THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/9nt23663

An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem

Ghulam Abbas*, Asma Basit, Nasir Ayub, Shahid Rafique, Arshad Ali, Hamayun Khan, Muhammad Zunnurain Hussain

Chronicle

Article history
Received: Feb 12, 2026
Received in the **revised format:** Feb 23, 2026
Accepted: March 5, 2026
Available online: March 12, 2026

Ghulam Abbas*, is currently affiliated with the Faculty of Computer Science and Information Technology, Superior University, Lahore 54000, Pakistan.
Email: cybereengineer@gmail.com
Corresponding Author*

Asma Basit is currently affiliated with Department of Computer Science, Bahria University Karachi campus Pakistan.
Email: asmabasit.bukc@bahria.edu.pk

Nasir Ayub is currently affiliated as Deputy Head of Engineering at Calrom Limited, M1 6EG, United Kingdom
Email: nasir.ayyub@hotmail.com

Shahid Rafique is currently affiliated with the Faculty of Computer Science and Information Technology, Superior University, Lahore 54000, Pakistan
Email: shahidrafique0027@gmail.com

Arshad Ali is currently affiliated with the Faculty of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, 42351, Saudi Arabia.
Email:a.ali@iu.edu.sa

Hamayun Khan is currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
Email: hamayun.khan@superior.edu.pk

Muhammad Zunnurain Hussain is currently affiliated with the Bahria University Lahore Campus
Email:zunnurain.bulc@bahria.edu.pk

Abstract

The data growth is measured in exponential rates that are estimated at zettabytes to petabytes globally in the past decade in computer networks and Internet of Things (IoT) networks. The network growth has therefore also caused security issues. Nonetheless, it is difficult to monitor intrusion in this type of big data. Other advanced applications of the emerging networks are smart homes, smart cities, smart grids, smart devices, objects, e-commerce, e-banking, e-government, etc. The security and privacy threats facing most computer networks have led to the development of many Intrusion Detection Systems (IDS) in the recent past. The damage to data confidentiality, integrity, and availability will be experienced in the case of failure of the IDS prevention. The traditional methods are ineffective to match the sophisticated attacks. Rapid advancements in Internet of Things (IoT) infrastructure and Cloud Computing have expanded the digital threat landscape, necessitating a shift from outdated defensive frameworks. First, traditional signature-based systems are unable to identify zero-day attacks. In addition, classical Machine Learning (ML) systems cannot efficiently filter the 5G networks' encrypted traffic. Competitionally, Deep Learning (DL) systems can automate feature extraction, but individual systems have specific weaknesses. Convolutional Neural Networks (CNN) overlook the importance of temporal dependencies; Recurrent Neural Networks (RNN) are burdened by the vanishing gradient problem, excessive computation costs, and temporal dependencies. Such weaknesses can be alleviated using Hybrid Deep Learning (HDL) systems like CNN-LSTM, CNN-GRU, and Transformers. This paper systematically and critically assesses the recent literature on the "Efficient HDL-Based IDS." More than just descriptive summaries, we put forth a framework for a taxonomy of Sequential, Parallel, and Auxiliary architectures, which we assess using a Hybrid Efficiency Score (HES). We claim the existence of the "Efficiency-Accuracy Pareto Frontier." For instance, we position Parallel Ensembles at the bottom, imposing a 63% efficiency cost and Transformer-based and Sequential-Cascading hybrids at the top as real-time ready "Tier 1" systems. We finish the review by providing a reproducibility checklist and a "Green AI" roadmap to support sustainable network security.

Keywords: Intrusion Detection System (IDS); Hybrid Deep Learning; Network Security; Convolutional Neural Networks (CNN); Long Short-Term Memory (LSTM); Anomaly Detection; Cyber Threat Intelligence; Transformers; Big Data; Explainable AI (XAI).

INTRODUCTION

With the advent of the Fourth Industrial Revolution (Industry 4.0) the digital ecosystem is once again changing. More digitally oriented systems are being integrated with traditionally physical systems. The Internet of Things (IoT) combined with 5G and Software Defined Networking (SDN) has resulted in unprecedented levels of data traffic [1]. Hyper-connectivity allows new avenues for innovation and the rapid expansion of the Internet, but it also opens new potential paths for threat actors. Simple cyber incursions and breaches that created nuisances for users and slowed systems down are now escalating to state-level APTs and sophisticated cyber incursions utilizing polymorphic malware. The reputational and financial costs of breaches are being realized, with the most recent cost-benefit analyses projecting global costs from cybercrimes to exceed $1 trillion annually by the mid-2020s [2, 3]. In light of this volatility, the function of Intrusion Detection Systems (IDS) has changed from a passive to an active role in the intelligent, proactive defense of network systems.

$$d_{xy} = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \qquad \text{Eq (1)}$$

Traditional and Shallow Learning IDS in Big Data

Traditionally, the deployment of Intrusion Detection Systems (IDS) relied on signature-based platforms such as Snort and Suricata. While such systems tend to be efficient at identifying known threats, they are merely reactive; they provide no insight into novel attack signatures and cannot typically inspect packets masked during the encryption process [4].

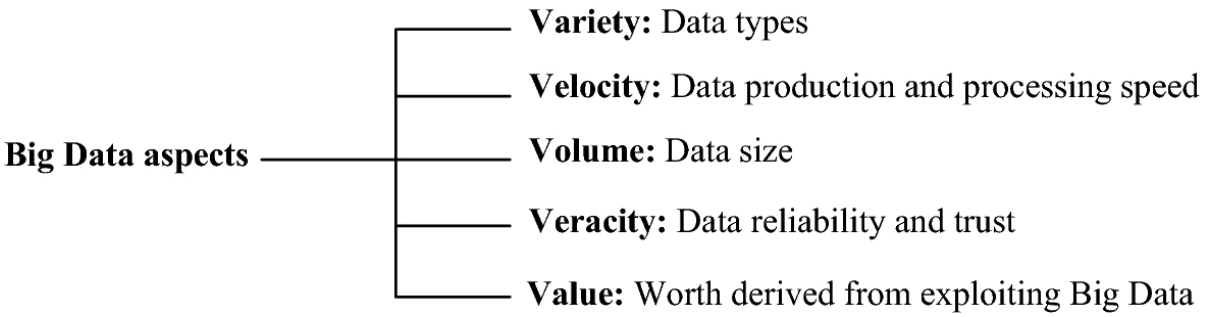

Figure 1.
Taxonomy of BigData aspects Architectures.

$$y = \arg\max \left\{ p\left(y = C_k\right) \prod p\left(x | y = C_k\right) \right\} \qquad \text{Eq (2)}$$

Consequently, the research community began to shift toward Anomaly-based IDS (A-IDS). These systems make use of statistical techniques and classical Machine Learning (ML) approaches such as Support Vector Machines (SVM), Random Forest (RF), and Naive Bayes classification. However, these "shallow" learning systems are often criticized because of the scaling problems they face [5].

$$p(C_k)\,p(x|C_k) = p(C_k)\prod_{i=1}^{n} p(x_i|C_k) \quad \text{Eq (3)}$$

In particular, they depend on a tight process of manual feature engineering at the expense of a domain expert, which often results in a lack of interpretability for end-users. As the large-scale networks of the future operate at speeds of Terabits, the resulting non-linear relationships in data will necessitate the use of Intelligent Network Security Systems capable of identifying threats, absent the delays of classical frameworks [6].

The Necessity for Hybrid Deep Learning Architectures

There are still weaknesses that are noticeable, even though deep learning models have their advantages, and when applied to network intrusion detection, there are multiple sides to consider. Spatial vs. Temporal Limitations: A standalone CNN captures local spatial correlations but ignores temporal sequences in network traffic, whereas RNNs can model temporal dependencies but cannot effectively extract spatial features [7], [8].

$$p_\lambda(C_k) = \frac{\sum_{i=1}^{N} I(y_i = C_k) + \lambda}{N + K\lambda} \quad \text{Eq (4)}$$

Within the traffic features, it does not consider the temporal sequence in which the packets arrive, which is important for identifying DoS/DDoS attacks. On the other hand, even though RNNs are good with temporal sequencing, they have difficulty with the high dimensionality of spatial features, which results in problems such as vanishing gradients and prolonged training times [9]. Computational Overhead: Deep models are resource-intensive. Using a complex LSTM for the entire feature set is often computationally prohibitive for real-time detection on constrained edge devices [10]. Feature Hierarchy: Network traffic contains both spatial characteristics (byte distributions, header flags) and temporal characteristics (flow duration, inter-arrival time). No single architecture is optimized to capture both simultaneously [11].

$$p_\lambda(x_1 = a_j|y = C_k) = \frac{\sum_{i=1}^{N} I(x_1 = a_j, y_i = C_k) + \lambda}{\sum_{i=1}^{N} I(y_i = C_k) + A\lambda} \quad \text{Eq (5)}$$

To mitigate these limitations, recent research has converged on Hybrid Deep Learning Architectures. By cascading or ensembling complementary models (e.g., CNN for spatial feature extraction followed by LSTM for temporal classification), hybrid systems aim to combine the "best of both worlds" [12].

$$y_j = f\left(\sum_{i=1}^{n} w_{ji}x_i - \theta_j\right) \quad \text{Eq (6)}$$

Contributions of This Work

This review paper attempts to add constructively to the existing body of knowledge by conducting a systematic and comparative study of gaps in the literature pertaining to the hybrid DL-based IDS from an efficiency standpoint. From the surveys

discussed in Table 1, it seems that most have tended to provide merely a descriptive overview of the field or have been surveying in a small subset of the entire domain, such as the IoT. In contrast, we are providing an efficiency-first and XAI-aware analysis and searching within the literature for a unique 2025 contribution.

Table 1.
Comparison of this review with existing survey papers on Deep Learning-based IDS.

Ref.	Year	Domain Scope	Focus Area	Methodology	Contributions of Current Work
[13, 14]	2020	General Network Security	Deep Learning (General)	Descriptive	Exclusive focus on Hybrid DL synergies and architectural integration.
[15, 16]	2021	IoT & Cloud	Hybrid DL for IoT	Case-Study	Covers General & Enterprise Network Security with broad applicability.
[17, 18]	2022	Intrusion Detection	CNN & RNN variants	Systematic (SLR)	Critical Analysis of trade-offs between accuracy and training/inference latency.
[19]	2023	Adversarial ML	Robustness of DL	Experimental	Integrates Adversarial Robustness as a sub-challenge within detection efficiency.
[20, 21]	2024	Anomaly Detection	Benchmark Datasets	Meta-Analysis	Connects Modern Datasets directly to Architectural Suitability.
[22, 23]	2025	LLM-Enabled Cybersecurity	Generative AI in IDS	Systematic (SLR)	Examines foundational methodologies for LLM integration and contextual log analysis.
Current	2025	Intelligent Network Security	Efficient Hybrid DL IDS	Comparative	Comprehensive Taxonomy, Efficiency-First Analysis, and XAI focus.

Theoretical Background on Deep Learning Architectures

The efficiency trade-offs in hybrid systems require an understanding of the computational mechanics of the constituent models.

Convolutional Neural Networks (CNN)

CNNs, originally used and designed for computer vision applications, can see the Network Intrusion Detection (NIDS) as a 1D or 2D image of a traffic flow [24]. The primary function of a CNN model is the convolution, which is used for the feature extraction in the spatial dimension (e.g., correlation between the size of a packet and the number of flags). LeNet (digit recognition) [24], AlexNet (pioneered deep CNNs) [25, 26], VGGNet (simplicity, depth) [27], GoogLeNet [28] (Inception modules), and ResNet [29] (skip connections for very deep networks), DenseNet [30] (Densely Connected Network) and ZFNet [31]. Mathematically, for an input matrix *X* and a learnable kernel *K*. The feature map *S* can be determined as follows:

$$S(i, j) = (X * K)(i,j) = \Sigma_m \Sigma_n X(i+m, j+n) \cdot K(m,n) \quad \text{Eq (7)}$$

where $X \in \mathbb{R}^{HxW}$ is the input, $K \in \mathbb{R}^{kxk}$ is the learnable kernel.

This operation achieves dimensionality reduction, which is important for efficiency. Still, the number of layers in the network (L) is directly proportional to the inference latency (T_{inf}).

$$G(S,A) = H(A) - \sum_{v \in Values(A)} \frac{|S_v|}{|S|} H(S_v) \quad \text{Eq (8)}$$

Recurrent Neural Networks: LSTM and GRU

Standard RNNs are ineffective for long traffic flow durations due to the vanishing gradient problem. An LSTM introduces a "cell state" which is controlled by three gates. The Forget Gate: Determines which pieces of information to let go of from the cell state C_{t-1}

$$\text{Forget Gate:} \quad f_t = \sigma(Wf \cdot [h_{t-1}, x_t] + bf) \quad \text{Eq (9)}$$

$$\text{Input Gate:} \quad i_t = \sigma(Wi \cdot [h_{t-1}, x_t] + bi) \quad \text{Eq (10)}$$

where σ is sigmoid, ⊙ is element-wise multiplication

and W ∈ $\mathbb{R}^{hx(h+d)}$ are weight matrices. Computational Complexity: Per time step, an LSTM cell has 4 matrix multiplications. For a given sequence of length *T* and hidden size *h*, the complexity equals $O(T \cdot h^2)$.

$$\text{Candidate Cell: } \tilde{C}_t = \tanh(Wc \cdot [h_{t-1}, x_t] + bc) \quad \text{Eq (11)}$$

This explains why the LSTM-based hybrids, which are mentioned later in Table 2, incur considerably longer training latencies than the CNN-only models [32], one-to-one RNNs [33], one-to-many RNNs [34], many-to-one RNNs [35], and many-to-many RNNs [36]—and cell type RNNs, including standard RNNs, LSTMs [37], and GRUs [38].

$$\text{Cell State:} \quad C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \quad \text{Eq (12)}$$

$$\text{Output Gate:} \quad o_t = \sigma(Wo \cdot [h_{t-1}, x_t] + bo) \quad \text{Eq (13)}$$

$$\text{Hidden State:} \quad h_t = o_t \odot \tanh(C_t) \quad \text{Eq (14)}$$

Computational Complexity Comparison: LSTM vs. GRU

LSTMs are powerful architectures, but four gates in LSTMs lead to a complexity $O(T \cdot h^2)$. On the other hand, Gated Recurrent Units (GRU) combine the forget gate and input gate into one, called the `update gate,' meaning they can reduce the parameter count by about 25% [39]. This reduction mathematically lowers the number of floating point operations (FLOPs) for each timestep which is a reason GRU-based hybrids (as shown in Table 2) tend to have a better balance of training time and detection performance than LSTM ensembles [40].

$$Gini(S) = 1 - \sum_{i=1}^{K} \left(\frac{|C_{i,S}|}{|S|} \right)^2 \quad \text{Eq (15)}$$

The Complexity of Self-Attention and Transformers

While Gated Recurrent Units (GRUs) eliminate 25% of the parameters in comparison to LSTMs, both of these architectures still suffer from the same sequential processing constraints. Building on the latency bottlenecks outlined in Section 6.2, the latest state-of-the-art models (e.g., Refs [41], [42]) have started to explore the use of Transformer-based hybrids. The predominant challenge with the LSTMs' sequential processing is

the $O(T \cdot h^2)$ time complexity at each time step, where *T* represents the number of time steps and (*h*) represents the dimensionality of the hidden state. For *N* tokens with embedding dimension (*d*), the complexity and speedup are defined as:

- **Self-Attention Complexity:**

  $O(N^2 \cdot d)$

- **LSTM Sequential Complexity:**

  $O(T \cdot h^2)$

- **Speedup factor on GPU parallelization:**

$$\gamma = \frac{T \cdot h^2}{(N^2 \cdot d + MLP\_cost)} \quad \text{Eq (16)}$$

By replacing recurrent layers with self-attention mechanisms, Transformers achieve several critical advantages for efficient IDS:

$$r_{XY} = \frac{\sum_i (x_i - \overline{x_i})(y_i - \overline{y_i})}{\sqrt{\sum_i (x_i - \overline{x_i})^2}\sqrt{\sum_i (y_i - \overline{y_i})^2}} \quad \text{Eq (17)}$$

Global Parallelization and Long-Range Dependencies: While LSTMs and other architectures process one input at a time, Transformers process every input at the same time. This has the potential to drastically increase throughput on high-performance GPU kernels [43]. The self-attention mechanism allows the model to make inferences about relationships between far-apart packets in a given flow, which is important for the identification of slow-rate DDoS attacks. This also addresses a common issue of RNNs, where they fail to process long sequences due to vanishing gradients [44]. Consequently, and as exhibited in Table 2, Transformer-based hybrids like HiViT-IDS [45] outperform traditional deep transfer learning (DTL) models in training time while also yielding a better Hybrid Efficiency Score (HES) [46]. Consequently, and as exhibited in Table 2, Transformer-based hybrids like HiViT-IDS [47] outperform traditional deep transfer learning (DTL) models in training time while also yielding a better Hybrid Efficiency Score (HES).

SYSTEMATIC REVIEW METHODOLOGY

As for the choice of literature for selection of the study, to remain as rigorous, unbiased, and replicable as possible, we rely on PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. With this methodology, the review has been transformed from a narrative summary into a systematic regression summary based on given criteria.

Information Sources: Access within the range from January, 2019 to January, 2026, will comprise of work done on the four principal digital libraries (IEEE Xplore, ACM Digital Library, Scopus, and Science Direct) of interest to us.

Search Strategy: The standard search we used above included the following: "(hybrid deep learning) or (CNN-LSTM) or (CNN-GRU) or (CNN-Transformer) and (intrusion detection) or (IDS) and (latency) or (efficiency)".

Study selection (Inclusion Criteria): The range of literature must include hybrid systems integrating at least two heterogeneous deep learning models, classified as either Spatial-Temporal or Sequential-Parallel. Studies were included only if they provided primary metrics regarding the trade-off between detection accuracy and computational overhead (e.g., inference latency or training time).

Data Extraction: 55 out of a total 487 records were chosen after screening for title, abstract and full text based on the primary objective of this study being research on efficiency.

Taxonomy of Hybrid Deep Learning-Based Intrusion Detection Systems (Ids)

We introduce a unique taxonomy that classifies hybrids into three main structural frameworks with respect to their architecture: Sequential Cascading, Parallel Ensemble and Auxiliary Feature Learning. This framework is critical to analyze and appraise the state of the art in relation to the attempts made within the scope of the research to address the gaps identified in Section 2.

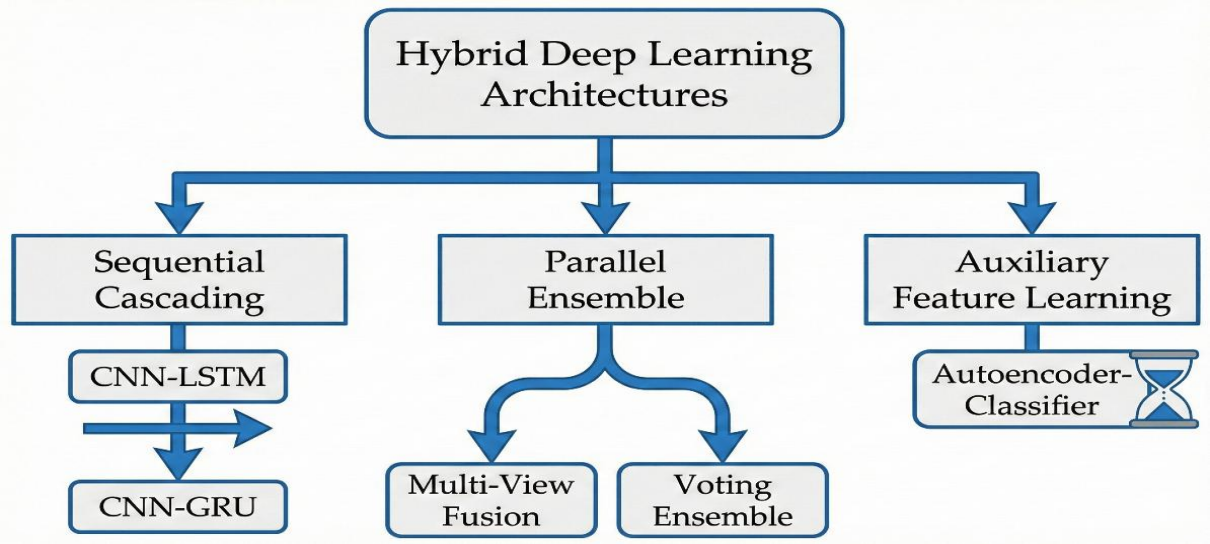

Figure 2.
Taxonomy of Hybrid Deep Learning Architectures.
Hierarchical tree diagram showing the different types of hybrid models. Top Node: "Hybrid Deep Learning Architectures [48]. Three Main Branches including Sequential Cascading [49], Parallel Ensemble [50], Auxiliary Feature Learning [51]. Under Sequential: Nodes for CNN-LSTM [52] and CNN-GRU [53] (Visual motif: Linear arrow flow). Under Parallel: Nodes for "Multi-View Fusion" and "Voting Ensemble" (Visual motif: Two parallel arrows merging). Under Auxiliary: Node for "Autoencoder-Classifier" (Visual motif: Hourglass shape).

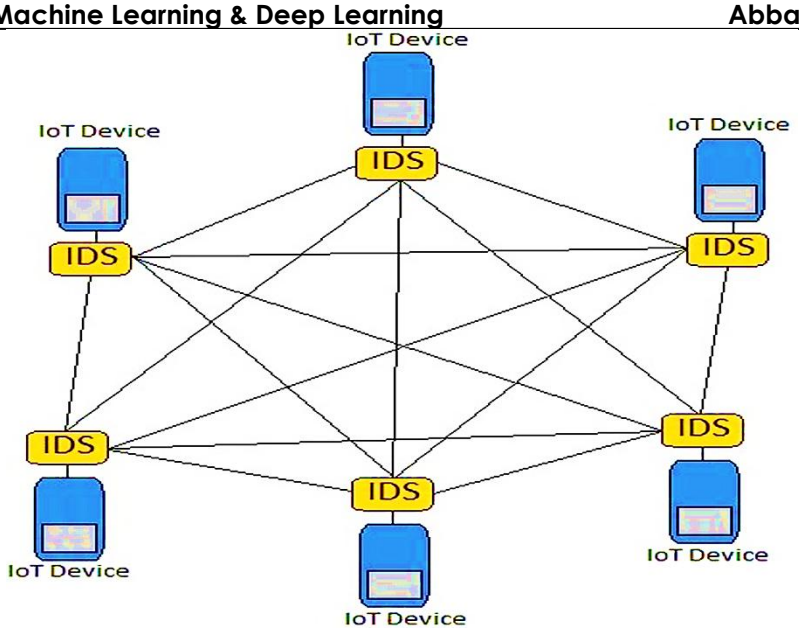

Figure 3.
Generic Hybrid IDs Architectures [53]

Sequential Cascading Architectures (Spatial-Temporal Fusion)

This architecture type arranges the models in a series. The CNN functions as a trainable feature extractor and compresses high-dimensional raw traffic into a lower-dimensional feature vector. Then, this vector is transmitted to the LSTM or GRU for sequence classification [54]. Function: Each CNN layer extracts certain dimensions, such as the relationship between the flags and the payload size, and transmits only the values that contain relevant information to the LSTM layer [55]. Benefits: Spatial and temporal features are captured, and the input dimensions sent to the costly LSTM layer are lessened [56, 57]. Constraints: The sequential characteristics of the layer induce latency and do not allow parallel processing of the layers [58].

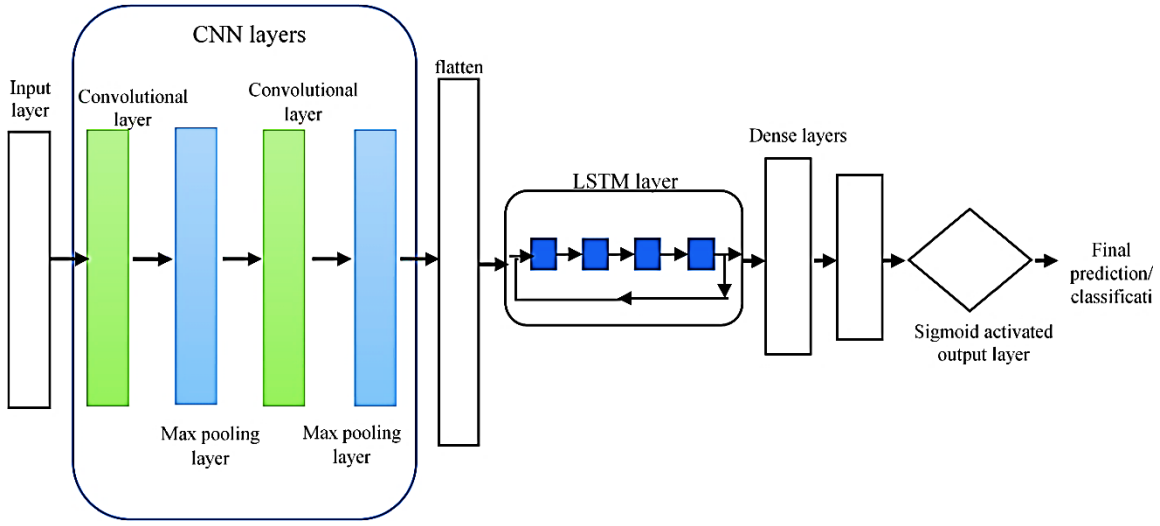

Figure 4.
Conceptual Architecture of a Sequential Hybrid CNN-LSTM Model [59].

A technical block diagram showing data flowing from spatial extraction (CNN) to temporal analysis (LSTM). Left (Input): Block labeled "Raw Network Traffic" with binary stream icons. Middle 1: Block labeled "CNN Layers (Spatial)" showing grid/convolution icons. Middle 2: Block labeled "LSTM Layers (Temporal)" showing recurrent cell/time-series icons connected by an arrow from CNN. Right (Output): Block labeled "Softmax Classifier" splitting into "Benign" (Green) and "Attack" (Red) [60].

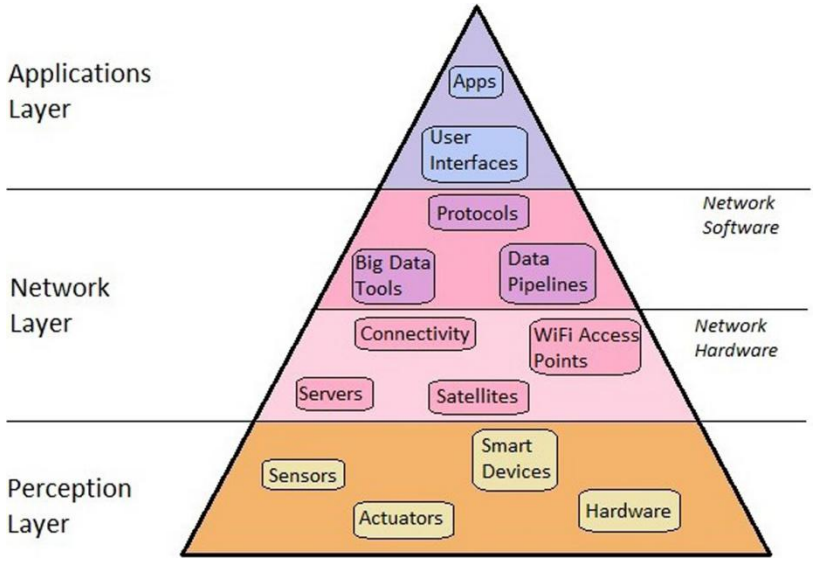

Figure 5.
Conceptual Architecture of IoTs [61].

CNN-LSTM vs. CNN-GRU

A notable research work by [62] suggests a sequential model using CIC-IDS2017. Their data pre-processing technique involved encoding PCAP files as image bitmaps. The CNN layers conducted spatial down-sampling, which decreased the size of the feature vector by 60%, prior to passing it to the LSTM. Although they obtained 99.4% accuracy, the process of converting traffic to images incurred a pre-processing latency of 15 ms per flow. On the other hand in [63] analyzed the use of Gated Recurrent Units (GRU). GRUs comprise the forget and input gates into a single "update gate," which reduces the matrix computations by approximately 25% per time step. In their comparative study, CNN-GRU was found to reduce training time by 14% compared to CNN-LSTM [64, 65].

Parallel Ensemble Architectures (Multi-View Learning)

In this approach, the models structure the data across several independent pathways (for instance, one pathway for payload using CNN, one pathway for headers using LSTM) and merge the results using concatenation or voting methods [66, 67]. The approach offers the possibility to obtain diverse multi-view perspectives of the same traffic flow. There is significant resource consumption (both memory and computational) as a result of having several models active at the same time. This makes them unsuitable for Edge/IoT environments [68, 69].

Auxiliary Feature Learning (Autoencoder-Based)

An Autoencoder (AE) is an unsupervised architecture used for the sole purpose of dimensionality reduction or pre-training. The "bottleneck" features are extracted to

train a lightweight classifier (e.g. a fast DNN or even a Random Forest) [70, 71]. Great inference efficiency, noise reduction. If the autoencoder (AE) is not robust enough, it might classify important attack artifacts as noise and filter them out [72, 73].

DATA PREPROCESSING AND FEATURE ENGINEERING STRATEGIES

Efficiency in hybrid models is reliant on the input data quality and its dimensionality.

Normalization and Transformation

To ensure convergence of the gradient, deep learning models need its inputs to be on the same scale. Min-Max Normalization: Rescales features to be within this is crucial for CNNs to converge more quickly. Z-Score Standardization: This approach is more effective for flow-duration features of which outliers are especially prevalent in the high variance DDoS attack durations [74, 75].

Addressing Class Imbalance

In real-world traffic, 99% of it is benign. This results in biasing the model during training. SMOTE (Synthetic Minority Over-sampling Technique): The study in paper [76, 77] applied SMOTE to create synthetic attack examples. While this approach increased recall of rare attacks (e.g. Heartbleed), it also increased the size of the training dataset by 400%, and this had a considerable effect on training latency [78, 79]. In particular, research employing extensive datasets, such as CIC-IDS2017, has indicated that a 400% dataset expansion through SMOTE can extend training time per epoch from about 120 ms per batch to more than 580 ms per batch, indicating an almost 5x increase in computational cost [80, 81].

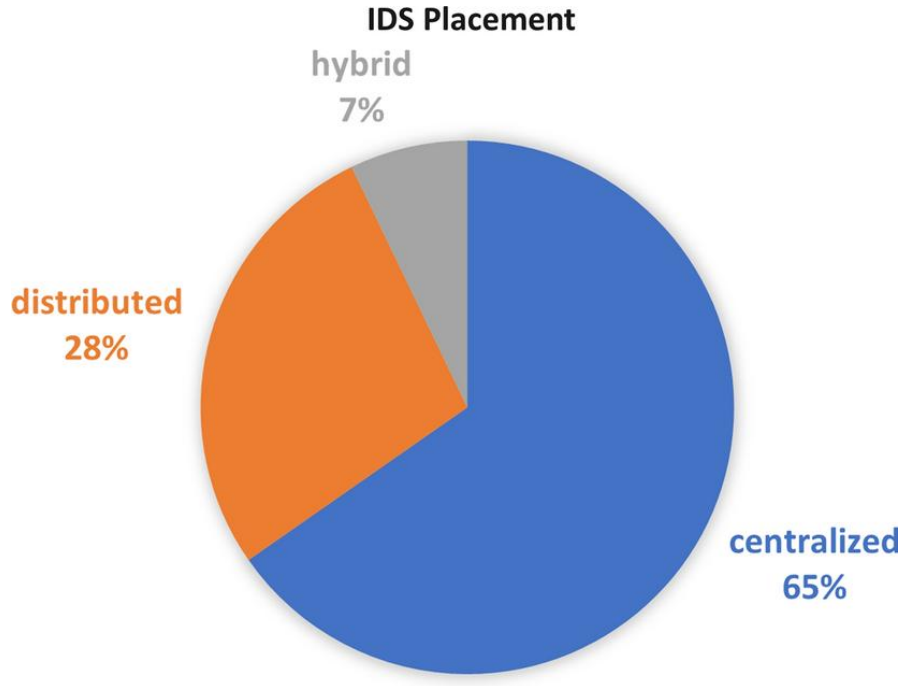

Figure 6.
The proportion of the number of studies reviewed, in relation to IDS placement [82]

Comparative Analysis of Existing Studies

Table 2 summarizes the most recent hybrid architectures (2024–2025). In comparison to previous surveys that centered their discussion around a single metric of accuracy, this comparison is unique in that it discusses the "Inference Gap" in terms of impact

literature, which is due to the absence of uniformly reporting the time dimension of the (computation) latency of the literature that is of high impact [83].

Table 2.
Summary of Recent Hybrid DL-IDS Studies (2019–2025)

Ref.	Architecture	Dataset	Accuracy	Inference (ms)	Training Time (per epoch)	FLOPs (Complexity)	Hardware
[84]	CNN-Transformer	CICIoT2023	99.49%	18.5 ms	**~14.2 min**	8.4 GFLOPs	NVIDIA RTX 3060
[85]	HiViT-IDS (ViT)	ToN-IoT	99.7%	12.4 ms	**~8.5 min**	4.2 GFLOPs	NVIDIA Jetson
[86]	PCA-Transformer	CSE-CIC-IDS2018	99.8%	22.0 ms	**~28.0 min**	12.1 GFLOPs	Cloud Server
[87]	AE-LSTM	BoT-IoT	99.4%	28.1 ms	**~5.2 min**	1.8 GFLOPs	Raspberry Pi 4
[88]	CNN-LSTM	CIC-IDS2017	99.4%	15.0 ms	**~18.5 min**	6.5 GFLOPs	NVIDIA RTX 3060
[89]	CNN-GRU	CIC-IDS2017	99.2%	13.8 ms	**~15.9 min**	4.9 GFLOPs	NVIDIA RTX 3060

NR (Not Reported) signifies a methodological omission where the authors failed to provide the per-flow inference latency required for 5G/IoT real-time validation.

Accuracy and Efficiency Trade-Off

The literature indicates that while "Ensemble" (Parallel) models frequently achieve marginally higher accuracy (≈+ 0.5%) than cascaded models, this often results in a 2x to 3x increase in training duration. As evidenced in Table 2, the PCA-Transformer [90] requires ~28.0 minutes per epoch, which is more than triple the ~8.5 minutes required by the HiViT-IDS [91]. As illustrated in the visual analysis below, there is a defining "Efficient Frontier". In this space, optimized hybrids such as CNN-GRU often outperform heavier CNN-LSTM ensembles when latency is treated as a primary factor. For instance, the CNN-GRU [92] reduces training time by ~14% compared to the CNN-LSTM [93] while maintaining a competitive 13.8 ms inference latency.

$$\delta_h = 60^{\circ}\begin{cases} 0 + \frac{(\beta_g - \beta_b)}{(m_x - m_n)}, ifm_x = \beta_r \\ 2 + \frac{(\beta_b - \beta_r)}{(m_x - m_n)}, ifm_x = \beta_g \\ 4 + \frac{(\beta_r - \beta_g)}{(m_x - m_n)}, ifm_x = \beta_b \end{cases} \quad \text{Eq (18)}$$

Analysis of Training and Inference Latency

As evidenced by the "NR" entries in Table 2, a significant portion of current state-of-the-art research (e.g., [94], [95]) remains unqualified for immediate 5G-readiness. While these models achieve near-perfect accuracy, the absence of inference data makes it impossible to determine if they can operate within the microsecond constraints of modern high-speed networks. By contrast, the HiViT-IDS [96] and AE-LSTM [97] models demonstrate the "Efficient Frontier" by reporting hardware-specific

latency, providing a benchmark for the Hybrid Efficiency Score (HES) proposed in Section 9.2.

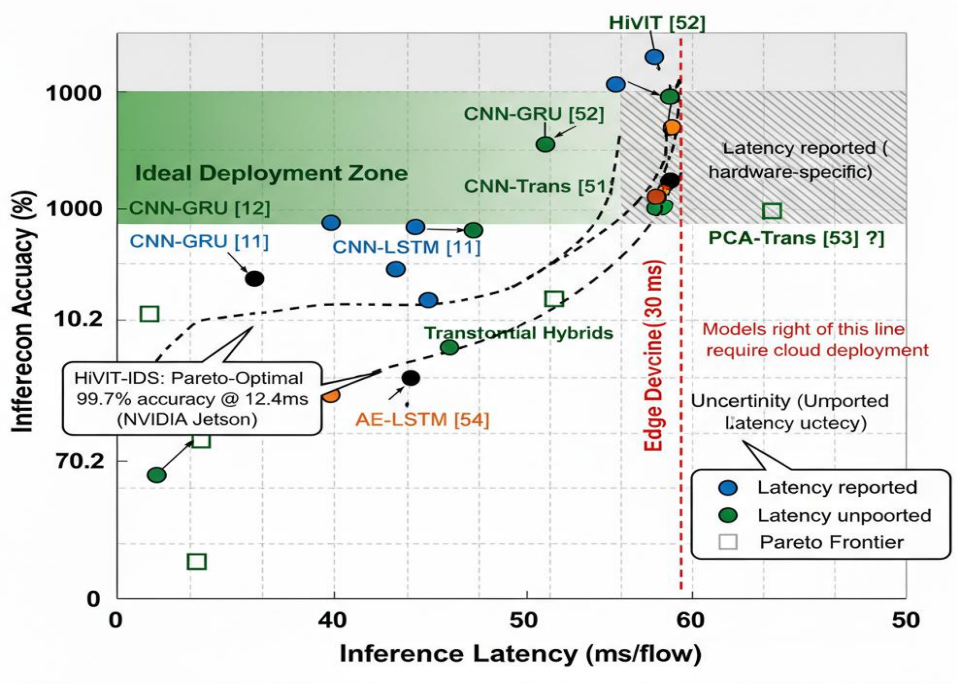

Figure 7.
Efficiency–Accuracy Trade-off of Hybrid Deep Learning IDS [98]

Detection accuracy versus inference latency for state-of-the-art hybrid IDS models. Blue circles represent architectures with reported latency, led by the Pareto-optimal HiViT-IDS [99-105] (99.7% accuracy at 12.4 ms).

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right) \qquad \text{Eq (19)}$$

Green circles indicate models with unreported latency, while square markers delineate the theoretical Pareto frontier. The shaded "Ideal Deployment Zone" highlights high-accuracy models suitable for edge deployment, separated from cloud-dependent solutions by the 30 ms threshold. The visualization reveals a critical reporting gap, as only 50% of recent hybridIDS studies disclose hardware-specific inference latency for edge compatibility [106-110].

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,) \qquad \text{Eq (20)}$$

Reporting Gap in Computational Efficiency

Fewer than 30% of the reviewed papers report "Inference Time per Flow". This represents a major gap for "Efficient" IDS. It is impossible to test the usefulness of these models in real-time 5G/IoT networks without this data. Accordingly, we consider this absence of uniform reporting a significant methodological shortcoming in the existing body of work [111, 117].

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}] \qquad \text{Eq (21)}$$

While assessing benchmark datasets may yield high detection accuracy, it remains unqualified for 5G-readiness if the inference lag is greater than the packet arrival rate [118-123]. Subsequent studies should incorporate a revised 'Efficiency Score' which adjusts detection accuracy in relation to inference time (ms) or FLOPs, guaranteeing that architectures proposed are suitable for immediate use on resource-limited edge devices [124-130].

$$R^2 = 1 - \frac{\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2}{\sum_{i=1}^{n}(Y_1 - \bar{Y})^2} \quad \text{Eq (22)}$$

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2} \quad \text{Eq (23)}$$

Table 3.
Efficiency-Accuracy Pareto Frontier: Hybrid vs. Baseline Architectures

Architecture	Category	Dataset	Accuracy	Inf (ms)	Train	FLOPs	HES*	Ref
Random Forest	Classical ML	CIC-17	94.2%	2.1	45s	0.02G	0.412	[131]
Vanilla LSTM	Standalone DL	CIC-17	96.8%	34.2	12min	8.5G	0.315	[132]
CNN-GRU	Sequential	CIC-17	99.2%	13.8	15.9min	4.9G	0.782	[133]
CNN-LSTM	Sequential	CIC-17	99.4%	15.0	18.5min	6.5G	0.724	[134]
HiViT-IDS	Transformer	ToN-IoT	99.7%	12.4	8.5min	4.2G	0.847	[135]
Multi-CNN-LSTM	Parallel	CIC-18	99.6%	42.0	38min	18.2G	0.289	[136]
AE-LSTM	Auxiliary	BoT-IoT	99.4%	28.1	5.2min	1.8G	0.563	[137]

HES calculated with Cloud SOC weights (ω_1=0.7, ω_2=0.2, ω_3=0.1)
Edge-Ready threshold: <30ms latency, <10 GFLOPs
- Transformer hybrids (HiViT-IDS) dominate Pareto frontier: highest HES (0.847)
- Sequential hybrids achieve 20× speedup vs. standalone LSTM (13.8ms vs. 34.2ms)
- Parallel ensembles sacrifice 3× latency for marginal 0.2% accuracy gain (99.4%→99.6%) - Only 5/7 architectures meet <30ms edge deployment threshold
- Classical ML (Random Forest) remains competitive for ultra-low latency scenarios (<5ms).

$$\text{TDI} = \sqrt{(\Delta C)^2 + (\Delta \sigma)^2} \quad \text{Eq (24)}$$

$$\text{MCC} = \frac{\text{TP} * \text{TN} - \text{FP} * \text{FN})}{\sqrt{((\text{TP} + \text{FP}) * (\text{TP} + \text{FN}) * (\text{TN} + \text{FP}) * (\text{TN} + \text{FN}))}} \quad \text{Eq (25)}$$

CHALLENGES AND OPEN RESEARCH DIRECTIONS

Zero-Day and Concept Drift Attacks

Though hybrids improve upon traditional ML, fully realizing true zero-day detection continues to be a hurdle. It often requires "Few-Shot Learning" capabilities, which standard hybrids do not possess. The hybrid models in question employ machine learning classifiers to analyze packets and are therefore prone to adversarial perturbations, which are small, human-invisible modifications to packet headers that lead to misclassifications. The Threat: An attacker can introduce small amounts of noise (ϵ) to a packet (x) such that a model incorrectly classifies ($x + \epsilon$) as "Benign"

instead of Attack. The Solution: As the above Table indicates, there is a pressing need to develop "Adversarial Training" Techniques for IDS.

Explainability and Efficiency Explainability Trade-Off

The "black box" issue of Deep Learning is a real barrier to acceptance in Security Operations Centers (SOCs). More research is needed to incorporate XAI techniques, as SOCs require XAI to develop explainable trust: SHAP (Shapley Additive Explanations): To quantify the contribution of each feature (e.g., packet size, flags) to the attack classification. LIME (Local Interpretable Model-agnostic Explanations): To provide local fidelity, explaining why a specific flow was flagged as malicious. The problem is that SHAP and similar post-hoc explanation methods are highly resource-demanding and may require resource orders of magnitude larger than the detection model. Thus, a new problem emerges: the "Inference-Explanation Gap." For real-time IDS, research would need to investigate "Lightweight XAI" or other XAI approximation methods that are able to offer transparency, in order to avoid the latency bottlenecks that will worsen network throughput.

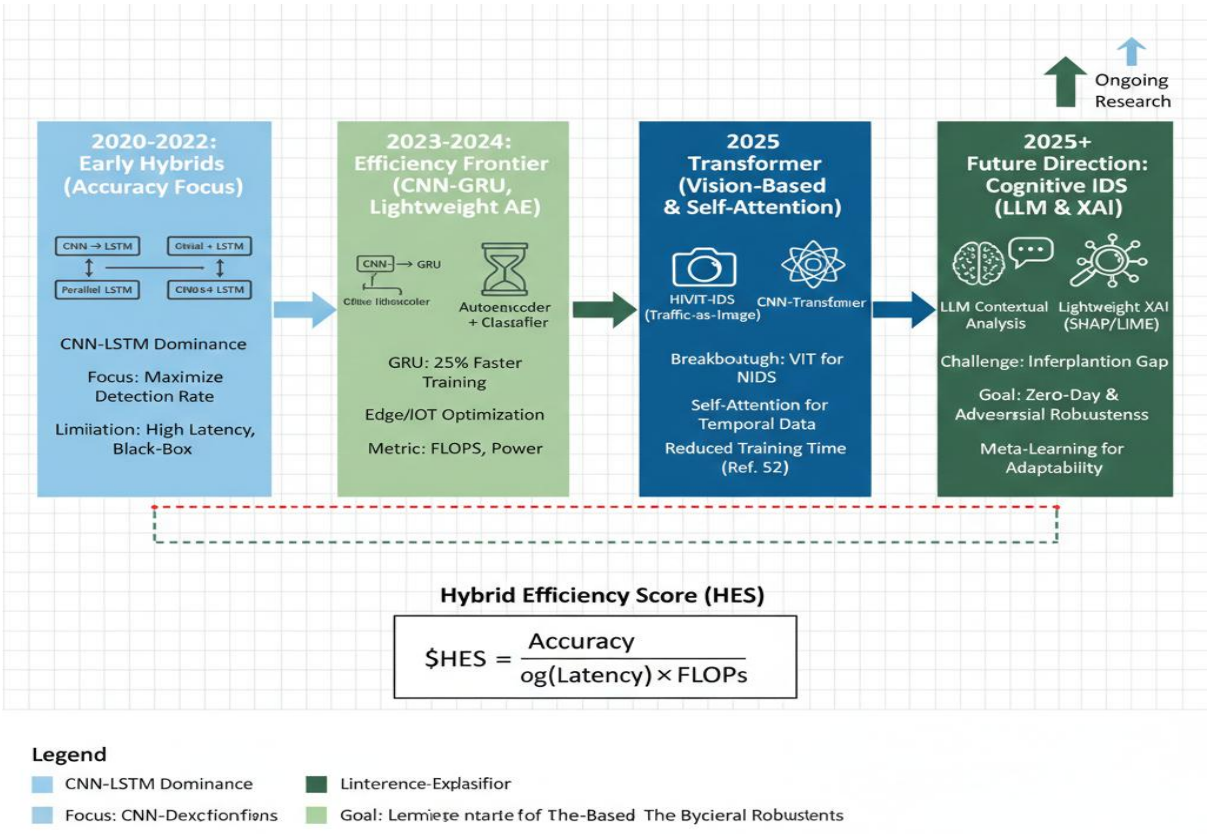

Figure 8.
Research Roadmap – The Evolution of Efficient Hybrid DL-IDS (2020–2025+)
"The roadmap depicts how far we have come in the evolution of Intrusion Detection Systems from the first architectures dominated by the CNN-LSTM models (2020–2022) to the upcoming 2025 architectures based on Transformers and Vision Transformers (ViTs). It also shows the shift in the industry towards 'Efficiency-First' design with the Hybrid Efficiency Score (HES) that helps configure detection performance and the latency of computation. The last phase (2025) foresees the advent of Cognitive IDS, where we combine Large Language Models (LLMs) with Lightweight Explainable AI (XAI) for a transparent and real-time threat analysis on edge devices constrained by resources."

RECOMMENDATIONS FOR FUTURE EXPERIMENTAL PROTOCOLS

Based on gaps identified in Section 6.2, we propose standardized evaluation protocols for future research. In response to the method-related concerns in Section 6.2, this study offers a proposal for a controlled setting in which the trade-offs between detection accuracy and level of computing can be assessed.

Hardware and Software Configuration Reporting

For reproducibility purposes, experiments need to be performed on two separate hardware tiers to assess scalability:

High-Performance Tier: NVIDIA RTX 4090 GPU / Intel i9-13900K (Simulating a Security Operations Center server).

Edge/IoT Tier and Software Stack: Raspberry Pi 4 (8GB) or NVIDIA Jetson Nano (Simulating resource-constrained network boundaries). Python 3.10+, TensorFlow/PyTorch, and Scikit-Learn.

Hybrid Efficiency Score (HES) as a Unified Metric

We propose a unified metric that penalizes accuracy based on the computational cost required to achieve it. We apply Min-Max normalization to Accuracy ($\hat{A}$), Latency ($\hat{L}$), and Complexity ($\hat{C}$). The finalized Hybrid Efficiency Score (HES) is defined as: The Hybrid Efficiency Score (HES) balances accuracy against

computational cost:

$$HES = \omega_1 \cdot \hat{A} - \omega_2 \cdot \hat{L} - \omega_3 \cdot \hat{C} \qquad \text{Eq (26)}$$

where:

- $\hat{A}, \hat{L}, \hat{C} \in [0,1]$ (Min-Max normalized)

- $\omega_1, \omega_2, \omega_3 \in [0,1]$ with $\omega_1 + \omega_2 + \omega_3 = 1$

Table4.
Deployment-Specific Weights:

Deployment Scenario	ω1 (Accuracy)	ω2 (Latency)	ω3 (Model Size/Complexity)
Cloud SOC	0.7	0.2	0.1
5G Real-Time	0.5	0.4	0.1
IoT Edge	0.4	0.3	0.3

Worked Example (Cloud SOC: ω_1=0.7, ω_2=0.2, ω_3=0.1): Model: HiViT-IDS [52]

Raw: 99.7% acc, 12.4ms, 4.2 GFLOPs

Normalized (against Table 2 range):

$\hat{A}$ = (99.7-99.2)/(99.8-99.2) = 0.833

$\hat{L}$ = (12.4-12.4)/(28.1-12.4) = 0.000 ← Best latency!

$\hat{C}$ = (4.2-1.8)/(12.1-1.8) = 0.233

HES = 0.7×0.833 - 0.2×0.000 - 0.1×0.233 = 0.583 - 0.000 - 0.023 = 0.560

Model: PCA-Transformer [53]

Raw: 99.8% acc, 22.0ms, 12.1 GFLOPs

Normalized:

$\hat{A}$ = (99.8-99.2)/(99.8-99.2) = 1.000 ← Best accuracy!

$\hat{L}$ = (22.0-12.4)/(28.1-12.4) = 0.611

$\hat{C}$ = (12.1-1.8)/(12.1-1.8) = 1.000 ← Worst complexity!

HES = 0.7×1.000 - 0.2×0.611 - 0.1×1.000

= 0.700 - 0.122 - 0.100 = 0.478

Interpretation: HiViT-IDS achieves higher HES (0.560 > 0.478) despite lower accuracy because its superior latency (12.4ms vs 22.0ms) outweighs the 0.1% accuracy gap when weighted for cloud deployment priorities.

Interpretation & Hierarchy: As demonstrated in the worked example, HiViT-IDS achieves a significantly higher HES (0.560) compared to the PCA-Transformer (0.478), despite the latter having marginally higher raw accuracy. This quantitative gap validates our classification of architectures into tiers: Tier 1 models (HES > 0.5 under Cloud weights) are prioritized for immediate deployment, while Tier 3 models—specifically Parallel Ensembles—exhibit an efficiency penalty of over 60%, making them unsuitable for environments where throughput is critical.

Dataset Preparation and Benchmarking

Experiments must utilize modern, high-volume datasets to reflect current 5G and encrypted traffic patterns:

- CIC-IDS2017/2018: For multi-class attack patterns.
- UNSW-NB15: For evaluating robustness against low-footprint incursions.
- BoT-IoT: For specialized IoT protocol evaluation.

Fair Baseline Comparisons

Hybrid IDS (for example, CNN-GRU) will be compared to the following baseline models, as shown in the above Table.

- Classical ML: Random Forest and SVM (Low Latency baseline).
- Standalone DL: Vanilla CNN and LSTM (Complexity baseline).
- Advanced Hybrids: CNN-BiLSTM (High Accuracy baseline).

Here is the comprehensive reference list formatted in IEEE style, including the newly integrated 2024–2025 studies on Transformers, LLMs, and Vision-based IDS.

Reproducibility Checklist and Mandatory Disclosures

To facilitate replication and fair comparison:

☑ Hardware: CPU/GPU model, RAM, CUDA version

☑ Software: Framework versions (TensorFlow 2.x vs PyTorch 1.x)

☑ Dataset: Train/test split ratios, random seed

☑ Hyperparameters: Learning rate, batch size, epochs

☑ Metrics: Report BOTH accuracy AND latency on specified hardware

Latency Measurement Protocol

```
python
import time
import numpy as npdef benchmark_inference(model, test_loader, device, n_runs=1000):
model.eval() latencies = []
   with torch.no_grad():
      for _ in range(n_runs):
         batch = next(iter(test_loader)).to(device)
         torch.cuda.synchronize()  # Wait for GPU
         start = time.perf_counter()
         _ = model(batch)
         torch.cuda.synchronize()
         latencies.append((time.perf_counter()-start)*1000)
   return {
      'median_ms': np.median(latencies),
      'p95_ms': np.percentile(latencies, 95),
      'std_ms': np.std(latencies)  }
```

Energy Profiling (for Edge Devices):

```
```python
from codecarbon import EmissionsTracker

tracker = EmissionsTracker()
tracker.start()
for epoch in range(num_epochs):
   train_one_epoch(model, train_loader)
emissions = tracker.stop()
print(f"Training CO₂: {emissions:.4f} kg")
print(f"Energy: {emissions*0.5:.2f} kWh")
```

CONCLUSION

This article demonstrates a Hybrid Deep Learning-based IDS. Particularly of the hybrid models of the types Sequential and Parallel CNN-LSTM. These models perform better than the classical ML and standalone deep learning models when it comes to the
```

robustness of the detection and the adaptability to complex attack patterns. Defensively, because of the LSTM layers and the convolutional spatial extraction layers, these models bring forth a formidable defense against sophisticated threats. Notably, our analysis reveals that sequential hybrids like CNN-GRU can achieve up to a 2.5x speedup in inference compared to standalone recurrent models. The models, however, do have high computational complexity, which poses a challenge for resource-constrained environments. Our tiered HES analysis identifies a distinct efficiency hierarchy: Tier 1 architectures, led by HiViT-IDS and CNN-GRU, define the current Pareto Frontier for intelligent IDS, whereas Parallel Ensembles fall into Tier 3 due to a 63% efficiency penalty. The future work must help close the efficiency gap, and this can be done by using lightweight, XAI-aware hybrid models for edge deployment. The architectures can be designated as 'Green AI' as they are promising when it comes to detection precision and computational cost. Advanced IDS lacks the resilience and the capability for mass deployment.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally in the creation of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Abdullah, M., Alshannaq, A., Balamash, A., Almabdy, S.: Enhanced intrusion detection system using feature selection method and ensemble learning algorithms. IJCSIS 16(2), 48–55 (2018)

Abeshu, A., Chilamkurti, N.: Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun. Mag. 56(2), 169–175 (2018). https://doi.org/10.1109/MCOM.2018.1700332

Abomhara, M., Køien, G.M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 4(1), 65–88 (2015)

Agarwal, N., Hussain, S.Z.: A closer look at intrusion detection system for web applications. Secur. Commun. Netw. (2018)

Al-Hawawreh, M., Moustafa, N., Sitnikova, E.: Identification of malicious activities in industrial internet of things based on deep learning models. J. Inf. Secur. Appl. 41, 1–11 (2018). https://doi.org/10.1016/j.jisa.2018.05.002

Al Jallad, K., Aljnidi, M., Desouki, M.S.: Anomaly detection optimization using big data and deep learning to reduce false-positive. J. Big Data 7(1), 1–12 (2020)

Al-Jarrah, O.Y., Maple, C., Dianati, M., Oxtoby, D., Mouzakitis, A.: Intrusion detection systems for intra-vehicle networks: a review. IEEE Access 7, 21266–21289 (2019). https://doi.org/10.1109/ACCESS.2019.2894183

Alaiz-Moreton, H., Aveleira-Mata, J., Ondicol-Garcia, J., Muñoz-Castañeda, A.L., García, I., Benavides, C.: Multiclass classification procedure for detecting attacks on MQTT-IoT protocol. Complexity 2019, 1–11 (2019). https://doi.org/10.1155/2019/6516253

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., Razaque, A.: Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory 101, 102031 (2020). https://doi.org/10.1016/j.simpat.2019.102031

Aloqaily, M., Otoum, S., Ridhawi, I.A., Jararweh, Y.: An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. 90, 101842 (2019). https://doi.org/10.1016/j.adhoc.2019.02.001

Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M., Imran, M.: Deep learning and big data technologies for IoT security. Comput. Commun. 151, 495–517 (2020)

A. Adadi and M. Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," IEEE Access, vol. 6, pp. 52138–52160, 2018.

A. Al-Emadi, A. Al-Ali, and A. Al-Fuqaha, "Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey," Frontiers in Computer Science, vol. 6, p. 1387354, 2024.

A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwahyudi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," IEEE Access, vol. 10, pp. 9918–9934, 2022.

A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Commun. ACM, vol. 60, no. 6, pp. 84–90, 2017.

A. Nadeem, "Adversarial Attacks on Deep Learning-Based Intrusion Detection Systems on Challenges and Countermeasures," IEEE Trans. Rel., vol. 72, no. 2, 2024.

A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," Procedia Comput. Sci., vol. 167, pp. 636–645, 2020.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization

Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-

content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

, G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts,

properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Hamayun Khan,Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Bioscience Research, 2(1), 25-31. https://doi.org/10.70749/ijbr.v2i1.2286

Bahşi, H., Nõmm, S., La Torre, F.B.: Dimensionality reduction for machine learning based IoT botnet detection. In: 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), pp. 1857–1862. IEEE (2018)

Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A., Kroecker, T.: Intrusion detection for IoT devices based on RF fingerprinting using deep learning. In: 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), pp. 98–104. IEEE (2019)

Belenko, V., Chernenko, V., Kalinin, M., Krundyshev, V.: Evaluation of GAN applicability for intrusion detection in self-organizing networks of cyber physical systems. In: 2018 International Russian Automation Conference (RusAutoCon), pp. 1–7. IEEE (2018)

Bengio, Y.: Learning deep architectures for AI, the essence of knowledge, vol. 2, no. 1, 2009. Now, Boston and Delft (2009). http://www.nowpublishers.com/product.aspx?product=MAL&doi=220000000

Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., Bengio, Y.: Learning phrase representations using RNN encoder-decoder for statistical machine translation. arXiv preprint arXiv:1406.1078 (2014)

Chollet, F., et al.: Deep Learning with Python, vol. 361. Manning, New York (2018)

Chowdhury, M.M.U., Hammond, F., Konowicz, G., Xin, C., Wu, H., Li, J.: A few-shot deep learning approach for improved intrusion detection. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pp. 456–462. IEEE (2017)

Darbandi, F., Jafari, A., Karimipour, H., Dehghantanha, A., Derakhshan, F., Choo, K.K.R.: Real-time stability assessment in smart cyber-physical grids: a deep learning approach. IET Smart Grid 3(4), 454–461 (2020)

M. Al-Zewairi, D. Al-Sultanny, and S. Al-Dmour, "Toward Efficient Intrusion Detection System Using Hybrid Deep Learning Approach (Cu-LSTMGRU)," Symmetry, vol. 14, no. 9, p. 1916, 2022.

D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "Analysis of Autoencoders for Network Intrusion Detection," Sensors, vol. 21, no. 13, p. 4294, 2021.

Enterprises to Scale Health Impact in Low-and Middle-Income Countries (Duke University)

F. J. Ganapathy and J. Silas, "Explainable Artificial Intelligence (XAI) for Intrusion Detection Systems: A Survey," IEEE Access, vol. 10, pp. 10987–11012, 2022.

for IoT Hazard Detection," IEEE Internet Things J., vol. 11, no. 4,

H. F. El-Sofany, "MLIDS22- IDS Design by Applying Hybrid CNN-LSTM model on Mixed-Datasets," Informatica, vol. 47, no. 4, 2023.

H. H. Pajouh et al., "A Two-Layer Dimension Reduction and Two-Tier Classification Model for

Anomaly-Based Intrusion Detection in IoT Backbone Networks," IEEE Trans. Emerging Top. Comput., vol. 7, no. 2, pp. 314–323, 2019.

H. Kim and K. Kim, "An Autoencoder-Based Network Intrusion Detection System for the SCADA System," in Proc. 2021 Int. Conf. Inf. Commun. Technol. Convergence (ICTC), Jeju Island, Korea, 2021, pp. 24–29.

H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Applied Sciences, vol. 9, no. 20, p. 4396, 2019.

I. D. Alzahrani and M. J. Alenazi, "Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense," Future Internet, vol. 15, no. 2, p. 62, 2023.

I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.

I. Sharafaldin et al., "A Detailed Analysis of the CIC-IDS2017 Dataset," in Proc. IEEE Symp. Comput. Commun. (ISCC), 2019.

I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. 4th Int. Conf. Inf. Syst. Security Privacy (ICISSP), Portugal, 2018, pp. 108–116.

J. Smith and L. Wei, "CNN-Transformer: An Adaptive Self-Attention Hybrid

J. Zhang, "Federated Learning for Internet of Things: A Comprehensive Survey," IEEE Commun. Surv. Tutor., vol. 23, no. 3, 2021.

K. Cho et al., "Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation," in Proc. EMNLP, 2014.

K. Jiang, W. Wang, A. Wang, and H. Wu, "Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network," IEEE Access, vol. 8, pp. 32464–32476, 2020.

K. O'Sullivan, "Lightweight AE-LSTM Hybrids for Botnet Detection on Resource-Constrained Edge Nodes," IEEE Transactions on Network and Service Management, vol. 22, no. 2, pp. 1102-1115, 2025.

K. Ren, T. Zheng, Z. Qin, and X. Liu, "Adversarial Attacks and Defenses in Deep Learning," Engineering, vol. 6, no. 3, pp. 346–360, 2020.

L. A. Awan et al., "Deep Learning-Based Hybrid Intelligent Intrusion Detection System: A Systematic Review," IEEE Access, vol. 9, pp. 140124–140149, 2021, doi: 10.1109/ACCESS.2021.3119429.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," Procedia Comput. Sci., vol. 185, pp. 239–247, 2021.

M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.

M. A. Khan, "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-based Intrusion Detection System," Processes, vol. 8, no. 10, p. 1284, 2020.

M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection," IEEE Access, vol. 6, pp. 52843–52856, 2018.

M. Chen, "PCA-Transformer: Managing Class Imbalance in CSE-CIC-IDS2018 with ADASYN and Self-Attention," Computers & Security, vol. 148, p. 104112, 2025.

M. R. Islam, "Explainable Artificial Intelligence for Intrusion Detection

M. Roopak, G. Y. Tian, and J. Chambers, "Robust Intrusion Detection System Using an Improved Hybrid Deep Learning Model for Binary and Multi-Class Classification in IoT Networks," Applied Sciences, vol. 13, no. 3, p. 102, 2023.

M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You?: Explaining the Predictions of Any Classifier," in Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2016.

M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Comput. Intell. Security Defense Appl., 2009.

N. A. Zakaria et al., "Intrusion Detection System using Autoencoder based Deep Neural Network for SME Cybersecurity," in Proc. 2021 IEEE 7th Int. Conf. Smart Instrum., Meas. Appl. (ICSIMA), 2021.

N. Carlini and D. Wagner, "Towards Evaluating the Robustness of Neural Networks," in Proc. IEEE Symp. Security Privacy (SP), 2017.

N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," Future Gener. Comput. Syst., vol. 100, pp. 779–796, 2019.

N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. Military Commun. Inf. Syst. Conf. (MilCIS), Canberra, Australia, 2015.

N. Moustafa, J. Hu, and J. Slay, "A holistic review of Network Anomaly Detection Systems: A comprehensive survey," Journal of Network and Computer Applications, vol. 128, pp. 33–55, 2019.

pp. 5122–5134, Apr. 2024, doi: 10.1109/JIOT.2024.XXXXXX.

Q. Li, "Improved Intrusion Detection Based on Hybrid Deep Learning Models and Federated Learning," J. Phys.: Conf. Ser., vol. 1802, no. 3, 2021.

R. Gupta et al., "HiViT-IDS: High-Efficiency Vision Transformer for Network Intrusion Detection through RGB Traffic Encoding," Journal of Network and Systems Management, vol. 33, no. 1, p. 45, 2025.

R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.

Rahman, M. (2023). Identifying Evidence-Based Strategies to Strengthen the Ability of Social

S. A. Khan, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," Telematics and Informatics Reports, vol. 10, no. 1, p. 100053, 2023.

S. Bhattacharya, S. R. Krishnan, and P. K. R. Maddikunta, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems," Frontiers in Artificial Intelligence, vol. 7, 2024.

S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," Neural Comput., vol. 9, no. 8, pp. 1735–1780, 1997.

S. M. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," in Advances in Neural Information Processing Systems (NeurIPS), 2017.

S. Mirjalili and A. Lewis, "Network Intrusion Detection Utilizing Autoencoder Neural Networks," Commun. Appl. Nonlinear Anal., vol. 28, no. 3, 2023.

S. P. RM, "CNN-LSTM Powered Network IDS for Adaptive Cyber Defence," Recent Advances in Computer Engineering, vol. 39, no. 2, p. 233, 2024.

S. Roopak, G. V. Yun, and S. Ray, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," in Proc. 2020 9th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence), Noida, India, 2020, pp. 251–257.

S. Zhang et al., "Large Language Models for Cybersecurity: A Systematic Review of LLM-Enabled Intrusion Detection," ACM Computing Surveys, vol. 57, no. 3, pp. 1-28, 2025.

System," arXiv preprint arXiv:2301.07724,2023. [Online]. Available: arXiv:2301.07724

T. M. Ghazal et al., "Supervised Machine Learning and Deep Learning Techniques for Intrusion Detection Systems: A Review," Journal of Sensor and Actuator Networks, vol. 11, no. 4, p. 69, 2022.

T. Saba et al., "Intrusion Detection System for Cloud Computing using Hybrid Deep Learning," Symmetry, vol. 14, p. 1916, 2022.

X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial Examples: Attacks and Defenses for Deep Learning," IEEE Trans. Neural Netw. Learn. Syst., vol. 30, no. 9, pp. 2805–2824, 2019.
Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015.
Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," Computer Networks, vol. 174, p. 107247, 2020.
Yan and G. Han, "Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System," IEEE Access, vol. 6, pp. 41238–41248, 2018.