptive Intrusion Detection System (IA-IDS) that integrates advanced deep learning (DL) models with a dynamic feature selection strategy known as Dynamic Correlation-based Recursive Feature Selection (DCRFS). Unlike traditional anomaly-based IDS approaches that often rely on shallow models or handcrafted features, the proposed IA-IDS enhances anomaly detection capabilities by integrating Convolutional Neural Networks (CNNs), Bidirectional Long Short-Term Memory (BiLSTM) networks, and an attention mechanism to synergize their strengths for improved detection accuracy and adaptability. CNNs are used to extract spatial traffic patterns from raw network data, enabling the detection of complex behaviors and anomalies. BiLSTM networks capture long-term temporal dependencies within traffic sequences. An attention mechanism further enhances detection by focusing on the most critical segments of the temporal data, improving both performance and interpretability. The core contribution of this study is the development of the DCRFS algorithm, which enables real-time adaptation to changing threat landscapes by identifying and utilizing only the most pertinent features. This dynamic strategy overcomes the inefficiencies of static feature selection techniques by minimizing computational overhead while preserving high detection accuracy. Comprehensive evaluations on the BoT-IoT and TON-IoT datasets validate the system's performance, with the IA-IDS achieving accuracies of 98.12% and 98.67%, and F1-scores of 98.08% and 98.51%, respectively. In addition to high accuracy and F1-scores, the IA-IDS achieves low False Positive Rates of 0.65% on the BoT-IoT dataset and 0.79% on the TON-IoT dataset, demonstrating its robustness in reducing false alarms and enhancing detection reliability in real-world IoT scenarios. These outcomes highlight substantial improvements compared to traditional intrusion detection models. The proposed approach offers a scalable, intelligent, and adaptive IDS framework, well-suited to counter both known and emerging threats within complex IoT ecosystems.

Keywords Intrusion detection system · IoT networks · Deep learning · CNN · BiLSTM · Attention mechanism · Feature selection · Anomaly detection

✉ Logeswari G
logeswari.g@vit.ac.in

Rudraksh Purbia
rudraksh.purbia2021@vitstudent.ac.in

Tamilarasi K
tamilarasi.k@vit.ac.in

Bose S
sbs@annauniv.edu

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600 017, India

[2] Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai, Tamil Nadu 600 025, India

Published online: 19 December 2025

1 Introduction

The IoT supports a diverse range of applications in areas such as smart homes, healthcare, industrial automation, and transportation, representing a major advancement in object-to-object interaction and communication [1–3]. By embedding sensors, software, and connectivity into physical objects, IoT facilitates the collection and exchange of data, forming a network of interconnected devices that enhances productivity, automation, and data-driven insights. In smart homes, IoT technology facilitates home automation systems that control lighting, heating, security, and appliances, enabling remote management through smartphones and improving energy efficiency and convenience [4]. In the healthcare industry, wearable sensors and remote monitoring systems are IoT devices that provide medical practitioners with continuous health tracking and real-time data. These technologies enhance patient care, enable early detection of health issues, and help reduce hospital admission rates [5].

In industrial automation, IoT connects machinery, sensors, and control systems, allowing for predictive maintenance, improved supply chain management, and enhanced operational efficiency through real-time monitoring and analytics. In transportation, IoT enhances systems with connected vehicles, smart traffic management, and logistics optimization, improving safety, reducing congestion, and providing real-time information to drivers [6–8]. The integration of IoT in these sectors brings numerous benefits, including increased efficiency and automation by reducing the need for human intervention, data-driven insights that optimize processes, improved quality of life through better health monitoring and more comfortable living environments, and resource optimization by enabling more efficient use of energy and materials [9]. The swift growth of IoT has brought about considerable security concerns. IoT devices, frequently used in varied and resource-limited settings, are especially prone to cyber-attacks [10]. Typical attack vectors encompass Denial of Service (DoS), data probing, malicious control and operations, scanning, eavesdropping, and configuration errors [11, 12]. These threats can result in serious outcomes, including operational disruptions, data breaches, and the exposure of sensitive information. IDS play a vital role in network security by monitoring traffic and identifying anomalous behavior that may indicate potential security threats [13].

In IoT environments, IDS must tackle the distinct challenges arising from the diverse and ever-changing nature of these systems. Among these difficulties are the vast amount of data produced, the necessity for real-time detection, and the constrained processing capabilities of IoT devices [14]. IDS are generally categorized into two main types: signature-based and anomaly-based detection. Signature-based IDS detect threats by matching network traffic against a database of known attack patterns, making them effective for identifying previously encountered threats. However, they struggle to detect novel or zero-day attacks, potentially leaving networks vulnerable [5, 15].

In contrast, anomaly-based IDS detect intrusions by recognizing deviations from established behavioral norms. While they offer the advantage of identifying unknown threats, they often suffer from high false positive rates, which can cause alert fatigue and reduce overall reliability. These challenges underscore the necessity for more sophisticated and adaptive IDS approaches capable of addressing the dynamic and complex nature of IoT environments [16]. Despite their widespread use, existing IDS solutions exhibit several limitations when applied to IoT environments. Traditional IDS frequently encounter scalability problems since they are not built to manage the vast scale and variety of IoT networks, resulting in performance bottlenecks. Moreover, IoT devices typically possess constrained processing capabilities, memory, and battery life, posing difficulties in deploying resource-intensive IDS algorithms effectively. Unnecessary alarms and administrative burden can result from anomaly-based IDS's high false positive rate [17].

IoT networks are exposed to new risks and sophisticated attacks since many of the IDS that are now in use are unable to keep up with the constantly changing threat landscape. Considering the shortcomings of conventional IDS solutions, there is a growing demand for intelligent and adaptive systems capable of effectively protecting IoT networks. Enhancing detection accuracy and adaptability in such environments necessitates the integration of advanced Machine Learning (ML) and DL techniques [18].

1.1 Key contributions

While conventional anomaly-based IDS models often suffer from high false positive rates and lack adaptability, this research introduces an enhanced anomaly-based IDS framework that leverages deep learning and dynamic feature selection to overcome these limitations. The proposed framework introduces several key innovations:

- We introduce the DCRFS method, which dynamically selects the most contextually relevant features in real-time. This significantly reduces dimensionality and computational overhead while enhancing detection accuracy outperforming conventional statistical and metaheuristic feature selection methods.
- While CNN and BiLSTM have been explored in isolation or tandem, we extend their integration by embedding a temporal attention layer that highlights salient sequential patterns in the network traffic. This significantly improves

interpretability and the model's focus on critical intrusion indicators contributing to a reduction in false positives.
- The proposed IA-IDS has been rigorously evaluated against several hybrid deep learning models across two benchmark IoT datasets (BoT-IoT and TON-IoT). It consistently outperforms state-of-the-art baselines in all metrics, including accuracy, F1-score, precision, recall, and false positive rate.
- Our model achieves a balance between detection performance and computational efficiency. Despite employing deep learning, the integration of DCRFS ensures reduced execution time, making the approach scalable and suitable for real-world, resource-constrained IoT environments.

1.2 Research gap

IDS for IoT networks face several persistent challenges that undermine their effectiveness against sophisticated and evolving cyber threats [19]. Signature-based IDS struggle to detect zero-day and polymorphic attacks due to their reliance on predefined attack patterns, making them inadequate against emerging threats such as the Mirai botnet [20, 21]. Although anomaly-based IDS can identify previously unseen attacks, they often suffer from high false positive rates because of the dynamic and heterogeneous nature of IoT environments, where fluctuating device behaviors and traffic patterns make it difficult to distinguish between benign and malicious activity [22]. Additionally, scalability remains a critical issue, as traditional IDS frameworks are not optimized to process the high-volume, high-velocity, and diverse traffic generated by large-scale IoT deployments. Centralized IDS architectures further exacerbate these limitations by introducing bottlenecks and latency, leading to delayed threat detection [23, 24]. Despite numerous studies, existing solutions have not sufficiently addressed these core issues. This research addresses the gap by proposing an IA-IDS that combines deep learning with dynamic feature selection to effectively adapt to varying network conditions, reduce false positives, and scale across complex IoT infrastructures. The integration of CNN, BiLSTM, and an attention mechanism enables nuanced analysis of spatial and temporal traffic patterns, while the proposed DCRFS algorithm ensures computational efficiency and adaptability in real-time scenarios.

2 Related work

This section presents a critical overview of existing methodologies and advancements in IDS, particularly focusing on IoT environments. While traditional and machine learning-based IDS techniques have made significant strides, several limitations remain especially in handling adversarial attacks, high-dimensional data, and real-time performance.

2.1 Traditional and ML-based IDS in IoT

Qiu et al. [25] investigated the susceptibility of Deep Learning-based Network Intrusion Detection Systems (NIDSs) in IoT settings to adversarial attacks. They introduced a novel black-box attack strategy against the Kitsune NIDS, employing two main techniques to demonstrate the system's vulnerabilities. First, they employed model extraction to replicate the black-box model with a limited amount of training data, creating a surrogate model that closely mirrored the original NIDS. Second, they implemented saliency mapping to identify the most critical packet attributes influencing detection outcomes, enabling the efficient creation of adversarial examples. By altering less than 0.005% of the bytes in malicious packets, the attack achieved a success rate of 94.31%. This revealed the susceptibility of DL-based NIDSs, such as Kitsune, to adversarial attacks and highlighted the need for stronger security measures in IoT networks.

Alkadi et al. [26] introduced a hybrid DL approach combining BiLSTM with a blockchain framework known as the deep blockchain framework, aimed at enhancing privacy and detecting malicious activities. The accuracy of the approach was assessed, and it was compared to a number of ML methods, including support vector machines (SVM), random forest (RF), mixture localization-based outliers (MLO), and Naive Bayes (NB). However, the study noted limitations, particularly that the IDS performance may degrade under high network traffic and may struggle to effectively detect and alert against complex attacks. The study in [27] examined recent progress in Deep Neural Network (DNN)-based NIDS and underscored the susceptibility of DNNs to adversarial threats. The authors emphasized that many adversarial techniques originally developed for Computer Vision (CV) applications fail to account for the fundamental differences between CV and NIDS tasks. The article offers a comprehensive review of literature from 2015 onward, covering NIDS architectures, adversarial attack strategies, and corresponding defense mechanisms. It also presents a taxonomy of DL-based NIDS and discusses both white-box and black-box adversarial attacks within the intrusion detection domain.

Alotaibi et al. [28] surveyed adversarial ML strategies and defenses in IDSs. The authors pointed out the shortcomings of traditional IDSs, particularly their inability to accurately detect previously unseen attacks, and emphasized the promise of ML techniques in enhancing detection accuracy. However, they noted that adversarial attacks exploited ML-based IDSs, leading to the misclassification of network packets. The paper reviewed various types of adversarial attacks that affected IDSs and discussed defense strategies aimed at mitigating these risks. Yang et al. [29] developed a CNN-LSTM model to detect malicious request attacks in

IoT networks. Their approach incorporated semantic relationships and feature extraction using knowledge graphs prior to classification. The CNN-BiLSTM-attention architecture efficiently captures extended contextual information, leveraging an attention mechanism to emphasize important features. Elsayed et al. [30] developed an IDS tailored for smart home environments using the IoT Intrusion Dataset and implemented a hybrid BiLSTM-CNN model to enhance detection capabilities. Their methodology demonstrated superior performance compared to existing models and proved adaptable to various smart home network gateways.

2.2 Hybrid and attention-driven architectures

Hnamte and Hussain [31] combined CNN with BiLSTM networks to detect DoS attacks using the CICIDS2018 dataset, as well as IoT system attacks leveraging the Edge_IIoT dataset. Despite its complexity, further research is necessary to enable real-time implementation of their model. Alotaibi et al. [32] conducted research on the resilience of DL techniques in IDS against adversarial attacks. Their research introduced a CNN-based IDS model, which was tested using the CIS-IDS2017 dataset. Multiple methods were used to simulate adversarial attacks, with the model achieving an accuracy of 89.40% in their detection. Vitorino et al. [33] evaluated ML models against adversarial attacks and examined at IoT security issues. The study evaluated three supervised algorithms—Light Gradient Boosting Machine (LightGBM), RF, and Extreme Gradient Boosting (XGBoost)—alongside one unsupervised method, Isolation Forest. The authors proposed a framework to assess adversarial resilience. Using adaptive perturbation pattern generation, they crafted constrained adversarial examples and conducted evasion attacks on models trained with both standard and adversarial data. According to the study, severe gradient boosting produced the best results in multi-class tasks whereas random forest was less influenced in binary classification tasks. It illustrated the susceptibility of adversarial assaults to tree-based models and the advantages of adversarial training and security-by-design for enhancing the security of IoT.

Sharma et al. [34] introduced a new anomaly-based IDS for IoT environments leveraging deep learning. Their approach incorporated a filter-based feature selection method powered by a deep neural network to eliminate features with strong correlations. The model was adjusted using a range of parameters and hyperparameters, and it was applied to the UNSW-NB15 dataset, which had four assault types. The proposed IDS achieved an accuracy of 84%. To address class imbalance, GANs were utilized to generate synthetic data for underrepresented attack classes. This approach produced an improved accuracy of 91% with a balanced class dataset.

The possibility of adversarial attacks against ML-based network intrusion detectors for the IoT was investigated in the paper [35]. An adversarial sample generation technique was first created by the authors, who then evaluated its effects on IoT network intrusion detectors. They then proposed a novel framework named FGMD (Feature Grouping and Multi-model Fusion Detector), which combines feature grouping with multi-model fusion techniques to enhance defense against adversarial attacks. Two open datasets were used to test the framework and compare it to other methods that are already in use. The results showed that FGMD effectively defended against adversarial attacks and preserved performance even in the absence of such attacks. The study emphasized the limited research on adversarial attacks in IoT intrusion detection and made a notable contribution to the field.

Louati & Ktata [36] introduced a sophisticated IDS employing DL techniques within a multi-agent framework. This innovative strategy enables autonomous agents to work together in monitoring and reacting to suspicious behaviors, thereby strengthening the system's overall security. Similarly, Balakrishnan et al. [37] utilized Deep Belief Networks (DBNs) alongside Domain Generation Algorithms (DGAs) to accurately detect a range of cyber-attacks. Their approach capitalized on the DBNs' capacity to identify intricate patterns linked to malicious actions, while the DGAs contributed to enhancing detection precision.

The goal of the work [38] was to use ML models to create an intelligent IDS for IoT networks. An attacker system was utilized to carry out sniffing and poisoning assaults on a testbed that was set up using a wireless network, DHT11 sensor, and Node MCU. A Man-In-the-Middle (MITM) attack that altered data while it was being sent was simulated in the study. Among the various ML techniques evaluated, the Markov model achieved a perfect detection rate of 100% while maintaining a false alarm rate (FAR) of 19%. The Markov model demonstrated greater security for IoT networks by outperforming other algorithms as NB, SVM, decision trees, and AdaBoost in terms of sensitivity and true-positive rate.

Nandanwar et al. [39] proposed a neural network-based IDS for Industrial IoT (IIoT), which overcame the limitations of traditional signature-based methods by effectively detecting anomalies and zero-day attacks with high accuracy. Building on this, they introduced TL-BILSTM IoT, a transfer learning model that adapted pre-trained architectures to dynamic IoT threat scenarios and achieved superior detection performance [40]. Further extending their research to Industry 5.0, their 2025 study presented an explainable deep learning model for cyber-physical systems, which balanced interpretability with robust threat detection in critical infrastructure [41].

Earlier, their collaborative 2023 work with Kauhsik validated a deep learning framework for IoT intrusion prevention using optimized neural networks on real-world datasets [42]. Collectively, these studies underscored the transformative potential of deep learning in addressing evolving cyber threats, offering scalable, adaptive, and high-accuracy solutions for IoT and industrial security. A Modified Variational Autoencoder combined with Attention-LSTM has been developed to improve intrusion detection under class-imbalanced traffic conditions [43]. Another contribution, XIDINTFL-VAE, integrates XGBoost with class-wise focal loss in a variational autoencoder, achieving strong performance in imbalanced datasets [44]. Furthermore, a hybrid ensemble learning framework has been proposed for anomaly detection in industrial sensor networks and SCADA systems, specifically tailored for smart city infrastructures [45].

The limitations of single detection models, in particular, were addressed by the study [46] while discussing NIDS in IoT scenarios. The authors presented the ADCL collaborative learning-based detection framework, which improved intrusion detection by combining many models learned in comparable settings. The assessment showed that ADCL outperformed single models in detecting several types of assaults, with increases as high as 80% in adaptability, 42% in learning integrity, and 85% in model capacity F-scores. Moreover, the ADCL detection findings helped update individual models, increasing their F-score by 15%. These studies collectively illustrate the diverse methodologies and advancements in applying DL and hybrid approaches to tackle the evolving landscape of cyber threats across various domains, from industrial systems to network infrastructures. To provide a comparative analysis, we summarize various existing approaches in Table 1.

Existing IDS face significant challenges, including high false positive rates, inefficient feature selection, and limited adaptability to evolving cyber threats. Conventional methods frequently struggle to effectively capture both spatial and temporal patterns within network traffic, leading to less-than-ideal detection outcomes. To overcome these challenges, the proposed IDS integrates CNNs for robust spatial feature extraction, BiLSTM networks to model long-term temporal dependencies, and a dynamic DCRFS algorithm to select the most relevant features. Moreover, an attention mechanism is employed to emphasize key features, thereby improving the system's capability to detect anomalies accurately. These innovations collectively improve detection accuracy, computational efficiency, scalability, and resilience, offering a more robust solution to securing IoT networks against sophisticated and emerging intrusions.

3 Proposed methodology

Safeguarding systems and data integrity in the field of cybersecurity requires the capacity to identify and mitigate network intrusions. The dynamic and complex nature of contemporary cyber threats frequently renders traditional tactics ineffective. The proposed IA-IDS enhances IoT security by combining a dynamic feature selection algorithm, DCRFS, with a hybrid deep learning model. DCRFS continuously selects the most relevant features in real time, reducing computational complexity while maintaining detection accuracy. The deep learning pipeline integrates CNNs to extract spatial traffic patterns, BiLSTM networks to capture temporal dependencies, and an attention mechanism to focus on critical data segments. This combination enables IA-IDS to effectively detect both known and novel attacks with high accuracy and adaptability, making it suitable for dynamic and complex IoT environments. The proposed IDS architecture, depicted in Fig. 1, illustrates how these components work together synergistically to strengthen cybersecurity defenses.

3.1 Theoretical framework

By combining CNNs, BiLSTM networks, and advanced feature selection methods like Correlation-Based Feature Selection (CFS), Recursive Feature Elimination (RFE), and DCRFS, this approach delivers a sophisticated and adaptive IDS designed for the complex and constantly changing IoT landscape. This integration harnesses DL's capabilities in pattern recognition and temporal sequence modeling alongside dynamic feature selection, enabling accurate and efficient detection of malicious behavior—even as threats continue to evolve.

3.1.1 Convolutional neural networks in IDS

CNNs have proven to be exceptionally effective at processing grid-like data, such as images and tabular data, by automatically extracting spatial features without the need for manual intervention. In the context of IDS for IoT, CNNs analyze the raw network traffic, which is structured as a time series or as packet-level data. The primary component of a CNN, the convolutional layer, uses small filters (also called kernels) that slide over the input data, detecting local patterns, such as recurring packet sizes, source-destination relationships, and protocol types. This enables the CNN to identify subtle, low-level anomalies in network traffic, which could be indicative of an attack. The pooling layer in CNNs serves to reduce the dimensionality of the feature maps generated by the convolutional layers.

Table 1 Comprehensive summary of existing approaches

Reference	Approach	Dataset	Key Findings	Limitations
Qiu et al. [25]	Black-box attack on Kitsune NIDS	Kitsune	Achieved a 94.31% attack success rate by modifying < 0.005% of malicious packet bytes	Demonstrated vulnerability of DL-based IDS to adversarial attacks
Alkadi et al. [26]	BiLSTM with blockchain-based IDS	Various ML benchmarks	Improved privacy and detection	Performance degrades under high network traffic
Alotaibi et al. [28]	Adversarial ML strategies in IDS	Various IDS datasets	Highlighted ML-based IDS vulnerabilities and defense strategies	ML-based IDS misclassifies adversarial samples
Yang et al. [29]	CNN-LSTM with knowledge graphs	IoT network traffic data	Captured semantic relationships for better detection	Further research needed for real-time implementation
Elsayed et al. [30]	BiLSTM-CNN for smart home IDS	IoT Intrusion Dataset	Superior performance over traditional IDS	Adaptability to other IoT environments not explored
Hnamte & Hussain [31]	CNN-BiLSTM on DoS attacks	CICIDS2018, Edge_IIoT	Effective in detecting DoS attacks	Requires further optimization for real-time deployment
Alotaibi et al. [32]	CNN-based IDS against adversarial attacks	CIS-IDS2017	Achieved 89.40% accuracy	Adversarial robustness remains a challenge
Vitorino et al. [33]	ML models vs. adversarial attacks	IoT security datasets	LightGBM best for multi-class tasks; RF resilient in binary tasks	Tree-based models still susceptible to adversarial attacks
Sharma et al. [34]	DNN-based anomaly IDS	UNSW-NB15	Feature selection and GAN improved accuracy to 91%	Limited attack scenarios tested
Louati & Ktata [36]	Multi-agent DL-based IDS	IoT network data	Enhanced security via autonomous agents	Requires efficient coordination among agents
Balakrishnan et al. [37]	Deep Belief Networks (DBN) with Domain Generation Algorithms (DGA)	Cyber-attack datasets	Improved attack detection using DBN	Detection performance under dynamic attack scenarios not evaluated
Ma et al. [46]	ADCL collaborative learning IDS	IoT traffic datasets	85% improvement in model capacity, 42% in learning integrity	Performance under unseen attack types needs validation

By summarizing the spatial information, pooling helps improve computational efficiency while retaining the essential patterns that are most relevant for identifying attacks. Max pooling is commonly used to select the most significant features, ensuring that the CNN learns the most critical spatial relationships. Additionally, the activation functions such as Rectified Linear Units (ReLU) introduce non-linearity into the model, allowing CNNs to learn complex and abstract patterns that are crucial for effective detection of both known and novel attack signatures [47]. The fully connected layers in CNNs flatten the features extracted through convolution and pooling, passing them through a dense network that ultimately classifies the input data into different categories: normal or anomalous behavior. This classification process culminates in an output layer, typically using a soft-max or sigmoid activation function, to provide a probability distribution over possible attack types, such as DoS, Malicious Control, or Data Probing. CNNs eliminate the need for manual feature engineering, a task that is often cumbersome and prone to human error [48]. Instead, CNNs learn relevant patterns directly from the raw network data, which makes them highly efficient and robust for detecting spatial relationships in the high-dimensional and noisy data typical in IoT environments. These models are capable of recognizing the presence of specific attack patterns without needing prior knowledge of the exact nature of the attack.

The CNN architecture in the proposed IDS consists of multiple convolutional layers, each employing kernel-based feature extraction to identify critical spatial patterns in network traffic. Each convolutional layer applies a set of filters that slide over the input feature space, capturing local dependencies and reducing dimensionality. This process is followed by batch normalization, which stabilizes learning by normalizing feature distributions, and ReLU activation, which introduces non-linearity to enhance feature learning. To further improve feature selection and reduce redundant information, max pooling layers are employed, which down-sample feature maps while preserving the

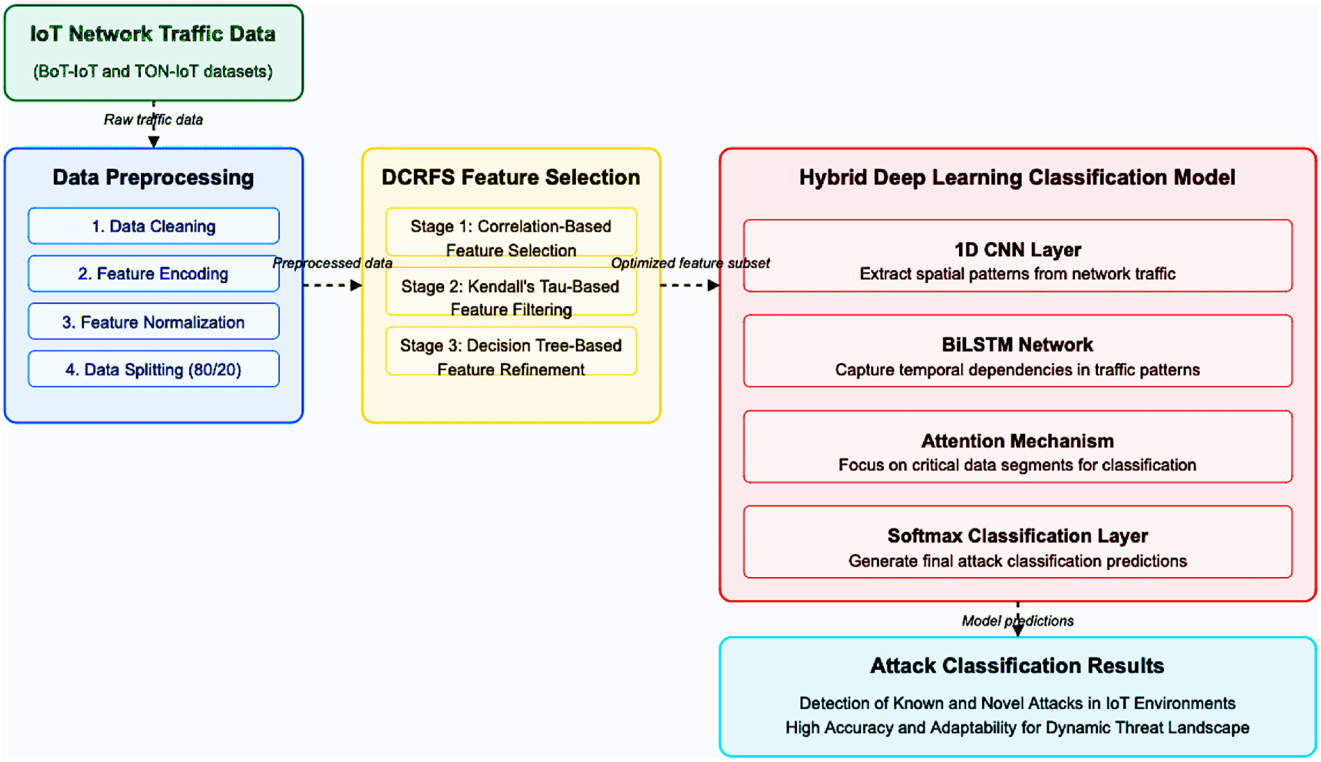

Fig. 1 Architectural diagram of proposed IA-IDS

most significant spatial characteristics. The final CNN output is then fed into a BiLSTM layer, which captures long-term dependencies and bidirectional temporal correlations in network behavior. This hybrid CNN-BiLSTM approach ensures both efficient spatial encoding and robust sequential learning, making the proposed system highly resilient to adversarial intrusion attempts. By leveraging CNN for spatial feature extraction and BiLSTM for sequential pattern learning, the proposed IDS demonstrates enhanced adaptability in detecting sophisticated adversarial attacks in IoT networks. The system's design ensures scalability, real-time processing efficiency, and robustness against evolving cyber threats, thereby significantly improving network security.

Bidirectional long short-term memory networks in IDS While CNNs excel at capturing spatial patterns, IoT networks often exhibit temporal behaviors, where the sequence of events and their timing are crucial for identifying malicious activities. This is where BiLSTM networks become valuable. A BiLSTM, a type of Recurrent Neural Network (RNN), is specifically designed to handle sequential data by capturing long-term dependencies and overcoming the vanishing gradient issue that often hampers the performance of traditional RNNs. BiLSTMs are particularly useful in IDS for analyzing network traffic patterns over time, capturing both short-term fluctuations and long-term trends. The LSTM units, which consist of memory cells and gates (input, forget, and output gates), manage the flow of information through the network, allowing it to remember important events over long periods and forget irrelevant ones. This selective memory helps prevent the model from being overwhelmed by noise or irrelevant data, improving its ability to detect subtle attack patterns that may unfold over time [49].

What sets BiLSTMs apart from traditional RNNs is their bidirectional processing capability. BiLSTM networks process the data sequence in both forward and backward directions, capturing not only past events but also future events. This bidirectional analysis allows the network to detect dependencies in the sequence that might otherwise be overlooked by unidirectional models. For instance, an attack may manifest as a delayed response to an earlier event, and a BiLSTM can capture these time-dependent patterns, making it highly suitable for detecting complex, time-sensitive anomalies or attack strategies in IoT traffic. In our proposed hybrid IDS, the BiLSTM layer processes the feature representations extracted by CNNs, providing enhanced temporal-spatial awareness for real-time intrusion detection.

3.1.2 Correlation-based feature selection in IDS

Feature selection is a critical step in improving the performance and efficiency of IDS. CFS is a statistical method

that evaluates the relevance of features by measuring their correlation with the target variable (e.g., whether the traffic is normal or anomalous) and their inter-correlation with other features [50]. The goal of CFS is to identify a subset of features that are most strongly correlated with the target variable while minimizing redundancy between them. CFS works by calculating the correlation coefficient between each feature and the target variable and considering how features relate to each other. Highly correlated features that provide redundant information are discarded. The result is a more compact set of features that preserves the most important information for detecting attacks [51]. In IoT IDS, relevant features might include characteristics such as packet size, time intervals between packets, or specific protocol flags that correlate strongly with attack types. By removing irrelevant or redundant features, CFS enhances computational efficiency and boosts the model's anomaly detection performance by concentrating on the most informative data.

In IoT intrusion detection, where real-time analysis is crucial, our proposed IDS integrates CFS within its feature selection pipeline, ensuring that only the most informative network characteristics are retained. This selective approach enhances the detection of zero-day attacks and anomalous behaviors, particularly in dynamic IoT environments where attack patterns continuously evolve.

3.1.3 Recursive feature elimination in IDS

RFE is another feature selection technique that iteratively evaluates the importance of each feature in a given model and removes the least significant ones. RFE starts by training a model (typically a linear classifier) on all available features, ranking them by their contribution to model performance. It then iteratively removes the least significant features, retraining the model at each step, until the most effective subset is identified. RFE is especially valuable in intrusion detection systems, as it simplifies the model while preserving only the most influential features, thereby enhancing both performance and interpretability. This is essential for increasing the model's interpretability and ensuring faster detection times without compromising performance [52]. For example, RFE might prioritize features such as network packet size or port activity while eliminating less important features, ensuring that the IDS remains responsive to the most critical indicators of attack.

In our proposed hybrid IDS, RFE plays a key role in refining the feature subset, complementing CFS by further eliminating redundant or weakly correlated attributes. This dual-stage selection strategy improves both computational efficiency and detection precision, making the system more adaptable to real-world IoT scenarios where feature distributions may shift over time.

3.1.4 Dynamic correlation-based recursive feature selection in IDS

DCRFS is a hybrid feature selection method that integrates the advantages of both CFS and RFE while introducing a dynamic aspect to account for evolving data patterns. Unlike conventional approaches where feature relevance remains fixed, DCRFS continuously reassesses feature importance in response to shifts in the network environment. This dynamic capability is especially vital in IoT networks, where the introduction of new devices, protocols, or attack vectors can rapidly alter traffic behavior. The method begins with correlation analysis to identify features highly associated with the target variable, followed by a recursive elimination process to discard less significant features. What sets DCRFS apart is its ability to adapt to changes in data distribution over time, ensuring that the selected features remain relevant and effective. This adaptability plays a key role in enhancing the detection of both known and emerging threats in ever-changing IoT ecosystems.

By combining CNNs, BiLSTM networks, and advanced feature selection techniques such as CFS, RFE, and DCRFS, this IDS framework provides a highly effective and adaptive solution for detecting sophisticated cyber threats in IoT networks. CNNs are utilized to autonomously extract spatial features from raw network traffic, while BiLSTM networks effectively model temporal dependencies within the data. Complementing these, feature selection techniques ensure that the detection process focuses exclusively on the most relevant and informative attributes, thereby enhancing both accuracy and efficiency. This synergy allows the system to accurately identify a wide range of attacks, including both known and novel threats, while minimizing computational complexity and adapting to changes in the network environment. The result is a highly efficient, robust, and scalable IDS that can effectively safeguard IoT networks against an ever-evolving landscape of cyber threats. In our proposed hybrid IDS, DCRFS enhances the CNN-BiLSTM model's adaptability, ensuring that only the most relevant and up-to-date features contribute to attack classification.

3.2 Data pre-processing

The BoT-IoT and TON-IoT datasets, widely adopted for evaluating IDS in IoT environments, contain rich, multi-dimensional network traffic data representing a wide array of attacks and normal behavior. However, these datasets present several preprocessing challenges due to their inherent characteristics, such as high dimensionality, class imbalance, presence of noise and outliers, mixed-type attributes (categorical and numerical), and temporal correlations. Therefore, an extensive data preprocessing pipeline

is employed before feeding the data into the deep learning components of the proposed IA-IDS framework. This pipeline comprises six sequential steps: data cleaning, feature encoding, feature normalization, temporal windowing, data labeling, and data splitting.

3.2.1 Data Cleaning

The raw BoT-IoT and TON-IoT datasets may include corrupted, incomplete, or redundant entries. The first stage of preprocessing involves cleaning these datasets by handling missing values, removing duplicates, and eliminating outliers. Missing values are addressed using mean imputation, where each missing entry x_i is replaced with the arithmetic mean of the observed values for the corresponding feature. Formally, this is given by Eq. (1):

$$x_i' = \bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i, \; x_i, \neq \; null \tag{1}$$

where, x_i denotes original missing value in feature column and x_i' represents Imputed value replacing missing x_i and n is the number of non-null values used to calculate mean.

Duplicates are removed by ensuring each record r_i is unique in the dataset D. Formally, if $r_i = r_j$ for any $i \neq j$, then one of the duplicates is discarded as shown in Eq. (2):

$$\forall i, \; j \in D, \; r_i \neq \; r_j \; if \; i \neq \; j \tag{2}$$

where, r_i and r_j are the data records in the dataset D.

Additionally, outlier removal is performed based on the Z-score method, where the Z-score for each value x is computed by using Eq. (3):

$$z = \frac{x - \mu}{\sigma} \tag{3}$$

Here, x is the feature value being normalized, μ is the mean and σ is the standard deviation of the feature. Any data point with |z|>3 is considered an outlier and removed, helping to improve the robustness of the model.

3.2.2 Feature Encoding

Feature Encoding is applied to categorical variables such as protocol types (TCP, UDP, ICMP). These are transformed via one-hot encoding into binary vectors to allow the deep learning models to process them numerically without implying any ordinal relationship. After encoding, feature normalization is conducted to scale all numeric features into the range [0,1][0,1] using Min-Max normalization. This scaling is expressed as shown in Eq. (4):

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{4}$$

where x is the original feature value, x_{min} and x_{max} are the minimum and maximum values of the feature across the dataset, and x_{norm} is the normalized value. Normalization ensures that all features contribute proportionally to model training and prevents dominance of features with large numeric ranges. Lastly, the cleaned and normalized datasets are split into training and testing sets using an $80-20$ split ratio as shown in Eq. (5).

$$N_{train} = 0.8 \times N, \; N_{test} = 0.2 \times N \tag{5}$$

where N_{train} and N_{test} represent the number of samples in the training and testing subsets, respectively. This split ensures the model is trained on the majority of the data while preserving a portion for unbiased evaluation. This preprocessing pipeline is applied uniformly to both BoT-IoT and TON-IoT datasets, ensuring consistency and facilitating effective feature learning for the proposed IA-IDS.

3.3 Feature extraction

The DCRFS algorithm is an advanced hybrid feature selection method that refines the feature subset iteratively, ensuring the most relevant features are retained while redundant and weakly correlated ones are eliminated. The process involves three key stages: correlation-based feature selection, Kendall's Tau-based filtering, and decision tree-based refinement. Each stage systematically enhances the feature subset by employing statistical and machine learning techniques.

Stage 1: Correlation-based feature selection The feature selection process begins with computing the Pearson correlation coefficient (ρ) for continuous features to assess their linear relationship with the target variable [53]. Pearson correlation is defined as Eq. (6):

$$\rho \; (X_i, \; T) = \frac{\sum \left(X_i - \bar{X_i} \right) (T - \bar{T})}{\sqrt{\sum \; (X_i - \bar{X_i})^{\; 2}} \sqrt{\sum \; (T_i - \bar{T_i})^{\; 2}}} \tag{6}$$

where X_i represents the feature values, T is the target variable, and $\bar{X}_i$ and $\bar{T}$ are their respective means. Features with $\rho(X_i,T)$ above a predefined threshold (ρ^{th}) are selected, ensuring only strongly correlated features are included. For categorical target variables, Point-Biserial Correlation (r_{pb}) is used, given by Eq. (7).

$$r_{pb} = \frac{\bar{X}_1 - \bar{X}_0}{s} \times \frac{n_0 n_1}{\sqrt{n(n-1)}} \tag{7}$$

where $\bar{X}_1$ and $\bar{X}_0$ are the means of X_i for two different classes, s is the pooled standard deviation, and n_1, n_0, and n are the sample sizes. The feature with the highest correlation is added first, and subsequent features are included only if they significantly contribute to the overall correlation strength.

Stage 2: Kendall's Tau-based feature filtering Once an initial subset is obtained, Kendall's Tau coefficient (τ) is used to evaluate ordinal associations between features and the target variable [54]. Kendall's Tau measures rank correlation, given by Eq. (8):

$$\tau = \frac{C - D}{C + D} \tag{8}$$

where C and D represent the number of concordant and discordant feature-target value pairs, respectively. Features with τ values below a threshold (τth) are removed to eliminate weakly correlated or noisy features. This step ensures that features included in the subset maintain a strong ranking relationship with the target.

Stage 3: Decision tree-based feature refinement To further optimize the feature subset, a Decision Tree Classifier is trained using the selected features. The importance of each feature is evaluated by analyzing the change in classification accuracy when the feature is removed. The accuracy before and after removing a feature f is computed as Eqs. (9) and (10):

$$ACC_{prev} = \frac{Corrct\ Predictions\ (before\ removal)}{Total\ samples} \tag{9}$$

$$ACC_{new} = \frac{Corrct\ Predictions\ (after\ removal)}{Total\ samples} \tag{10}$$

If $ACC_{new} > ACC_{prev}$, the feature is deemed redundant and removed. This process is repeated for all features until no further accuracy improvements occur. By leveraging decision trees, this step ensures that the final feature subset contains only the most predictive attributes while eliminating redundant ones. The DCRFS algorithm iterates until no further improvement in classification accuracy is observed. Additionally, it stops if the feature subset reaches an optimal balance between dimensionality reduction and predictive performance, performance, ensuring that only the most valuable features are retained.

Algorithm 1: DCRFS Algorithm

Input: D: Pre-processed dataset, T: Target variable, ρ_{th}: Correlation threshold, τ_{th}: Kendall's Tau threshold.
Output: S: Final selected feature subset
Steps:
Initialization:
1: Initialize empty feature subset: S ← ∅.
Correlation-based Feature Selection:
2: While Corr(S, T) < ρ_{th}, do:
3: Select f_{max} = arg $max_{\mathbf{f}\in D\setminus S}\ PearsonCorr\ (f,T)$
4: Update S ← S ∪ $\{f_{max}\}$
Kendall's Tau-based Feature Refinement
5: For each f ∈ S, do:
6: Compute $\tau_f = kendallTau\ (f,T)$
7: If $\tau_f < \tau_{th}$: S← S \ {f}
Recursive Feature Selection using Decision Tree:
8: Let ACC_{prev}= TrainDT (S,T)
9: For each f ∈ S do:
10: Create a new subset: $S' = S \setminus \{f\}$
11: $ACC_{new} = TrainDT(S',T)$
12: If $ACC_{new} \geq ACC_{prev}$:
13: update S←S'
14: Set $ACC_{prev} \leftarrow ACC_{new}$
Termination
15: Repeat steps 2-14 until no further improvement in ACC_{prev}.
16: Return S

3.4 Classification model

The classification module of the proposed IA-IDS is responsible for identifying the specific type of cyberattack in an IoT environment by employing a hybrid deep learning framework comprising CNN, BiLSTM units, an Attention Mechanism, and a final Softmax-based prediction layer. The input to this module is a temporally ordered feature matrix $X \in R^{T\times F}$, where T denotes the number of time steps in a given sequence and F represents the number of features selected via the DCRFS.

To begin with, a 1D CNN layer is applied to each time step in the sequence to extract localized spatial patterns. The convolution operation at time step t is defined as:

$$FCC_{(t)} = ReLU\ (W_c \times\ X_t + b_c) \tag{11}$$

In Eq. (11), $FCC_{(t)} \in R^{d_c}$ is the is the CNN-transformed feature vector at time step t, $W_c \in R^{k \times F}$ is the convolutional kernel with window size k, $X_t \in R^F$ is the raw input vector at time step t, $b_c \in R^{d_c}$ is a bias term, and ReLU(x)=max(0,x) is the Rectified Linear Unit activation function used to introduce non-linearity. This step enhances detection of critical local feature interactions such as sudden spikes in traffic or irregular port access patterns.

The CNN output is passed into a Bidirectional LSTM layer to capture both past and future temporal dependencies across the sequence. The BiLSTM computes two separate hidden states for each time step t: one in the forward direction and one in the backward direction $\overleftarrow{h_t}$. These are concatenated to form the complete hidden representation:

$$h_t = [\overrightarrow{h_t}; \overleftarrow{h_t}] \tag{12}$$

In Eq. (12), $h_t \in R^{2d_h}$, with d_h being the dimensionality of each LSTM direction. The forward LSTM, $LSTM_{fw}$ processes the sequence from t=1to T, while the backward LSTM, $LSTM_{bw}$, operates from t=T to 1. This dual encoding helps in understanding attack patterns that are temporally complex or exhibit dependencies over long time horizons.

Not all time steps contribute equally to final classification. Hence, an attention mechanism is employed to weigh each h_t based on its contextual importance. The attention score e_t for each time step is computed using a learnable transformation as shown in Eq. (13).

$$e_t = \tanh(W_a h_t + b_a) \tag{13}$$

where $W_a \in R^{d_a \times 2d_h}$ and $b_a \in R^{d_a}$ are attention parameters and d_a is the dimensionality of the attention space. These raw scores are then normalized via the softmax function to derive attention weights α_t:

$$\alpha_t = \frac{\exp(e_t)}{\sum_{k=1}^{T} \exp(e_k)} \tag{14}$$

The attention weights indicate the relative importance of each time step. A context vector c$\in R^{2d_h}$ is computed as the weighted sum of the hidden states as shown in Eq. (15).

$$c = \sum_{t=1}^{T} \alpha_t h_t \tag{15}$$

This context vector captures the most relevant temporal features needed for accurate classification.

To generate the final prediction, the context vector cc is passed through a fully connected layer, which computes the raw score or logit z_i for each class $c_i \in \{1,2,\ldots,C\}$, where C is the number of attack categories:

$$z_i = W_i^\top c + b_i \tag{16}$$

In Eq. (16), $W_i \in R^{2d_h}$ is the weight vector and $b_i \in$ R is the bias term associated with class i. These logits are then normalized using the Softmax activation function in Eq. (17) to obtain class probabilities:

$$P(y = c_i \mid c) = \frac{\exp(z_i)}{\sum_{j=1}^{C} \exp(z_j)} \tag{17}$$

The final predicted class label $\hat{y}$ is obtained by selecting the class with the highest probability:

$$\hat{y} = \arg max_i \; P(y = c_i \mid c) \tag{18}$$

For training the model, the Categorical Cross-Entropy Loss is minimized, defined as in Eq. (19):

$$L_{CCE} = -\sum_{i=1}^{C} y_i \log(P(y = c_i \mid c)) \tag{19}$$

where $y_i \in \{0,1\}$ is the one-hot encoded true label for class c_i, and $P(y = c_i \mid c)$ is the predicted probability from Eq. (17). This loss penalizes the model proportionally to its confidence in incorrect predictions, thereby encouraging accurate and confident classification of intrusion types.

Attention mechanism In our proposed model, we employ the additive attention mechanism, also known as Bahdanau attention, due to its suitability for lightweight and interpretable architectures. Compared to self-attention or multi-head attention, additive attention is computationally less expensive and performs effectively with smaller datasets. This is especially important for our task, where explainability and resource efficiency are crucial. Furthermore, additive attention computes alignment scores using a feedforward network, which offers intuitive insight into the relevance of each input feature or time step.

4 Performance evaluation

4.1 Dataset

This research utilizes the BoT-IoT and ToN-IoT datasets, both of which are publicly accessible and widely recognized as standard benchmarks for evaluating intrusion detection systems in IoT environments. These datasets provide extensive network traffic data, supporting the training and assessment of machine learning-based IDS models tailored to IoT scenarios. The BoT-IoT dataset replicates realistic IoT network behavior by generating both normal and malicious

traffic. It includes crucial attributes such as timestamps, IP addresses for source and destination, port information, communication protocols, flow durations, packet sizes, and various flow-based statistical metrics. It also offers clearly labeled instances to support supervised learning, facilitating the differentiation between legitimate and attack traffic. The dataset encompasses a wide range of cyber threats, including Distributed Denial of Service (DDoS), DoS, botnet activity, keylogging, scanning, data theft, and operating system-level intrusions. Its rich feature set and detailed labeling make highly suitable for developing and validating IDS solutions in IoT-focused security research. A detailed distribution of benign and malicious records in the BoT-IoT dataset is presented in Table 2.

The ToN-IoT dataset encompasses telemetry data from both IoT and IIoT sensors, along with network traffic and system logs gathered from Windows and Linux (Ubuntu) environments. It contains over 22 million records, structured to support both binary classification (normal versus malicious) and multi-class classification across ten labels, which include nine distinct attack types and one category for legitimate activity. The attack types featured in the dataset include Backdoor, DoS, Distributed Denial of Service (DDoS), Injection attacks, Password attacks, Ransomware, Scanning, Cross-site Scripting (XSS), and Man-in-the-Middle (MITM) attacks. For this study, a refined subset consisting of 461,043 samples was extracted using a combination of random and stratified sampling techniques to ensure a representative and balanced distribution of normal and attack data. This selection facilitates a robust evaluation of the proposed model across a broad spectrum of attack scenarios. Table 3 presents a detailed summary of the extracted subset from the ToN-IoT dataset.

4.2 Experimental setup

To evaluate the proposed IA-IDS, a robust experimental setup was established to facilitate efficient training and thorough performance analysis. The implementation was conducted on a high-performance computing platform featuring a 10th Generation Intel Core i7 processor (2.31 GHz), 16GB of DDR4 RAM, and 512GB of SSD storage. For accelerated deep learning operations, the system was equipped with an NVIDIA GeForce RTX 2060 GPU with 6GB of VRAM. The development environment utilized either Ubuntu 20.04 LTS or Windows 10 (64-bit), with Python 3.8 as the core programming language. The model was built using deep learning libraries such as TensorFlow 2.9 and Keras 2.8, complemented by essential machine learning packages including Scikit-learn, NumPy, and Pandas. This configuration was chosen to ensure that the IDS could be rigorously evaluated in terms of efficiency, scalability, and its capability to detect a variety of intrusion attempts within IoT ecosystems.

Table 2 Data composition of normal and threat patterns in BoT-IoT

Behavior type	Number of instances
Normal	477
OS fingerprinting	17,914
Service scanning	73,168
DoS TCP	615,800
DoS HTTP	1485
DoS UDP	1,032,975
Data theft	6
Keylogging	73
DDoS UDP	948,255
DDoS TCP	977,380
DDoS HTTP	989

Table 3 Statistical overview of the selected ToN-IoT records

Behavior type	Number of instances
Normal	300,000
Backdoor	20,000
DDoS	20,000
DoS	20,000
Injection	20,000
Password	20,000
Ransomware	20,000
Scanning	20,000
XSS	20,000
MITM	1043

Hyper-parameter setting The hyperparameters for the proposed IA-IDS framework were optimized as shown in Table 4, ensuring balanced model complexity and performance.

4.3 Performance assessment parameters

The efficiency of the proposed system was evaluated using a range of standard performance indicators. The evaluation process compared the model's predictions with the ground truth labels, resulting in four primary classification metrics: True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). TP and TN represent correct identifications of malicious and normal behavior, respectively, while FP and FN denote incorrect classifications. These fundamental metrics serve as the basis for calculating higher-level performance measures such as accuracy, precision, recall, and the F1 score.

Accuracy as computed in (20) reflects the overall correctness of the model by measuring the ratio of accurate predictions (both normal and attack instances) to the total number of predictions made.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{20}$$

Table 4 Optimal hyperparameters for the proposed IA-IDS model

Component	Hyperparameter	Optimal value
DCRFS algorithm	Relevance threshold	0.3
	Redundancy threshold	0.8
CNN layers	Number of filters	64
	Kernel size	3
	Activation fnction	ReLU
BiLSTM layers	Number of units	128
	Number of layers	2
Attention mechanism	Attention type	Additive
	Attention size	64
Training parameters	Batch size	64
	Learning rate	0.0005
	Optimizer	Adam
	Epochs	50

Precision determines how many of the instances predicted as attacks were actually malicious, providing insight into the model's reliability in identifying threats. It is computed using Eq. (21).

$$Precision = \frac{TP}{TP + FP} \tag{21}$$

As computed in Eq. (22), Recall indicates the model's ability to correctly detect actual attack instances among all true malicious events.

$$Recall = \frac{TP}{TP + FN} \tag{22}$$

The F1 Score, calculated using Eq. (23), integrates both precision and recall through their harmonic mean, providing a comprehensive measure of model performance particularly useful in scenarios with imbalanced class distributions.

$$F1\ Score = \frac{2\ X\ (Precision\ X Recall)}{Precision + Recall} \tag{23}$$

In addition to Accuracy, Precision, Recall, and F1-Score, we now include the False Positive Rate (FPR), which is computed as shown in Eq. (24):

$$FPR = \frac{FP}{FP + TN} \tag{24}$$

Where, FP is False Positives (normal instances wrongly classified as attacks) and TN represents True Negatives (normal instances correctly classified).

A lower FPR indicates fewer false alarms, which is essential for practical intrusion detection deployment.

5 Discussion of findings

Table 5 presents the performance of various feature selection methods evaluated on the BoT-IoT and TON-IoT datasets. Using all features without selection yields respectable accuracy and F1-scores; however, applying feature selection techniques generally improves classification performance while reducing the number of features. Among the methods compared, the DCRFS method achieves the highest accuracy and F1-score on both datasets, with only 14 and 13 selected features for BoT-IoT and TON-IoT respectively. This indicates that DCRFS not only effectively reduces dimensionality but also enhances model performance significantly compared to traditional methods like Chi-Square, Mutual Information, and PCA, as well as metaheuristic approaches like GWO and PSO. Therefore, DCRFS stands out as a superior feature selection approach for improving intrusion detection systems in IoT environments.

The AU-ROC (Area Under the Receiver Operating Characteristic) curves for the BoT-IoT and TON-IoT datasets, as illustrated in the Fig. 2, demonstrate the classification performance of the proposed hybrid model. The BoT-IoT dataset achieved an AUC of 0.98, while the TON-IoT dataset recorded a slightly lower AUC of 0.95. These high AUC values indicate that the model is highly effective in distinguishing between benign and malicious traffic in both datasets. The curve for BoT-IoT consistently stays closer to the top-left corner, reflecting a superior true positive rate with minimal false positives. The TON-IoT curve, while slightly under the BoT-IoT line, still shows strong separability. Overall, the AU-ROC curves confirm the robustness and generalization capability of the proposed hybrid intrusion detection framework across diverse IoT environments.

In order to ensure a fair and unbiased comparison, we implemented and evaluated several hybrid intrusion detection models commonly reported in the literature. The hyperparameters for all models were tuned using a validation set, and training was conducted under identical experimental conditions to ensure consistency. This setup allowed us to empirically benchmark our proposed approach against diverse hybrid frameworks. The results presented in Table 6 and illustrated in Fig. 3 clearly demonstrate that the proposed DCRFS+CNN-Attn-BiLSTM model significantly outperforms all existing hybrid models on the TON-IoT dataset. With an accuracy of 98.67%, F1-score of 98.51%, precision of 98.60%, and recall of 98.45%, the proposed model surpasses the previous best-performing approach (QPSO+Transformer-BiLSTM) by notable margins across all evaluation metrics. This superior performance highlights the effectiveness of integrating dynamic feature selection with a deep hybrid architecture that combines convolutional,

Table 5 Comparison of feature selection methods on BoT-IoT and TON-IoT datasets

Method	#Features (BoT-IoT)	Acc (%)	F1-score	#Features (TON-IoT)	Acc (%)	F1-score
No Selection	38	96.24	0.956	34	95.01	0.942
Chi-Square	18	97.03	0.964	17	95.65	0.950
MI	20	97.38	0.967	18	96.23	0.956
PCA	15	96.72	0.960	14	95.83	0.948
GWO	16	97.85	0.972	16	96.80	0.961
PSO	17	97.68	0.970	15	96.49	0.958
DCRFS	14	98.47	0.981	13	97.92	0.975

attention, and recurrent layers for robust intrusion detection in IoT environments.

As shown in Fig. 4 and detailed in Table 7, the proposed DCRFS+CNN-Attn-BiLSTM model achieves superior performance compared to existing hybrid intrusion detection systems on the BoT-IoT dataset. It attains the highest values across all evaluation metrics: Accuracy (98.12%), F1-Score (98.08%), Precision (98.00%), and Recall (98.15%). This demonstrates that the integration of DCRFS with an attention-augmented CNN and BiLSTM classifier effectively captures complex intrusion patterns, outperforming models based on Grey Wolf Optimizer, Quantum PSO, Genetic Algorithm, and other metaheuristic feature selectors. The results underscore the advantage of dynamic

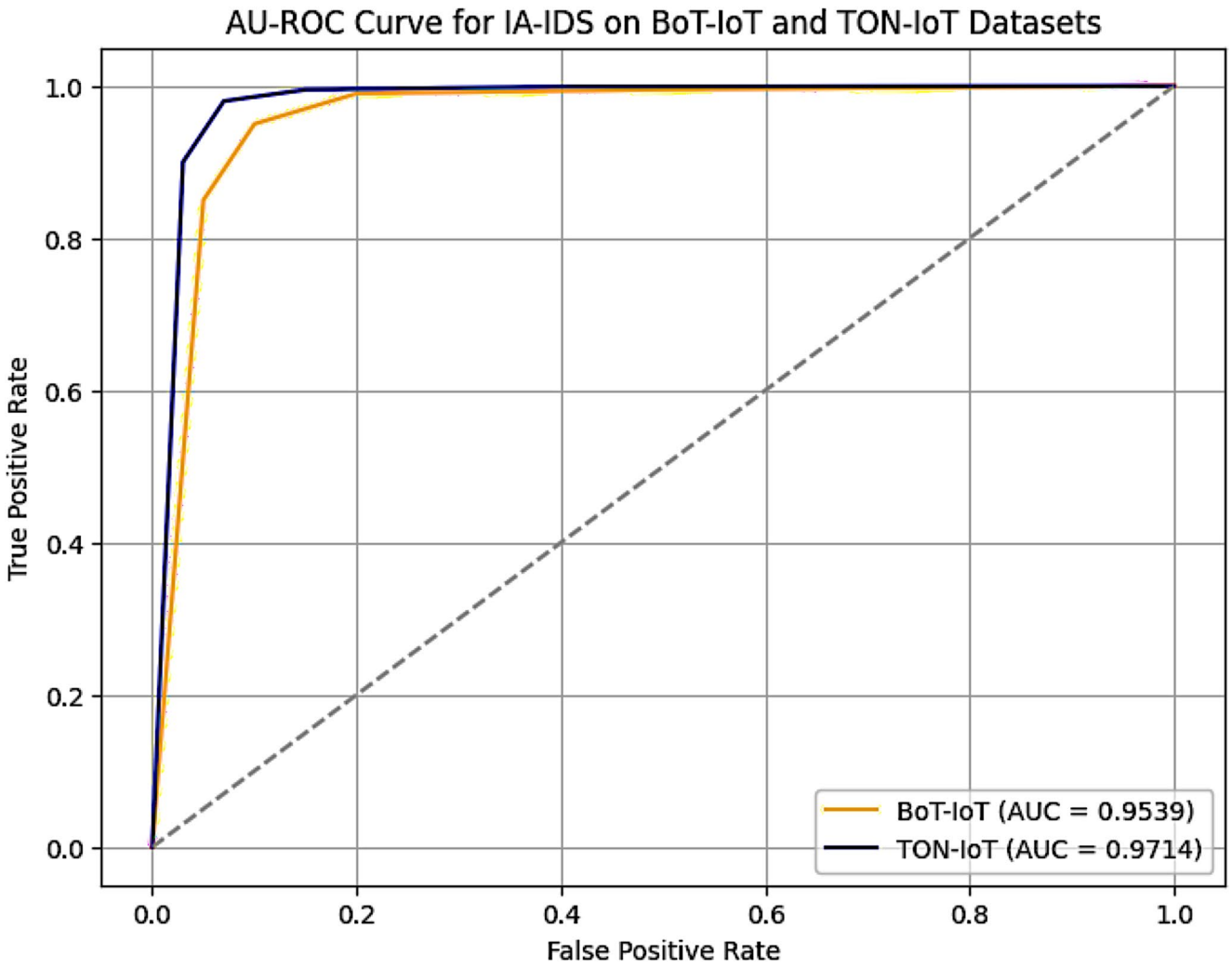

Fig. 2 AU-ROC curve for the IA-IDS model

Table 6 Comparison with existing hybrid models on TON-IoT

Model	Accuracy (%)	F1-score (%)	Precision (%)	Recall (%)
IG+LSTM-AE	95.34	95.12	95.30	94.95
ReliefF+CNN-GRU	96.08	95.85	96.00	95.70
QPSO+Transformer-BiLSTM	97.41	97.25	97.40	97.10
ALO+GRU	95.67	95.43	95.55	95.32
RFE+CNN-BiLSTM	96.54	96.32	96.45	96.20
Chi2+RNN-Attention	95.88	95.50	95.60	95.40
GA+AutoML-DNN	96.22	96.05	96.10	96.00
Boruta+LSTM-CNN	96.38	96.20	96.30	96.10
AE+CNN-GRU	95.75	95.52	95.60	95.45
(DCRFS+CNN-Attn-BiLSTM)	**98.67**	**98.51**	**98.60**	**98.45**

feature selection combined with deep learning architectures for enhancing IoT network security. The execution time comparison (Fig. 5) reveals that traditional machine learning models like Decision Tree, Random Forest, and LightGBM run significantly faster than deep learning models across both datasets. While deep learning models such as CNN, CNN+LSTM, Transformer, and BiLSTM+Attention generally require more time due to their complexity, the proposed IA-IDS model, which combines feature selection and advanced neural architectures, demonstrates a moderate execution time—higher than traditional models but comparable to other deep learning approaches. This indicates that the proposed model achieves a trade-off between detection accuracy and computational efficiency, making it well-suited for scenarios where both performance and processing speed are critical considerations. Additionally, the consistently lower execution times on the TON-IoT dataset indicate it may be less computationally demanding than BoT-IoT.

Performance evaluation on edge devices To assess the real-time applicability of IA-IDS in dynamic and resource-constrained IoT environments, we deployed the trained model

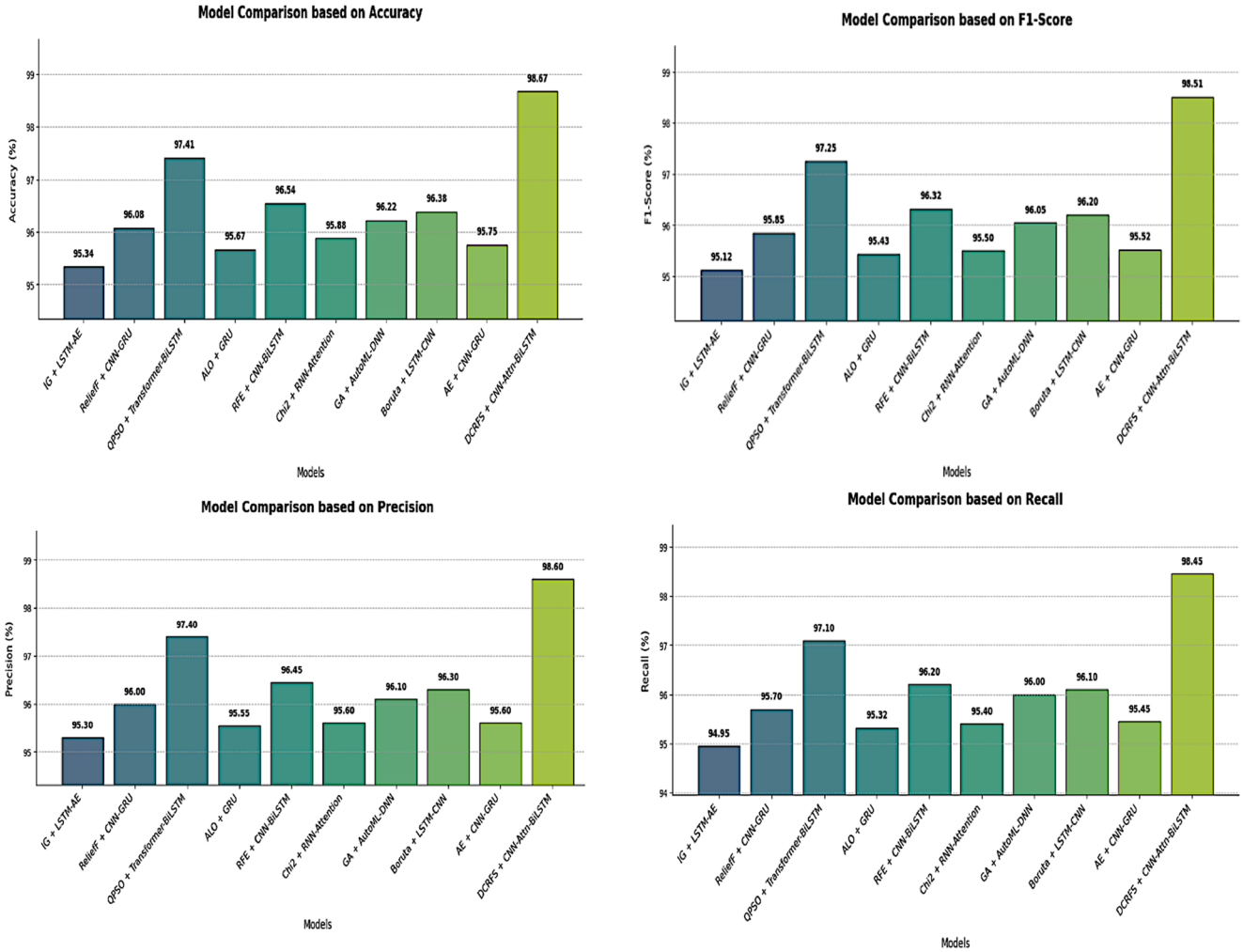

Fig. 3 Comparison with existing hybrid models on Ton-IoT

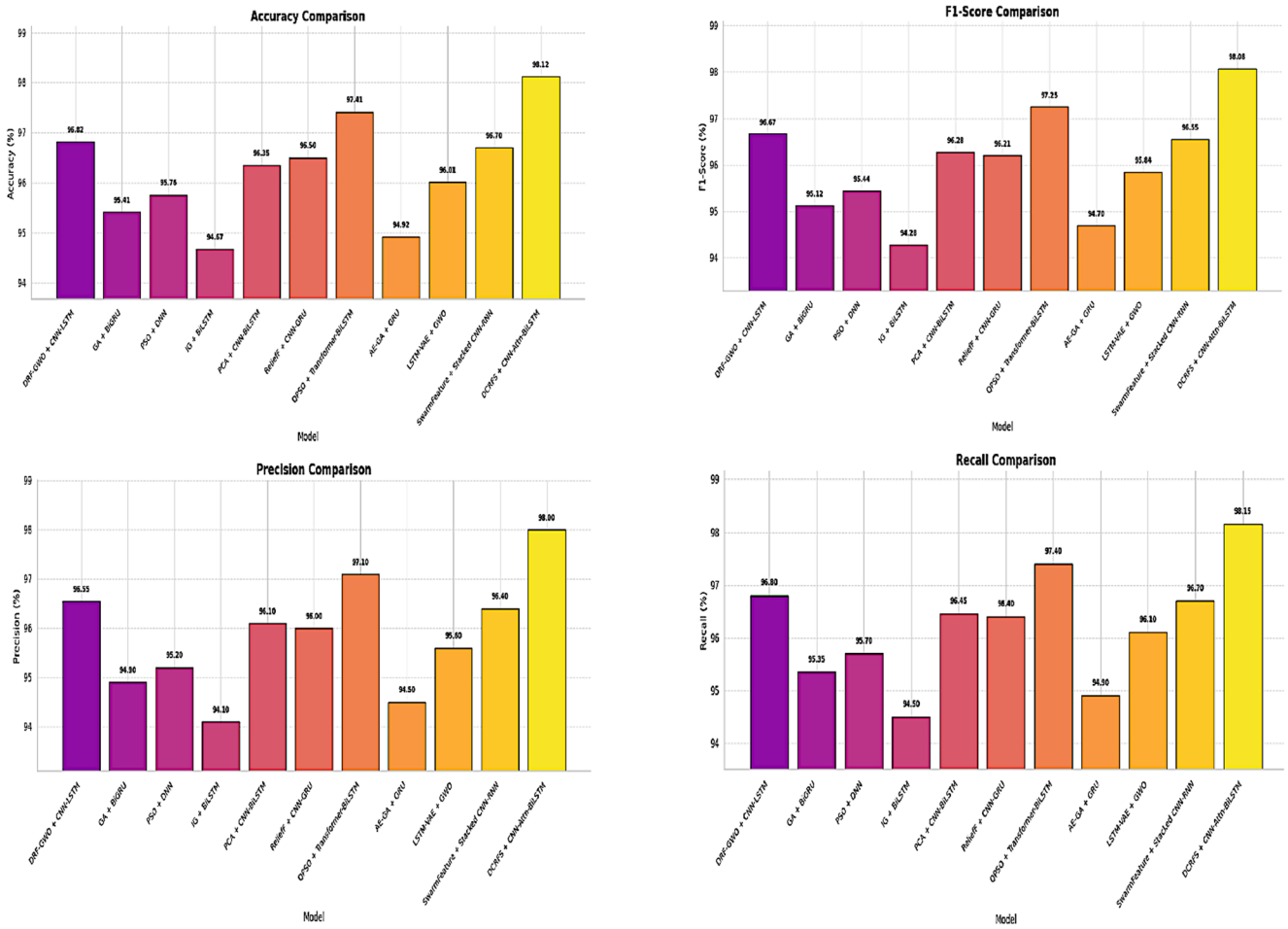

Fig. 4 Comparison with existing hybrid models on Bot-IoT

Table 7 Comparison with existing hybrid models on BoT-IoT

Model	Accuracy (%)	F1-score (%)	Precision (%)	Recall (%)
DRF-GWO + CNN-LSTM	96.82	96.67	96.55	96.80
GA + BiGRU	95.41	95.12	94.90	95.35
PSO + DNN	95.76	95.44	95.20	95.70
IG + BiLSTM	94.67	94.28	94.10	94.50
PCA + CNN-BiLSTM	96.35	96.28	96.10	96.45
ReliefF + CNN-GRU	96.50	96.21	96.00	96.40
QPSO + Transformer-BiLSTM	97.41	97.25	97.10	97.40
AE-GA + GRU	94.92	94.70	94.50	94.90
LSTM-VAE + GWO	96.01	95.84	95.60	96.10
SwarmFeature + Stacked CNN-RNN	96.70	96.55	96.40	96.70
DCRFS + CNN-Attn-BiLSTM	**98.12**	**98.08**	**98.00**	**98.15**

on a Raspberry Pi 4 Model B (1.5 GHz quad-core CPU, 4GB RAM), which emulates a typical edge device. The model achieved an average inference latency of 4.2 milliseconds per sample, with a throughput of approximately 238 samples per second and a peak memory usage of 114 MB during operation. These results affirm that IA-IDS is lightweight and efficient enough for real-time intrusion detection in IoT ecosystems, even on low-power hardware.

5.1 Adversarial robustness evaluation

To evaluate the resilience of the proposed IA-IDS model against adversarial attacks, we conducted experiments using the Fast Gradient Sign Method (FGSM), a widely used gradient-based attack technique. This method perturbs the input data in the direction of the gradient of the loss function to generate adversarial examples that can potentially mislead the model. We tested IA-IDS with adversarial samples generated at varying perturbation strengths ($\varepsilon = 0.01$ to 0.1) on the BoT-IoT dataset. Table 8 summarizes the classification accuracy under different levels of adversarial noise.

The results indicate that IA-IDS exhibits a robust performance under mild to moderate adversarial perturbations, with only a gradual degradation in accuracy as ε increases. Even at $\varepsilon = 0.1$, the accuracy remained above 94%, reflecting the model's capability to handle adversarial evasion

Fig. 5 Comparison of execution time

Table 8 Classification accuracy of IA-IDS under FGSM adversarial attacks with varying perturbation strengths (ε)

Epsilon (ε)	Accuracy (%)
0.00	99.12
0.01	98.84
0.03	98.17
0.05	97.45
0.07	95.81
0.10	94.42

attempts to a reasonable extent. These findings suggest that IA-IDS maintains a level of adversarial robustness suitable for real-world deployment in hostile environments.

5.2 Ablation study

5.2.1 DCRFS feature selection

To validate the effectiveness of the proposed DCRFS algorithm, we conducted an ablation study by comparing the performance of the complete IA-IDS model (which includes DCRFS) against a baseline version that uses all original features without any feature selection. Both variants use the same classification backbone (CNN-Attn-BiLSTM) and were trained and evaluated under identical experimental conditions on the BoT-IoT and ToN-IoT datasets. The results, presented in Table 9, show that the inclusion of DCRFS leads to consistent improvements in accuracy, precision, recall, F1-score, and a reduction in false positive rate. This indicates that DCRFS effectively eliminates irrelevant or redundant features, enhancing the model's generalization and computational efficiency.

These findings affirm that DCRFS plays a crucial role in boosting both accuracy and robustness of the IA-IDS framework while maintaining a lightweight computational profile suitable for real-time IoT deployments.

5.2.2 Attention mechanism

To validate our design choice, we conducted an ablation study comparing additive attention with self-attention and multi-head attention within our architecture. The results, detailed in Table 10, demonstrate that additive attention achieves comparable or better accuracy while maintaining reduced complexity and better interpretability.

5.3 Limitations

Despite the promising results, this study has certain limitations. The evaluation was carried out on benchmark datasets

Table 9 Performance comparison of IA-IDS with and without DCRFS on BoT-IoT and ToN-IoT datasets

Dataset	Model Variant	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
BoT-IoT	Without DCRFS	97.86	97.62	97.31	97.46	1.83
BoT-IoT	With DCRFS	**99.21**	**99.18**	**99.02**	**99.10**	**0.65**
ToN-IoT	Without DCRFS	96.73	96.55	96.28	96.41	2.04
ToN-IoT	With DCRFS	**98.94**	**98.82**	**98.71**	**98.76**	**0.79**

Table 10 Performance comparison of different attention mechanisms

Attention mechanism	Accuracy (%)	F1-score	Model size (MB)	Inference Time (ms/sample)
Additive attention	94.3	0.941	12.5	4.2
Self-attention	93.8	0.935	17.9	6.8
Multi-head attention	94.1	0.937	22.6	8.4

which, while widely adopted, may not fully capture the diversity and evolving nature of real-world network traffic, and the dataset size and imbalance may have influenced performance metrics such as the false positive rate. The generalizability of the proposed system to other domains, including IoT networks, industrial control systems, and encrypted traffic, remains to be validated, and adapting the framework to unseen environments may require retraining or fine-tuning. Furthermore, although the integration of feature selection and hybrid deep learning reduces complexity compared to many existing approaches, computational overhead still poses challenges for large-scale or resource-constrained environments. Finally, the scope of this work was limited to detection and classification, and did not extend to proactive prevention or automated response strategies. Future work will address these limitations by incorporating larger and more diverse datasets, optimizing computational efficiency, evaluating robustness across varied domains, and extending the framework to include adaptive prevention and real-time response mechanisms.

6 Conclusion and future work

The rapid expansion of IoT networks has brought forth significant security concerns that traditional IDS solutions are ill-equipped to handle. In response to these challenges, this study proposed an IA-IDS that leverages a hybrid deep learning architecture incorporating CNN, BiLSTM, and an attention mechanism. The integration of these components allows the system to effectively learn both spatial and temporal features in network traffic, improving the identification of complex and previously unseen attack patterns. Additionally, the proposed DCRFS method enhances system efficiency by dynamically selecting the most relevant features, ensuring adaptability to changing threat landscapes. Experimental validation on the BoT-IoT and TON-IoT datasets demonstrated the robustness and superior performance of IA-IDS, achieving high accuracy and F1-scores while maintaining low false positive rates. These findings highlight the potential of the proposed framework as a reliable and scalable solution for securing modern IoT environments. While the proposed IA-IDS model delivers promising results, there are several directions for future enhancement. One key area is real-time deployment and testing in diverse and large-scale IoT environments to assess the system's effectiveness under real-world conditions. Additionally, incorporating reinforcement learning techniques could enable the IDS to autonomously update its detection strategies based on feedback from live traffic. Exploring lightweight DL architectures may also help reduce computational costs, making the system more suitable for resource-constrained IoT devices. Further, integrating explainable AI methods can enhance transparency and trust in detection decisions, especially for critical applications. Finally, expanding the system's capabilities to detect adversarial attacks and encrypted traffic remains an essential direction for future research.

Supplementary information The online version contains supplementary material available at https://doi.org/10.1007/s12083-025-02177-4.

Author contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Logeswari G, Rudraksh Purbia, Tamilarasi K and Bose S. The first draft of the manuscript was written by Logeswari G and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability The datasets analysed during the current study are available in the Kaggle repository, https://www.kaggle.com/datasets/amaniabourida/ton-iot, https://www.kaggle.com/datasets/vigneshvenkateswaran/bot-iot.

Declarations

Consent for publication All authors have read and approved the manuscript.

Competing interests The authors declare no competing interests.

References

1. Jurcut AD, Ranaweera P, Xu L (2020) Introduction to IoT security. IoT Security: Adv Authentication, 27–64
2. Perwej Y, Haq K, Parwej F, Mumdouh M, Hassan M (2019) The internet of things (IoT) and its application domains. International Journal of Computer Applications 975(8887):182
3. Gardašević G, Veletić M, Maletić N, Vasiljević D, Radusinović I, Tomović S, Radonjić M (2017) The IoT architectural framework, design issues and application domains. Wirel Pers Commun 92:127–148
4. Gurani P, Sharma M, Nigan S, Soni N, Kumar K (2019) IoT smart city: introduction and challenges. Int J Recent Technol Eng 8(3):3484–3487
5. Aminanto E, Kim K (2016) Deep learning in intrusion detection system: An overview. In 2016 International Research Conference on Engineering and Technology (2016 IRCET). Higher Education Forum
6. Yadav N, Badal N (2020) Introduction to IoT technologies and its applications. Handbook of research on the internet of things applications in robotics and automation. IGI Global 238–264
7. Rathee P (2020) Introduction to blockchain and IoT. Advanced applications of blockchain technology 1–14

8. Soumyalatha SGH (2016), May Study of IoT: understanding IoT architecture, applications, issues and challenges. In 1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. Int Adv Netw Appl 478
9. Colizzi L, Caivano D, Ardito C, Desolda G, Castrignanò A, Matera M, Shi H (2020) Introduction to agricultural IoT. Agricultural internet of things and decision support for precision smart farming. Academic, pp 1–33
10. Chaudhary S, Mishra PK (2023) DDoS attacks in Industrial IoT: a survey. Comput Netw. https://doi.org/10.1016/j.comnet.2023.110015
11. Kadri MR, Abdelli A, Mokdad L (2023) Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments. IEEE Internet Things 101021
12. Hajiheidari S, Wakil K, Badri M, Navimipour NJ (2019) Intrusion detection systems in the internet of things: a comprehensive investigation. Comput Netw 160:165–191
13. Smys S, Basar A, Wang H (2020) Hybrid intrusion detection system for internet of things (IoT). J ISMAC 2(04):190–199
14. Logeswari G, Bose S, Anitha TJIA (2023) An intrusion detection system for SDN using machine learning. Intell Autom Soft Comput 35(1):867–880
15. Logeswari G, Thangaramya K, Selvi M, Roselind JD (2025) An improved synergistic dual-layer feature selection algorithm with two type classifier for efficient intrusion detection in IoT environment. Sci Rep 15(1):8050
16. Logeswari G, Bose S, Anitha T (2022) December Designing a SDN-Based Intrusion Detection and Mitigation System Using Machine Learning Techniques. International Conference on Advanced Communications and Machine Intelligence. Singapore, Springer Nature SingaporeAQ, pp 303–314
17. Natarajan B, Bose S, Maheswaran N, Logeswari G, Anitha T (2023) A Survey: An Effective Utilization of Machine Learning Algorithms in IoT Based Intrusion Detection System. In 2023 12th International Conference on Advanced Computing (ICoAC) (pp. 1–7). IEEE
18. Aminanto E, Kim K (2016) Deep learning in intrusion detection system: An overview. In 2016 International Research Conference on Engineering and Technology (2016 IRCET). Higher Education Forum
19. Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA (2023) Zero-day attack detection: a systematic literature review. Artif Intell Rev 56(10):10733–10811
20. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J (2019) Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2(1):1–22
21. Sutheekshan B, Basheer S, Thangavel G, Sharma OP (2024) Evolution of malware targeting IoT devices and botnet formation. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT). IEEE 5:1415–1422
22. Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E (2009) Anomaly-based network intrusion detection: techniques, systems and challenges. Computers Secur 28(1–2):18–28
23. Asharf J, Moustafa N, Khurshid H, Debie E, Haider W, Wahab A (2020) A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions. Electronics 9(7):1177
24. Alotaibi A, Rassam Ma (2023a) Adversarial machine learning attacks against intrusion detection systems: a survey on strategies and defense. Future Internet 15(2):62
25. Qiu H, Dong T, Zhang T, Lu J, Memmi G, Qiu M (2021) Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet Things J 8(13):10327–10335
26. Alkadi O, Moustafa N, Turnbull B, Choo K-KR (2020) A deep blockchain Framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet Things J 8:1
27. He K, Kim DD, Asghar MR (2023) Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 25(1):538–566
28. Alotaibi A, Rassam Ma (2023a) Adversarial machine learning attacks against intrusion detection systems: a survey on strategies and defense. Future Internet 15(2):62
29. Yang X, Peng G, Zhang D, Lv Y (2022) An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph. Secur Commun Networks. https://doi.org/10.1155/2022/4748528
30. Elsayed N, Zaghloul ZS, Azumah SW, Li C (2021) Intrusion detection system in smart home network using bidirectional LSTM and convolutional neural networks hybrid model, in Proc. 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 13
31. Hnamte V, Hussain J (2023) DCNNBiLSTM: an efficient hybrid deep learning-based intrusion detection system. Telematics and Informatics Reports 10:100053
32. Alotaibi A, Rassam Ma (2023b) Enhancing the sustainability of deep-learning-based network intrusion detection classifiers against adversarial attacks. Sustainability 15(12):9801
33. Vitorino J, Praça I, Maia E (2023) Towards adversarial realism and robust learning for IoT intrusion detection and classification. Ann Telecommun 78:401–412
34. Sharma B, Sharma L, Lal C, Roy S (2023) Anomaly based network intrusion detection for IoT attacks using deep learning technique. Comput Electr Eng 107:108626
35. Jiang S, Lin H, Kang H (2022) FGMD: a robust detector against adversarial attacks in the IoT network. Future Gener Comput Syst 132:194–210
36. Louati F, Ktata FB (2020) A deep learning-based multi-agent system for intrusion detection. SN Applied Sciences 2(4):675
37. Balakrishnan N, Rajendran A, Pelusi D, Ponnusamy V (2021) Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things. Internet Things 14:100112
38. Kiran KS, Devisetty RK, Kalyan NP, Mukundini K, Karthi R (2020) Building a intrusion detection system for IoT environment using machine learning techniques. Procedia Comput Sci 171:2372–2379
39. Nandanwar H, Katarya R (2024) Deep learning enabled intrusion detection system for Industrial IOT environment. Expert Syst Appl 249:123808
40. Nandanwar H, Katarya R (2024) TL-BILSTM IoT: transfer learning model for prediction of intrusion detection system in IoT environment. Int J Inf Secur 23(2):1251–1277
41. Nandanwar H, Katarya R (2025) Securing Industry 5.0: an explainable deep learning model for intrusion detection in cyber-physical systems. Comput Electr Eng 123:110161
42. Kauhsik B, Nandanwar H, Katarya R (2023) Iot security: a deep learning-based approach for intrusion detection and prevention. In 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT) (pp. 1–7). IEEE
43. Abdulganiyu OH, Tchakoucht TA, Saheed YK, El Mouhtadi M, Alaoui AEH (2025) Modified variational autoencoder and attention mechanism-based long short-term memory for detecting intrusions in imbalanced network traffic. Security and Privacy 8(3):e70044

44. Abdulganiyu OH, Tchakoucht TA, Saheed YK, Ahmed HA (2025) XIDINTFL-VAE: xgboost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder. J Supercomput 81(1):16
45. Saheed YK, Abdulganiyu OH, Ait Tchakoucht T (2023) A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and SCADA systems for smart city infrastructures. J King Saud Univ-Comput Inf Sci 35(5):101532
46. Ma Z, Liu L, Meng W, Luo X, Wang L, Li W (2023) ADCL: toward an adaptive network intrusion detection system using collaborative learning in IoT networks. IEEE Internet of Things J 10(14):12521–12536
47. Vinayakumar R, Soman KP, Poornachandran P (2017) Applying convolutional neural network for network intrusion detection. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE 1222–1228
48. Mohammadpour L, Ling TC, Liew CS, Chong CY (2018) A convolutional neural network for network intrusion detection system. APAN 46:50–55
49. Zhang S, Zheng D, Hu X, Yang M (2015) Bidirectional long short-term memory networks for relation classification. In Proceedings of the 29th Pacific Asia conference on language, information and computation (pp. 73–78)
50. Farahani G (2020) Feature selection based on cross-correlation for the intrusion detection system. Secur Commun Networks 2020(1):8875404
51. Shahbaz MB, Wang X, Behnad A, Samarabandu J (2016) On efficiency enhancement of the correlation-based feature selection for intrusion detection systems. In 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 1–7). IEEE
52. Ustebay S, Turgut Z, Aydin Ma (2018) Intrusion detection system with recursive feature elimination by using random forest and deep learning classifier. 2018 international Congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT). IEEE 71–76
53. Jebli I, Belouadha FZ, Kabbaj MI, Tilioua A (2021) Prediction of solar energy guided by pearson correlation using machine learning. Energy 224:120109
54. Puth MT, Neuhäuser M, Ruxton GD (2015) Effective use of spearman's and kendall's correlation coefficients for association between two measured traits. Anim Behav 102:77–84

Dr. Logeswari G received her B.E. degree in Computer Science and Engineering and her M.Tech. in Information Technology from Anna University, Chennai, India, in 2012 and 2014, respectively, followed by a Ph.D. in 2024. She is currently serving as Assistant Professor Sr in the School of Computer Science and Engineering at Vellore Institute of Technology, Chennai. With ten years of professional experience in teaching and research, she has published over 45 papers in esteemed international journals and conferences. Her primary research areas include Software-Defined Networks, Internet of Things, Machine Learning, Deep Learning, and Information Security.

Rudraksh Purbia has completed his undergraduate studies at Vellore Institute of Technology, Chennai. He is an enthusiastic student with academic interests in computer science and emerging technologies. His areas of focus include software development, data analysis, machine learning, and intelligent systems. He actively participates in academic projects and research-oriented activities, aiming to apply theoretical knowledge to solve real-world problems. His long-term goal is to contribute to innovative research and technological advancements in the field of computing.

Dr. Tamilarasi K holds a distinguished academic career with a Master of Engineering in Computer Science from Anna University, Chennai (2010), and a Ph.D. awarded in 2020. She currently serves as an Assistant Professor (Senior Grade-2) in the School of Science and Engineering at VIT University, Chennai Campus, with more than 15 years of extensive experience in academia. Her areas of expertise encompass Cloud Computing, Artificial Intelligence, Database Management Systems, and Healthcare Analytics. She has made significant contributions to her fields of specialization, with over 20 research papers published in reputed international journals and conference proceedings.

Dr. Bose S is a Professor in the Department of Computer Science and Engineering at the College of Engineering, Guindy, Anna University, Chennai. With over 25 years of experience in teaching, research, administration, and industry, his areas of specialization include Cybersecurity, Machine Learning, Blockchain Technology, Cloud Computing, and Future Generation Networks (5G/6G). He holds a Ph.D. in Information Security, with a focus on developing an anomaly-based, multi- layer Intrusion Detection and Prevention System for Ad-Hoc Networks. His research portfolio includes 69 international journal publications, 74 conference papers, and 4 granted patents, including innovations such as a blockchain-based secured document verification system using IoT. He has also authored notable academic books, including Cryptography and Network Security and Information Security. Over the years, he has successfully guided 18 Ph.D. scholars and is currently supervising 6 research scholars, continuing to lead groundbreaking research. In his administrative roles, he has made significant contributions as Dean, Deputy Director (CUIC), and Zonal Coordinator, advancing the growth of Anna University institutions. He is an active member of professional organizations such as IEEE, ACM, ISTE, and IETE, and frequently serves as a reviewer for prestigious journals and conferences. Dr. S. Bose contributions to academia and research have been recognized with multiple Best Paper Awards and the Distinguished Alumni Award for Academic Excellence. He remains dedicated to advancing innovative technologies to address real-world challenges and mentoring the next generation of researchers and professionals.