Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

# An Optimal Hybrid Deep Learning Based Intrusion Detection System (IDS) Using Intelligent Network Security

**Ghulam Abbas (Corresponding Author)**
Faculty of Computer Science & IT Superior University, Lahore, 54000, Pakistan
Email: cybereengineer@gmail.com
**Shahid Rafique**
AITEEC- AI Technology Exchange and Engineering Consultancy, Lahore, Punjab,
Email: shahidrafique0027@gmail.com
**Nasir Ayub**
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com
**Chaudary Umair Mehmood**
Edge Hill University, Ormskirk L39 4QP, United Kingdom
Email: umairmehmood.pk@gmail.com
**Hamayun Khan**
Department of Computer Science, Faculty of Computer Science & IT, Superior University, Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk
**Syed Muhammad Rizwan**
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan
Email: rizwan.naqvi@ieee.org
**Muhammad Waleed Khawar**
Innova Network, 184 C, Airline Society, Lahore, 54000, Pakistan
Email: waleedkhawar19@gmail.com
**Osama Imran**
School of Electrical Engineering and Computer Sciences, NUST, Islamabad, National University of Science and Technology (NUST) Email: oimran.mscs25seecs@seecs.edu.pk

## ABSTRACT

The amount of interdependent digital infrastructure has swamped us and enabled the rise of an unprecedented no of complex cyber-attacks, making perimeter-based security measures more and more obsolete. Traditional network intrusion detection systems (NIDS) face the challenge of catastrophic attack classes, which have abysmal detection rates, and also have issues of class imbalance, inadequate temporal-spatial feature extraction, and mismatch between the probability output. Researchers continue to struggle with traditional network intrusion detection systems (NIDS), which suffer from catastrophic attack classes with abysmal detection rates and issues of class imbalance, inadequate temporal-spatial feature extraction, and mismatched probability outputs. To fill the inadequacies, the optimal hybrid deep learning framework for intelligent network security is introduced, named Threat-Aware Selective Calibration Hybrid Deep Learning-based Intrusion Detection System (TASC-HDLIDS). The proposed

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

model combines a 1D CNN for spatial feature extraction, Bi-LSTM for temporal sequence modeling, with different heads of attention for focusing on varying contexts. A multi-task learning approach is introduced to tackle the class imbalance, which is formulated with dual focal losses, one for attack classification and another for identification of the rare threats. A novel post-hoc threat-aware selective calibration mechanism is presented to optimize a column vector of attack probabilities according to severity for the validation set. The model is tested on the benchmark NSL-KDD dataset with an accuracy of 96.93%, a weighted F1 of 97.00% and a macro F1 of 72.22%. Notably, the rate of recall for the U2R product of 36.00% is much better than the present one. With 307,846 parameters, an inference time of 2-3ms per sample, and a low-weight design, it can be deployed in the real world. The key innovations of this research are the novel architectural integration, multi-task learning framework involving dual focal losses, the threat-aware selective calibration mechanism, the thorough benchmarking process followed by statistical validation, and lastly, interpretability through SHAP analysis. The TASC-HDLIDS framework proves that an intelligent calibration and multi-task learning approach can considerably improve the detection of serious threats in an imbalanced network environment and sets a new state-of-the-art benchmark on NSL-KDD.

**Keywords:** Intrusion Detection System, Deep Learning, Network Security, NSL-KDD, Convolutional Neural Network, Bidirectional LSTM, Multi-Head Attention, Focal Loss, Multi-Task Learning, Class Imbalance, Threat Calibration

## INTRODUCTION

Modern network environments have become increasingly complex, heterogeneous, and data-intensive, creating substantial challenges for cybersecurity and continuous threat monitoring. The rapid growth in network traffic volume, diversity of communication patterns, and complexity of attack behaviours has increased the difficulty of distinguishing legitimate activities from malicious network events. Recent research highlights the need for network intrusion detection systems capable of analysing high-dimensional network telemetry while maintaining effective detection performance and low computational overhead [1].

$$\mathrm{Yi} = \frac{\mathrm{Xi}-\mu\beta}{\sqrt{2\sigma^2\beta+\varepsilon}} \qquad \text{Eq (1)}$$

The threat landscape has also significantly changed, with attacks becoming more and more sophisticated, adaptive, and undetectable by traditional security methods. A multi-stage intrusion approach, polymorphic behaviour and attack patterns that are not previously defined but may resemble predefined attack patterns can all be used by attackers. Network Intrusion Detection Systems (NIDS) have therefore emerged as a crucial element in present-day cyber security infrastructure, especially in Security Operations Centres (SOCs) where real-time monitoring and quick detection of potentially suspicious network activities are paramount. Recent research highlights the need to adopt intelligent detection schemes that are capable of processing massive volumes of network data flows with low false-positive and high detection rates for various classes of attacks [2].

$$\sigma\beta = \frac{1}{M}(\mathrm{Xi} - \mu\beta)^2 \qquad \text{Eq (2)}$$

In traditional IDS systems, the major limitation of intrusion detection is the lack of adaptability to today's network environments, such as the signature-based systems and the traditional anomaly detection methods. Signature-based techniques are very effective at catching known attacks but have the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

downfall of being less flexible toward new or modified attacks. Likewise, classical anomaly detection methods can produce many false alarms if "normal" network activity changes with time. Decision Trees, Support Vector Machines and Random Forests are examples of machine learning techniques that have been used to boost the automated detection of intrusion in modern networks, but many traditional methods continue to rely on manually crafted features and are hard to model intricate nonlinear relationships in network traffic. More recent work also shows that distribution changes, concept drift, and strong class imbalance can severely impact the performance and reliability of traditional intrusion detection models [3].

$$\mu\beta = \frac{1}{M} + \sum_{t=1}^{M} \mathrm{Xi} \qquad \text{Eq (3)}$$

As a way to deal with the architecture-constrained shallow DL models, the cybersecurity industry has latched onto deep DL (Deep Learning) methodologies. Using deep architectures, a hierarchical representation of features can be extracted directly from the raw or minimally preprocessed network data, while avoiding manual bias in applying heuristic feature selection. In huge traffic sets, deep neural networks (DNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs) have been found to have greater potential to model complex, non-linear relationships.

$$S = w2 \times h2 \times d2 \qquad \text{Eq (4)}$$

However, each deep learning paradigm has its own set of trade-offs: For spatial feature extractors such as CNNs, sequential dependencies between the temporal neighbors of packets in consecutive packet bursts can easily be lost, while for temporal models like Long Short-Term Memory (LSTM), such networks incur a significant amount of computational latency to capture the spatial correlation across large sets of features. Some early 2025 research indicates that monomodel deep learning approaches do not have the power to represent both small resource lateral movements and large volume volumetric attacks [4].

$$w2 = \frac{(\mathrm{w1} - \mathrm{f})}{A+1} \qquad \text{Eq (5)}$$

These constraints require a paradigm shift towards systematic hybrid deep learning topologies, combining complementary neural topologies. Hybrid models combine spatial feature extraction, temporal sequence modeling and multi-head self-attention with adaptive calibration to capture complex representations of network telemetry.

$$\mathrm{h2} = \frac{(\mathrm{h1} - \mathrm{f})}{A+1} \qquad \text{Eq (6)}$$

In this study, we focus on this fundamental need by developing a Threat-Aware Selective Calibration Hybrid Deep Learning Intrusion Detection System (TASC-HDLIDS). It proposes Convolutional Neural Networks for extracting local spatial information, Bidirectional Long Short-Term Memory (BiLSTM) for modeling temporal information, Multi-Head Self-Attention to weight long-range feature dependencies, and Global Pooling to reduce dimensionality without discarding the spatiotemporal context.

$$d2 = d1 \qquad \text{Eq (7)}$$

TASC-HDLIDS also leverages two focal loss functions and a threat-aware selective confidence calibration to tackle commonly encountered issues of rare attack category bias and model overconfidence in rare attack categories resulting from extreme class imbalance.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$G_B = \sum_{i=1}^{N} W_i . G_{L_i}$$

Eq (8)

### 1.1 Network Intrusion Detection Systems

Network Intrusion Detection Systems (NIDS) are important monitoring systems placed at key points in a network topology to examine incoming and outgoing traffic in terms of the packet payload, header configurations and the speed, frequency, and timing of packet transmission. Hanley noted that Host-based Intrusion Detection Systems (HIDS) look inside localized host operating systems and track what is changing on those files and what processes are running there; NIDS will analyze the total capacity or network fabric to determine if there are any malicious activities, policy violations or unauthorized login attempts issued at any distributed endpoint.

$$S_i^{(b,t)} = \sum_{z=1}^{E} p_{iz}^{(b)} J_z^{(b-1,t)} + \sum_{i'}^{y} x_{ii'}^{(b)} J_{i'}^{(b,t-1)}$$

Eq (9)

$$J_i^{(b,t)} = \beta^{(b)}(S_i^{(b,t)})$$

Eq (10)

Often, they use Hybrid IDS architectures that combine hostbased and network-edge logs to create a holistic security posture over multi-tenant cloud platforms, industrial control systems, and clusters of edge nodes. In a recent comparative analysis conducted towards the end of 2024, one can find that whereas the HIDS provides a high level of granular visibility into the internal system state transitions, the NIDS is still the foremost defense layer to be able to detect proper lateral movement and probing of the perimeter before internal systems are compromised [5].

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + b_o)$$

Eq (11)

The four primary functional phases to the design of a modern NIDS pipeline are data acquisition, feature pre-processing, detection inference, and alerting/response mitigation. While gathering data, network packets are transferred through the port mirror or TAP devices. The preprocessing pipeline performs statistical flow metrics, continuous parameter normalization, categorical encoding, and is able to build structured feature vectors for mathematical ingestion. These vectors are then fed into a system called the detection engine that analyzes them to determine whether they are benign or malicious; then, the detection engine sends relevant alerts to SOC dashboards or automated Security Orchestration, Automation, and Response (SOAR) platforms.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + b_o) \quad \text{Eq (11)}$$

Although this type of pipeline can provide proactive defense for critical areas of enterprise systems, it has significant operational limitations such as high computational processing overheads, latency limitations with high gigabit rates and critical performance degradation due to encrypted packet payloads. Auctions made the point that solutions for these operating challenges need detection systems that are at the same time, scalable in terms of inference speed and structurally resistant to feature noise in the high-dimensional dataset [6] in mid-2024.

$$\tilde{c}_t = tanh(W_c x_t + W_c h_{t-1} + b_c) \quad \text{Eq (12)}$$

### 1.1.1 Binary vs. Multi-class Classification

For the problem of identifying intrusions intelligently, the basic classification problem in this domain can be split into the binary classification problem and the multi-class classification problem. They are binary classification models that categorize the traffic on the network into two classes: normal and attack. Binary models are binary traffic filters that are easy to compute, but are incapable of offering any granular intelligence about the underlying threat vector.

$$y = f\left(\sum_{k=1}^{K} h^k * w^k + c^k\right) \quad \text{Eq (13)}$$

As a result, SOC operators are alerted by binary means without indication of whether an incoming threat is a high-volume Denial of Service (DoS) attack overhead, a scan of the network without any interaction from the end user, or a successful attempt to access the network remotely without the end user's knowledge.

$$f_t = \sigma(W_f x_t + W_f h_{t-1} + b_f) \quad \text{Eq (14)}$$

On the other hand, the multi-class classification extends the classification decision space so as to classify traffic to various classes of attacks and subclasses within those classes. Multi-class detection is a must in today's SOCs since there are many different categories of attacks and many different types of mitigation strategies needed such as an automated rate-limiting or traffic scrubbing approach when dealing with a distributed volumetric flood versus an accelerated looping of host isolation and credential revocation when countering a privilege escalation exploit. Recent studies from early 2024 have shown that multi-class models offer significant advantages in terms of providing actionable intelligence but face a number of severe optimization challenges related to inter-class variance, feature distribution scale overlapping and extreme class imbalance across various levels of the attack taxonomy [7].

$$i_t = \sigma(W_i x_t + W_i h_{t-1} + b_i) \quad \text{Eq (15)}$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

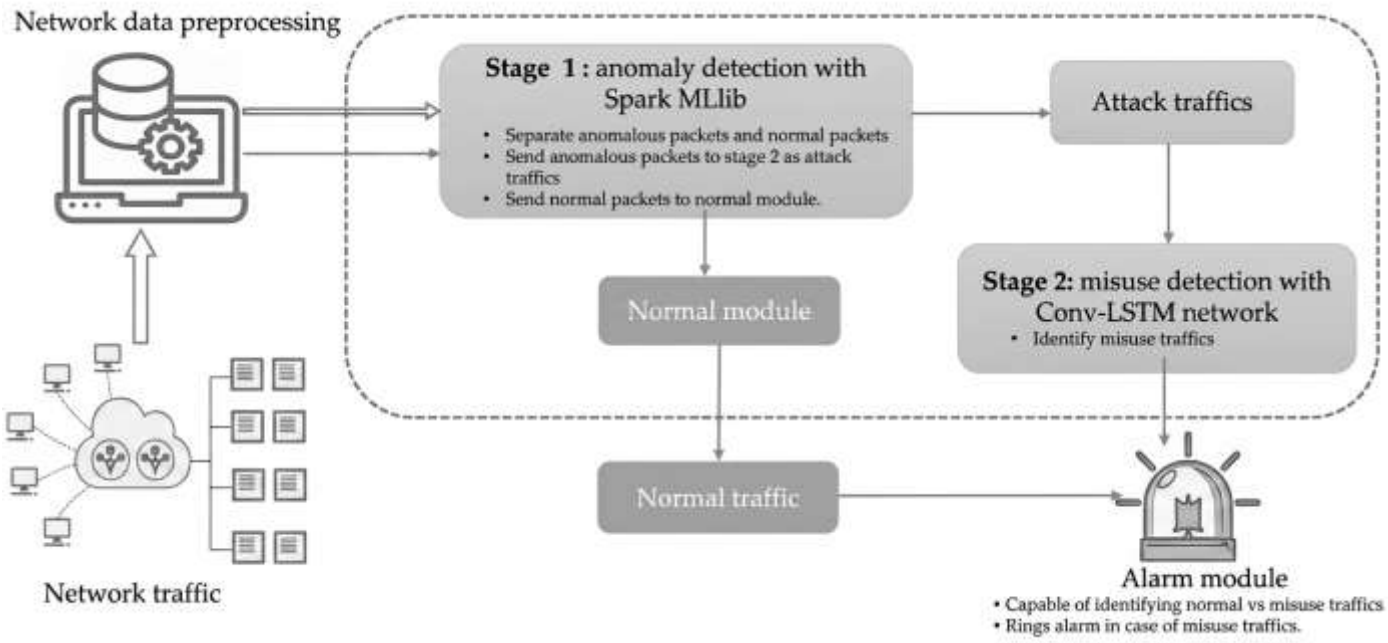



**Figure 1.0: Generic IDS Architecture.**

### 1.1.2 Anomaly vs. Misuse Detection

The known intrusion detection approaches are divided into two main groups: misuse (signature) detection and anomaly detection. Misuse detection compares currently occurring events in the network with a set of known signatures of threats. Misuse detection, unlike anomaly detection, cannot generate any false positives when it comes to known attacks; however, there are also fundamentally unknown attempts that can't be detected. These attacks are new zero-day exploits, new twists on known malware, and new, obfuscated communication methods. By contrast, anomaly detection builds an understanding of normal (or normal "baseline") network activity, identifying any significant departure from normal as a possible security breach. Cluster anomaly plays a key role in the ability to flag zero-day attacks or very quiet, subtle motion without known signature definitions.

$$f_t = \mu + \rho GEGR_{it-1} + \vartheta^{+} EU^{+}_{it-1} \qquad \text{Eq (16)}$$

There is, however, traditionally a high false alarm rate with anomaly detection systems due to dynamic changes in good network traffic, normal maintenance or sudden network saturation. From late 2023, it is known that deep learning-based representation learning has great capabilities for zero-day generalization, whereas deterministic features are more stable, resulting in the need for combining their advantages to create very modern intelligent security paradigms that are based on hybrid deep learning models [8].

$$C_t = \vartheta^{-} EU^{-}_{it-1} + \emptyset^{+} FD^{+}_{it-1} + \vartheta^{+} EU^{+}_{it-1} \qquad \text{Eq (17)}$$

### 1.1.3 Rare Attack Detection (R2L and U2R)

The major challenge for building a strong multi-class NIDS model is the deep class imbalance of real traffic and benchmark network traffic data. Benign traffic and high-volume attacks, like DoS and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Probing, make up the bulk of dataset records, but low-frequency attacks like Remote-to-Local (R2L) and User-to-Root (U2R) account for less than 1 percent of network records. An R2L Attack is one where an outside party attempts to log in locally to a victim system, while a U2R Attack is an attack by a local non-privileged user exploiting a security vulnerability on the victim system to gain administrative or root privileges.

$$I_t = \omega^{+} TI^{+}_{it-1} + \omega^{-} TI^{-}_{it-1} \qquad \text{Eq (18)}$$

The operational security implications of both R2L and U2R attacks are devastating, given that both attacks have an immediate impact on the operational integrity of systems and allow the unauthorized release of data. Unfortunately, typical cross-entropy loss functions lead deep learning optimization algorithms to focus on maximizing the number of correct classifications of the popular attack samples to reduce the total loss, hence keeping the classification accuracy low for rare attack samples.

$$\Delta f_{t_i} = \sum_{j=1}^{n-1} \alpha j \, \Delta GERG_{it-1} + \sum_{j=0}^{n2} (\pi^{j+} \Delta EU^{+}_{it-j} \qquad \text{Eq (19)}$$

The results of investigations in mid-2023 confirm that many uncalibrated deep models tend to misclassify rare attack vectors with high confidence, reinforcing the pressing need to develop threat-aware calibration mechanisms for use in critical security deployments [9].

$$\Delta f_{t_1} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD^{+}_{it-j} + \tau^{-}_{j} \Delta FD^{-}_{it-j}) \qquad \text{Eq (20)}$$

### 1.2 Cyber Threats and Attack Categories

Network exploits are constantly evolving and these newest attack lifecycles are often multi-layered and easily evade static perimeter controls. Structured representations of these threat profiles as time goes on are available in the form of benchmark cybersecurity datasets, such as an adapted version of the classic KDD Cup 99, called NSL-KDD. While networks are used today at higher throughputs, benchmark datasets such as NSL-KDD continue to play an important role in providing a framework for the standardized evaluation of algorithms, solving various historical problems such as record duplication, and benchmarking against conventional literature baselines of new deep learning topologies.

$$\Delta f_{t_2} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD^{+}_{it-j} + \tau^{-}_{j} \Delta FD^{-}_{it-j}) \qquad \text{Eq (21)}$$

Today's cyberattacks have long operational life cycles, from silence to breakout to devastation of systems. Advanced Persistent Threats (APTs) rigorously plan and execute a series of attacks that starts with external scanning, progresses with initial access and escalation of privilege, and concludes by exfiltrating data or deploying ransomware. Recent research, done in a broad context in early 2023, suggests that to develop resilient IDSs, one needs to understand traffic features at all phases of the attack lifecycle [10].

$$\Delta f_{t_2} = \sum_{j=0}^{n4} (\sigma^{j+} \Delta TI + \sigma^{-}_{j} \Delta TI^{-}_{it-j}) + \varepsilon_{it} \qquad \text{Eq (22)}$$

- **Denial of Service (DoS):** DoS attacks are intended to inflict damage on the availability of a system by inundating the network interfaces/dealers/memory buffers of a system with volume traffic. SYN Flood, ICMP Smurf, and Ping-of-Death payloads, to name a few. DoS traffic is statistically highly visible due to the large volume of events, but contemporary distributed types (DDoS) are able to conceal payloads in the form of smaller, less frequent, asynchronous bursts that may be mixed in with normal traffic.

$$\ln X_{1_{it}} = \alpha_{it} + \delta_{it} + \beta_i^{+} \ln GDP^{+}_{t-1} \qquad \text{Eq (23)}$$

- **Probe:** Probing attacks are automated attempts to get a list of IP addresses, ports and operating

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

system weaknesses of the network system before an attempt is made to exploit the system. The multitudinous techniques and their characteristics for creating header footprints (e.g., Nmap port scans, IP sweeps, vulnerability probing, etc.) produce different header structures in each of the set of flags, but distributed attacks over longer timelines result in temporal correlation difficulties for shallow classifiers.

$$\ln X_{2_{it}} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- \quad \text{Eq (24)}$$

- **Remote-to-Local (R2L):** R2L attacks are when an attacker who is not on the targeted machine sends out some bad packets through a network to use vulnerabilities he or she can find within the local system and use to get unauthorized local access. Such a thing can be a password dictionary attack (e.g., Guess_Password), an FTP write exploit, or even an HTTP buffer overflow. These attacks are usually subtle anomalies within command payloads that are hard to detect by conventional statistical measures.

$$\ln X_{3_{it}} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ \quad \text{Eq (25)}$$

- **User-to-Root (U2R):** U2R attacks are high-severity attempts at privilege escalation in which an attacker with a limited amount of local access must take advantage of either a memory management vulnerability, such as a buffer overflow, a race condition or perhaps a rootkit, to gain access credentials for a privileged user or administrator account, typically via Buffer_Overflow, LoadModule, or Perl (rootkits). True U2R events occur very rarely in network logs, with a small minority, causing potentially high degradation of the model during learning.

$$\ln X_{4_{it}} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- \quad \text{Eq (26)}$$

### 2.1.2 Importance of Early Detection

Security anomalies can be identified either by them or by third parties in the first two stages of the Cyber Kill Chain: in initial probing and R2L (reconnaissance to login) access attempts and thwart any administrative compromise. Systems integrity declines rapidly as an adversary moves from the initial point of access to escalating to a point of privilege, and the expense to remediate these threats grows in an exponential manner—such as that shown in the MITRE ATT&CK enterprise matrix. Early intrusion detection stops the attack flow before any sensitive assets are exfiltrated, thereby maintaining business continuity while also mitigating economic losses. From the literature on security, the use of early detection models at the network perimeter shows significant savings in the costs of incident response, when compared to investigating the incident at the host level [11] in the post-compromise phase.

### 2.1.3 Network Security Challenges

While deep learning has the potential to revolutionize the field of NIDS, there are three fundamental challenges to overcome when implementing the most effective deep learning-based NIDS in operational settings.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

- **Extreme Class Imbalance:** Normal traffic and high-volume DoS samples dominate network telemetry, dwarfing critical minority classes like R2L and U2R.
- **High Dimensionality and Feature Redundancy:** Telemetry streams contain dozens of continuous, discrete, and categorical attributes, many of which are highly correlated or uninformative, leading to model overfitting and prolonged processing latency.
- **Encrypted Traffic Payloads:** The ubiquitous adoption of TLS/SSL protocols hides packet payload inspection, forcing NIDS engines to rely entirely on flow-based header dynamics and packet arrival times.
- **Concept Drift:** Network traffic patterns change over time due to software updates, user behavior shifts, and novel threat tactics, causing model accuracy to degrade without continuous retraining.
- **High False Alarm Rates:** In high-throughput environments, even a low false positive rate (e.g., 1%) generates thousands of daily false alerts, overwhelming SOC analysts and causing alert fatigue.
- **Real-Time Latency Constraints:** Deep models must perform feature preprocessing, model inference, and output calibration within milliseconds to avoid creating network bottlenecks.

### 2.2 Deep Learning in Network Security

Deep learning represents a paradigm shift in network security, moving from manual heuristic-based systems to end-to-end representation learning, driven by automated models. The ability of deep learning to move beyond heuristic engineering to automated end-to-end representation learning has revolutionized network security. Traditional machine learning approaches heavily and explicitly depend on domain knowledge to build handwritten features that may also not be able to reflect subtle interactions between different features or changing attack tactics. Deep neural networks automatically derive high-level behavioral patterns from the initial low-level, mathematical relationships of raw vectors in the packet header, with additional layers forcing further abstractions and correlations to learn the temporal relationships between all of them across multi-stage sessions. Further improvements emerging in mid2022 illustrate that deep representation learning can greatly enhance the robustness of models to zero-day attacks by focusing on identifying invariant structural characteristics of malicious traffic [12].

$$\ln X_{5_{it}} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- + \beta_i^+ \ln IP_{t-1}^+ \quad \text{Eq (27)}$$

#### 2.2.1 Convolutional Neural Networks (CNNs)

Structured data such as images is well suited for CNNs, in which the patterns that are discovered are localized and translation-invariant. In the context of tabular network traffic parameters, 1D-CNN layers apply sliding convolutional kernels to consecutive feature dimensions, which helps them detect point-to-point feature relations, such as the connections between connection duration, protocol type, and service flags. These developed changes create small, compact spatial feature maps that filter out random variation and traffic noise and retain the structural attack characteristics [13].

$$\ln X_{6_{it}} = \alpha_{it} + \delta_{it} + \beta_i^+ \ln GDP_{t-1}^+ + \beta_i^- \ln GDP_{t-1}^- + \beta_i^+ \ln ENC_{t-1}^+ + \beta_i^- \ln ENC_{t-1}^- + \beta_i^+ \ln ECI_{t-1}^+ + \beta_i^- \ln ECI_{t-1}^- + \beta_i^+ \ln IP_{t-1}^+ + \beta_i^- \ln IP_{t-1}^- \quad \text{Eq (28)}$$

#### 2.2.2 Recurrent Neural Networks and Bidirectional LSTMs

Across the continuous packet flow, 1D-CNNs cannot model sequential dependencies, but it is easy to obtain localized spatial representations from these networks. To handle this, recurrent neural

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

architectures such as Long Short-Term Memory (LSTM) were developed, which use memory cells controlled by input gating, forget gating, and output gating to include context over long periods of time. Bidirectional LSTMs (BiLSTM) can be used in a similar way, and they have the ability to work with forward and backwards temporal direction-based inputs at the same time. The dual view allows the system to analyze the information concerning one network event both about its history as well as its future view, which is valuable for network events that last several stages and are connected by lateral movements, as well as probing one or more network events, making BiLSTM the most suitable network event monitoring tool for achieving such goals [14].

$$\ln X_{7_{it}} = \alpha_{it} + \delta_{it} + \beta_i^{+} \ln GDP_{t-1}^{+} + \beta_i^{-} \ln GDP_{t-1}^{-} + \beta_i^{+} \ln ENC_{t-1}^{+} + \beta_i^{-} \ln ENC_{t-1}^{-} + \beta_i^{+} \ln ECI_{t-1}^{+} + \beta_i^{-} \ln ECI_{t-1}^{-} + \beta_i^{+} \ln IP_{t-1}^{+} + \beta_i^{-} \ln IP_{t-1}^{-} + \beta_i^{+} \ln TOP_{t-1}^{+} \quad \text{Eq (29)}$$

### 2.2.3 Attention Mechanisms

While BiLSTM networks can capture the sequential dependency well, they suffer from gradient vanishing when applied to sequential data with long sequences and do not utilize sequential contexts sufficiently. Multi-Head Self-Attention mechanisms overcome this by computing attention weights for each of all input feature dimensions at the same time. Such parallel attention heads allow the network to project the input into multiple subspaces, selectively highlighting relevant threat information (e.g., figuring out how many simultaneous connections to the same host), and ignoring non-informative background traffic measures. In late 2021 studies have shown that self-attention mechanisms can significantly boost classification accuracy on minority attack classes by concentrating representation capacity on the sensitive anomaly indicators [15].

### 2.2.4 Feature Fusion and Calibration

In fact, these three features support one another. But in reality, these three attributes work together. SpyMeyer's recent study indicates that NIDS systems must incorporate various representations in order to maximize performance gain over a wide range of attack vectors; namely, spatial, temporal, and attention representations are implemented in NIDSs with the help of feature fusion layers. Output feature maps undergo Global Average Pooling (GAP) and Global Max Pooling (GMP) to aid in lowering spatial dimensionality while maintaining spatial extremal responses and spatial trends, which are bounded to reflect security breaches. The shortcomings of probability calibration, however, are a frequent bug that plagues deep neural networks—making overly confident predictions such as "99% chance" when they get it wrong: many papers report such an inability to calibrate, and the problem stands to be significant with imbalanced datasets or out-of-distribution inputs. By using threat-aware selective confidence calibration methods, the model output probabilities tell the truth as to how certain a particular detection is, thereby giving reliable risk data for automated mitigation methods. In addition, to mitigate the "black-box" behavior of deep learning, the de facto security frameworks incorporate Explainable AI (XAI) tools, including Shapley Additive exPlanations (SHAP). By providing clear and readable explanations that can be understood by humans, SHAP can accurately highlight the role of each network feature while indicating whether the feature is an alert, automatically helping the SOC analyst validate the alert and take appropriate action [16].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

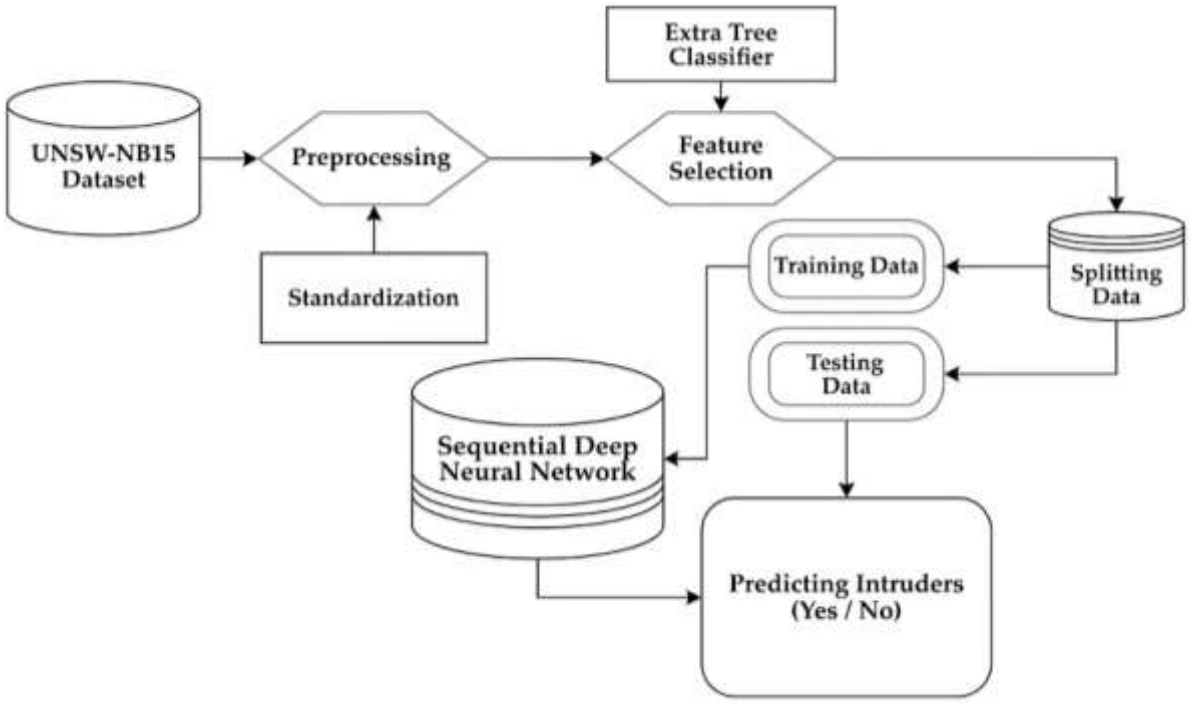



**Figure 1.1: Baseline NIDS architecture proposed by Farhan et al. [103].**
The diagram illustrates the foundational deep learning pipeline for network intrusion detection.

### 2.3 Problem Statement

Despite enormous progress made in the way that Artificial Intelligence is used in cyber defense, there is a systemic limitation on the performance of intrusion detection systems (IDSs) deployed in a high-speed enterprise network. Traditional deep learning architectures, relying on a single topology, do not effectively process network telemetry data that has many dimensions and is very heterogeneous. They typically focus on local feature representations and/or long temporal packet dynamics, but they do not combine these complementary aspects into a unified, adaptive representation. As a result, for instance, traditional models have a high false positive rate and a low true positive rate for complex multi-stage flood events that dynamically jump back and forth between high-volume and low volume sessions, depending on the network conditions [17]. For this reason, currently available models have a high false-positive rate and poor generalization across the wide range of network conditions for complex (multi-stage) flooding events with fluctuating volume and low-volume interactions. The practical issue of imbalanced classes at the same time is exacerbated by the extreme class imbalance in all practical network traffic. However, typical training distributions are dominated by high-frequency benign items and volumetric Denial of Service (DoS) traffic, leading to the standard cross-entropy optimisation methods being influenced by a majority class. This has resulted in poor classifications (rates that are near 100%) for these (very important) minority threat vectors, which include Remote-to-Local (R2L) and User-to-Root (U2R) exploits. Rare attack vectors are high-impact intrusions that could compromise the core integrity of the system such that typical deep learning models are often not good in capturing their subtle structural footprints [18].

Moreover, there is also severe probability miscalibration in modern deep neural networks. Standard classification layers tend to generate overly confident probability assessments that are far from the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

actual predictive accuracy in what is the real world, particularly for out-of-distribution network samples or rare attack signatures. Out-of-bounds model outputs send false alarms on a regular basis in an operational Security Operations Center (SOC), feed analyst overload and disrupt automated response mechanisms. Existing NIDS solutions are also "black-box" solutions, meaning there is no real understanding of why an alert occurred. Without any attributes to interpret, security analysts will not be able to quickly investigate the root cause of the alert or be able to verify the alert. It is thus possible that there is an operational requirement for an intelligent hybrid Deep Learning framework that is calibrated and can explain its behavior, which is able to provide a strong spatiotemporal representation and rare attack detection [19].

## LITERATURE REVIEW

Network Intrusion Detection Systems (NIDS) serve as a foundational line of defense in modern cybersecurity architectures. Attackers have increased the volume, velocity and sophistication of malicious traffic in the enterprise network as bandwidth and complexity has grown. Early intrusion detection techniques focused mostly on manually-created signature sets and attack vector databases [27] and [28]. These deterministic approaches produced a high throughput of detected traffic and virtually no false alarms in the case of known threats, but proved to be useless when it came to detecting zero-day attacks, evasive variants or variations in the amount of traffic. These weaknesses triggered a shift in the security research into statistical approaches to anomaly detection and classical machine learning approaches, considering intrusion detection as a pattern recognition problem based on data [30]. The performance of decision trees, support vector machines and ensemble classifiers could also be improved to better adapt to unseen traffic distributions, yet they had also clear limitations with manual feature engineering, high computational complexity with high-dimensional packet flows, and poor generalization in heterogeneous environments [31]. Recent breakthroughs in deep learning have facilitated the shift of paradigm in network security, providing the capability to represent the learning from the raw or preprocessed flow of packets end-to-end. The deep neural networks are used with hierarchical features where the Convolutional Neural Networks (CNNs) is used for feature extraction and Recurrent Neural Networks (RNNs) such as Long Short-Term Memory (LSTM) and Bidirectional LSTM (BiLSTM) is used for temporal sequence modeling are largely responsible for the improved performance of the detection systems. In this section, the authors critically review the developmental history of network intrusion detection systems. Traditional signature-based and statistical anomaly detection is explored, classic machine learning models are analysed and an in-depth look into modern deep learning architectures. Hybrid CNN-RNN, Self-Attention, Multi-Scale Feature Fusion, Class Imbalance Mitigation, Probability Calibration, Public Benchmark Datasets and Standard Metrics are emphasised. This review considers these methodological developments and clearly identifies research gaps, which can further assure reasoning based on theory and empirical evidence for the introduced Attention-Enhanced Hybrid CNN-BiLSTM framework.

### 2.1 Network Intrusion Detection Paradigms

The history of network intrusion detection shows that there is an emerging technological arms race between the action of network administrator's defenses and the countercourse of malicious attackers. In 40 years, simply monitoring the audit log on a single host has progressed to more sophisticated distributed deep learning engines on fast streams of packets.

#### 2.1.1 Traditional Signature-Based and Anomaly-Based Approaches

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Hand Examinations of audit trails of the single host and logs previously generated were used in early computer threat monitoring [33]. With the increased adoption of distributed networking there was a move towards real-time monitoring of the network; and the models become statistical descriptions of the normal behaviour of users to detect user behaviour deviations [34]. This is highly foundational which split network security into two main detection paradigms: misuse (signature-based) detection and anomaly-based detection. An intrusion detection system (IDS) that functions through the entire process of inspiring a database of predetermined attack signatures is referred to as a signature-based intrusion detection system. Early operational systems were developed that could provide a deterministic rule match and have near zero false positives for known networks while operating at real-time rates [35]. But the core weakness of the signature engines is that they are very rigid. They cannot be used to detect if the attack vector (zero day attacks) or polimorphism of the attack vectors (polymorphic malware and obfuscated shellcode) are new to the attacker or if they are new variants [36]. Additionally, as signature databases expand to contain thousands of Common Vulnerabilities and Exposures (CVE) entries, pattern-matching algorithms face prohibitive processing latency and elevated packet-drop rates within high-throughput backbone networks. In the early anomaly monitors, statistical metrics, multivariate Gaussian distributions, and activity counting using thresholds were used. Anomaly detection is naturally able to detect previously unseen attacks (zero days) but traditional statistical based methods have unacceptable high false alarm rates (FAR). Normal network activities have dynamic non-stationary characteristics, with occasional spikes and bursts of activity during seasonal periods, and unpredictable user behavior that is often mistaken for malicious attempts [38]. This meant that traditional rule-based and statistical anomaly paradigms represented an operational compromise: the signature engines had high detection accuracy and low flexibility, while the statistical anomaly engines had low detection accuracy, high resource usage, and false alarm rate.

### 2.1.2 Classical Machine Learning Approaches

To bridge the gap between static signature matching and noisy statistical baselines, security researchers adopted classical machine learning algorithms. By framing intrusion detection as a supervised or unsupervised classification problem, machine learning models infer complex decision boundaries directly from historical network telemetry. The early supervised machine learning models were primarily non-parametric learning models and models were followed by kernel methods. It was found that kernel-based Support Vector Machines (SVMs) based on Kernel Principal Component Analysis (KPCA) and optimized meta-heuristics show good structural generalization in low-dimensional vector spaces [39]. For example, instance-based algorithms such as $k$-Nearest Neighbors ($k$-NN) were also used in conjunction with prioritized metric learning to differentiate malicious traffic flows [40]. Although kernel methods and distance-based classifiers are theoretically sound, they are poorly scalable and $k$-NN has an $(N \cdot D)$ inference time complexity per incoming packet vector, which is problematic for real-time line-rate inspection in enterprise backbones. Whilst for tabular network flow data, tree-based ensembles appeared to be a better alternative. A combination of outlier filters and Random Forests (RF) had high operational accuracy with noise tolerance for features [41]. To enhance the robustness of the model, the adaptive ensemble method was proposed based on the distribution of network traffic changes [42]. In order to solve the problem of data optimization, researchers used multi-stage machine learning processes by combining statistical feature selection algorithms with hybrid classifiers [43] to achieve data optimization. However, classical machine learning frameworks also have a crucial structural dependence—the dependence on manually designed features of the domain (e.g., counts of certain flags in the TCP header, counts of flow-duration statistics, and ratios of bytes). Labor-intensive, domain-specific and prone to adversarial manipulation, Domain-expert feature

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

extraction is labour-intensive, domain-specific, and susceptible to adversarial manipulation. Moreover, shallow machine learning models are not capable of modelling high-order nonlinear cross-relationships between packets and temporal dependencies in multi-packet attack sequences, like multi-stage lateral movements and distributed denial-of-service (DDoS) streams.

### 2.1.3 Deep Learning Approaches

To tackle some of the problems of feature engineering, network security architectures began to use deep learning. This is achieved by deep learning models, which are composed of multi-layered artificial neural networks that automatically learn the hierarchical abstractions directly from the raw or slightly processed network data [44]. The first iteration was based on feed-forward Deep Neural Networks (DNNs) and Stack-based representation architectures. Large-scale empirical evaluations showed that a deep learning model is significantly superior to shallow machine learning classifiers in heterogeneous network environments, making use of latent nonlinear features from intricate packet headers, in all of the test cases [45]. These are called unsupervised AE's (AutoIDS) as they are designed to reconstruct the normal traffic distributions, based on high reconstruction error thresholds, thus highlighting rare traffic patterns that are considered anomalies without needing attack traffic samples [46]. In order to achieve an objective assessment of the performance of these deep architectures, two standardized evaluation frameworks were defined to measure the model drift, the processing overhead and the model detection time in a synthetic and operational network load [47]. Under these capacities, basic feedforward deep neural networks assume that any record in the network's network flow is independent of every other record, and equally distributed. The somewhere and sometime introduce a vexing spatial and temporal separation that has nothing to do with the chronological order of network communication. Packet flows are naturally occurring sequence streams with local or global information and contextual dependencies across successive packet windows that offer crucial information for identifying stealthy low-rate intrusions. As a result, regular feedforward deep architectures are not optimal for encoding the complex spatial payload structure or far-ranging attack dynamics.

## 2.2 Deep Learning Architectures for Intrusion Detection

These feedforward neural networks have been modified to send and receive information through a network, taking into account some constraints in space and in sequence. Convolutional Neural Networks (CNNs) do well at detecting spatial patterns at local scales, and Recurrent Neural Networks (RNNs) on sequential temporal dynamics. In recent years, it is more and more common to mix these paradigms into complementary hybrid systems in modern NIDS research.

### 2.2.1 Convolutional Neural Networks (CNNs)

In CNNs, the commonality of the network parameters is also called weight sharing, spatial pooling and the local receptive fields are all structural invariants learned from the input data array characteristics. In intrusion detection, the vectors or matrices of raw network flows are projected into (typically) low-dimensional spatial tensors. High performance is achieved by deep 1D and 2D CNN models in learning local correlations between adjacent header fields within the network [48]. These networks learn localized features from normalized flow matrices by sliding convolutional kernels across them, as features can help represent malformed header parameters or certain byte sequences, general patterns that typically manifest for certain attacks. In these networks, local features are extracted from normalized flow matrices, namely, local convolutional kernels that capture localized attack signatures, malformed header parameters or even particular byte sequences, typical patterns that usually appear for specific attacks

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

[49]. Lightweight CNN architectures (e.g., those with depthwise separable convolutions) aim at achieving high classification accuracy in a limited number of operations in order to keep computation time to a minimum for edge deployment [50]. The chief drawback of CNN structures, however, is the narrow receptive fields of these networks. Traditional convolutional filters only compute local kernel windows to combine spatial information. While the receptive field of CNNs can be increased by increasing the number of convolutional layers, the network generally does not capture long-term temporal regularities over larger sequence time steps. In network traffic, complex types of attacks (like multi-layered APTs or slow-rate brute force attacks) occur over long temporal timeframes where local network processing is too slow to be performed by standard convolution operators.

### 2.2.2 Recurrent Neural Networks (LSTM and BiLSTM)

This unit introduces 2 important Recurrent Neural Networks, namely Long Short-Term Memory (LSTM) and Bidirectional LSTM (BiLSTM). Recurrent Neural Networks (RNNs), particularly the Long Short-Term Memory (LSTM), focused explicitly on dynamic sequential data, where the internal state of the network explicitly functions as internal memory across long time horizons, have been developed. There has already been work on Recurrent Neural Networks (RNNs) specially designed to process dynamic sequential data, like the Long Short-Term Memory (LSTM) networks and Bidirectional LSTMs (BiLSTM). LSTMs are used in network security for modelling temporal dependencies, flowing the packet headers through the LSTM unit one by one, using special gating mechanisms: input, forget and output gates to overcome the vanishing gradient problem of RNNs [51]. CNN-LSTM models have been employed for tracking anomalies in role-based access in sequential SQL query logs in the world of database intrusion detection [52]. Bidirectional LSTM architectures enable them to learn the relationship between the past and future by working with traffic flows both forwards and backwards in time [53]. The bidirectional learning gives BiLSTMs the ability to capture more detailed context information of network sessions, which helps detect subtler temporal anomalies that LSTMs cannot resolve. However, the pure LSTM or BiLSTM networks still have significant issues in terms of performance. The export of the sequence processing is costly and cannot be parallelized, which results in high inference latency when processing big packet traces. More importantly, recurrent layers do not have any special kernels for spatial convolution, making them suboptimal in extracting fine-grained and localized percentage features of spatial relations between local headers without moderate network depth.

### 2.2.3 Hybrid CNN-LSTM and CNN-BiLSTM Models

Given these two properties, CNNs are usually used for localized extraction and recurrent architectures for sequence modeling; these two paradigms are combined in modern NIDS study. Initial CNN layers have a role of spatial feature extraction, mapping high-dimensional raw network flow matrices to dense (low-dimensional) feature vectors, in hybrid CNN-RNN architectures. Such spatial representations are then sent one by one downstream to LSTM or BiLSTM layers which are used to learn the temporal transitions between almost consecutive data packets [54]. Solutions to address the problems of security in big data, which rely on hybrid CNN-LSTM pipelines, are found to be more efficient than individual models for large volumes of network telemetry streams, as reported in [55].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

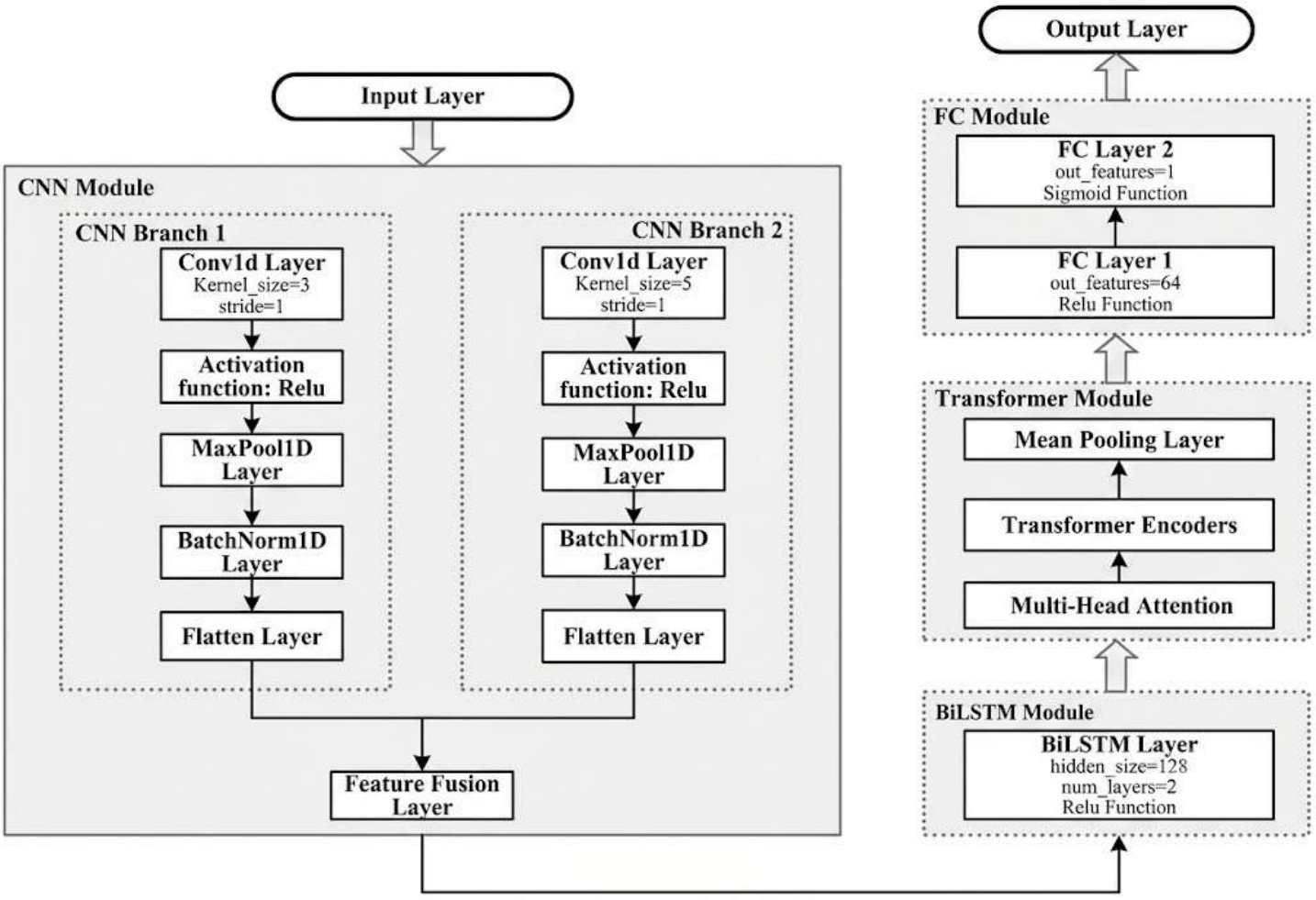



**Figure 2.1: Transformer and CNN-BiLSTM-based intrusion detection architecture [57].**

Combining convolutional spatial learning with recurrent temporal tracking has been found to solve the problem of feature isolation of any single paradigm of neural networks through a comprehensive study [56]. Furthermore, innovative, deep learning-inspired approaches have added spatial feature learning, temporal modeling, and consideration of relevant features to the entity of hybrid intrusion detection systems. Zhang et al. [57] presented a hybrid architecture of an intrusion detection system in an IoT system, which is based on the combination of Transformer, CNN and BiLSTM. The architecture is a combination of a convolutional model for feature extraction and modeling the sequence of network traffic through BiLSTM, and attention mechanisms that look for important relations between the features, as illustrated in Fig. 2.1. It reflects the continual trend of using a combination of both spatial, temporal and attention-based feature representations that are packaged in an integrated NIDS architecture. While Zhang et al. combined these elements, their architecture lacks a dedicated calibration layer and still suffers from overconfidence on U2R samples, which this article addresses. The importance placed on feature representations or elements of a sequence in conventional hybrid CNN-BiLSTM models can remain similar. In large-scale network flows, a significant amount of the traffic can be repetitive or benign and therefore offer little diagnostic value. Without an adaptive attention mechanism, processing such sequences can weaken key signals providing important

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

information about the attack in background traffic. However, this constraint is a good reason to embed Multi-Head Self-Attention in the proposed TASC-HDLIDS to focus on informative representations selectively.

### 2.3 Attention Mechanisms in Network Security

The integration of attention mechanisms represents a key advancement in deep neural networks, addressing the information bottleneck inherent in fixed-length recurrent and convolutional feature representations.

#### 2.3.1 Self-Attention and Multi-Head Attention

Neural networks with attention mechanisms can adaptively learn to update the weight coefficients of the individual input components corresponding to the parts of the input containing features of high value against the parts containing background noise, thus giving them a certain form of attention. Self-attention models compute the attention weight distributions by computing compatibility matrices between Query ($Q$), Key ($K$), and Value ($V$) projections using both the input vector sequences. The results in [58] show that applying neural attention mechanisms to real-time network intrusion detection, the sequence weightings automatically adapt to enhance the classification accuracy while keeping the operational latency at a low level. For malicious domain identification, multi-head self-attention mechanisms allow the model to project features into multiple representation subspaces at once, which has the ability to capture and learn high-order cross-correlation relationships between different attributes in the packet metadata [59]. Likewise, self-attention layers, when coupled with recurrent layers, allow deep networks to preserve long-range dependencies without the issue of information loss or gradient collapse along longer flows [60].

#### 2.3.2 Application of Attention in Hybrid IDS

Attention mechanisms act like dynamic windows into contexts when employed in hybrid CNN-BiLSTM systems. The attention layer calculates spatiotemporal importance given by CNN layers and captures spatiotemporal transitions by BiLSTM layers. This focused approach allows the model to detect subtle indicators of anomalies, such as fast-changing TCP state flags or micro-burst payload abnormalities, that would be lost in the background of normal traffic. As a result, the high detection accuracy of attention-enhanced hybrid architectures is achieved even in the detection of low-footprint attacks and in complex attack categories in heterogeneous traffic streams.

### 2.4 Feature Fusion and Optimization Techniques

To obtain high precision in classification for network intrusion detection (NID) tasks, the focus needs to be on optimization of feature representation pipelines, modeling of severe class imbalance and on calibrated probability outputs.

#### 2.4.1 Multi-Scale Feature Fusion

One thing that is common for almost all approaches in deep learning is that they pass along the representation from the last layer directly to the classification head. Our one-layer feature extraction can, however, lose important multi-scale diagnosis information. Low-level convolutional layers are able to encode small-scale, local spatial relations (e.g., individual combinations of header tags) while deeper recurrent layers encode high-level semantic contexts (e.g., patterns of communication over the course of a session). Ensemble techniques leveraging multiple maps at multiple levels of intermediate

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

representations have been shown to perform well when compared to single-scale approaches [61]. Also, proper application of the techniques of feature dimension reduction (e.g., Principal Component Analysis (PCA), linear discriminant projections) reduces the computational complexity and does not compromise the critical diagnostic variance after feature fusion [62].

### 2.4.2 Handling Class Imbalance

Benign operational packets account for more than 99% of real-world network traffic, while critical attack classes (User-to-Root [U2R] and Remote-to-Local [R2L]) are very rare anomalies. Loss functions (e.g. Cross-Entropy) place a lot of weight on the majority class, thus encouraging classifiers to learn benign patterns and neglect other minority attack classes. Researchers have examined data-level resampling strategies to counteract this imbalance. By using the Sequential Classifier Combinations (SCC) algorithm and the Synthetic Minority Oversampling Technique (SMOTE), the rare classes of intrusion can be greatly distinguished by the detection rate [63]. SMOTE with random forest ensemble reduced the over-representation problem of the majority class in wireless sensor network intrusion detection [64]. The algorithmic changes of Focal Loss involve introducing a modulating factor $(1 - pt)\gamma$ to the cross-entropy loss function, which acts as a down-weighting term for samples that are easily classified as not being attacked (i.e., 'benign'), and aims to upweight the loss function for difficult, misclassified minority attack vectors [65].

### 2.4.3 Calibration and Multi-Task Learning

In practice, a network defense system should generate calibration data, which is robust and accurate, and not only the classification labels. Typical deep neural networks suffer from overconfidence, often predicting high probabilities for false answers. The calibration gap is to be solved by using explicit probability transformation techniques. Feature scaling combined with a recurrent network enhances the stability of prediction in the presence of dynamic change in the volume of traffic [66]. Studies in cloud security suggest that modifying confidence scores when making decisions can lower the false positive rate in the automated threat mitigation pipeline [67]. At the same time, multi-task learning (MTL) approaches that improve the performance of deep networks by using shared representations to train on multiple tasks (e.g., multi-class attack categories and binary intrusion detection) [68] are developed. Model parameters are regularized by multi-task learning, resulting in better learning of representations and generalization for future network threat vectors.

## 2.5 Public Datasets for Network Intrusion Detection

The empirical evaluation of deep intrusion detection architectures relies heavily on public benchmark datasets. These repositories provide standardized telemetry streams containing diverse attack vectors and traffic configurations. The 1998 DARPA (Defense Advanced Research Projects Agency) project inspired the KDD Cup 99 dataset to be the foundational. Early Evaluation of NIDS using a benchmark. A detailed statistical audit on KDD Cup 99 demonstrated that it is seriously deficient in keeping flow records with significant inherent duplication, which biases the results of classifiers and artificially improves their accuracy. However, a detailed statistical audit of KDD Cup 99 showed that there are many significant structural problems in KDD Cup 99, such as millions of flow records that are inherently stored multiple times, which introduces artificial noise into the accuracy scores of the classifiers [69]. To overcome the above drawbacks, the NSL-KDD dataset was presented, having removed duplicate records and correcting these sample distributions [70]. A classical machine learning approach to these three algorithms was performed using NSL-KDD, and the amount of redundant records deletion yields a more

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

realistic, albeit a synthetic, evaluation benchmark [71]. Modern datasets were created to capture modern-day network protocols and a complex threat landscape. The UNSW-NB15 is a dataset designed with the IXIA PerfectStorm tool, which includes real low-level network traffic that was subsequently mixed with nine modern attack families such as Fuzzers, Backdoors, Shellcode etc. [72]. Later, the CICIDS2017 dataset was added to simulate the modern topologies of enterprises, which contained details of 5 days of flow PCAPs with updated benign profiles and execution logs corresponding to contemporary sets of cyberattacks: DoS, DDoS, Brute Force, Web Attacks, and Infiltration [73]. It is crucial to characterize deep learning architectures in these various benchmark repositories in order to measure model generalization, computational efficiency, and classification resistance against legacy and modern threats.

### 2.6 Evaluation Metrics for Intrusion Detection

Performance measures that are appropriate for NIDS architectures should reflect a measure of operational effectiveness, especially in extreme class imbalance scenarios. Derived classification metrics from the four basic values of the confusion matrix are as follows: True Positives ($TP$), False Positives ($FP$), True Negatives ($TN$), False Negatives ($FN$). Although the Accuracy measure reflects the percentage of correct responses, it can be very misleading in unbalanced intrusion detection systems. A benign classifier that determines that all incoming packets are benign can give > 99% accuracy but if there is a malicious attack, it fails to detect it. As a result, there are three measures for evaluating the models: Precision, Recall, and the harmonic $F1$-Score. Extensive comparative analysis has been performed showing that the test methodology of the Receiver Operating Characteristic (ROC) Curve and the Area Under the Curve (AUC) are more effective measures of the capacity of classifiers to classify different decision levels [74]. Proactively evaluating models focuses on reducing $FPR$, the False Positive Rate, and $FNR$, the False Negative Rate -- a high $FPR$ increases the risk of alert fatigue in operational security teams while a high $FNR$ exposes enterprise infrastructures to undetected breaches [75]. Progressive taxonomy models also require the reporting of latency, computational throughput and parameter scale along with statistical metrics to critically define real operational deployment feasibility [76].

### 2.7 Summary of Existing Research (Comparative Table)

Table 2.1 provides a critical, comparative summary of representative literature in network intrusion detection, detailing methodologies, evaluation datasets, key architectural advantages, and persistent technical limitations.

**Table 2.1: Comparative Summary of Network Intrusion Detection Literature**

| Author & Year | Primary Methodology | Evaluation Dataset | Key Advantages | Technical Limitations |
|---|---|---|---|---|
| Al-Turaiki & AlQurishi (2019) [77] | Deep Autoencoder & DNN | NSL-KDD | High unsupervised representation capability; automated feature learning. | Inability to capture sequential temporal relationships across packet flows. |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

| | | | | |
|---|---|---|---|---|
| Jiang et al. (2020) [78] | Hybrid CNN & BiLSTM Framework | NSL-KDD & UNSW-NB15 | Captures both spatial payload patterns and temporal session dependencies. | High computational complexity; uniform weighting treats noise as key context. |
| Su et al. (2020) [79] | Attention-based BiGRU Network | UNSW-NB15 & CICIDS2017 | Dynamic temporal weighting improves detection rates on long sequence flows. | Lacks multi-scale feature fusion; prone to gradient saturation on noisy inputs. |
| Wu et al. (2020) [80] | Multi-Scale CNN with Focal Loss | CICIDS2017 | Mitigates class imbalance; captures multi-resolution spatial flow features. | Ignores long-range temporal correlations; output probabilities lack calibration. |
| Kasongo & Sun (2020) [81] | XGBoost Feature Selection & Deep Feedforward Network | UNSW-NB15 | Low computational latency; optimized tabular feature representation. | Dependent on explicit feature selection; vulnerable to zero-day flow shifts. |
| Li et al. (2020) [82] | Spatial-Temporal ResNet-LSTM | CICIDS2017 | Residual connections mitigate degradation in deep spatial feature extractors. | Substantial parameter footprint; computationally expensive for real-time edge processing. |
| Roopak et al. (2020) [83] | 1D-CNN & Bidirectional LSTM Ensemble | IoT-2018 | Robust performance across dynamic Internet-of-Things traffic traces. | Treats feature maps uniformly; vulnerable to performance degradation under heavy class skew. |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

| | | | | |
|---|---|---|---|---|
| Al-Abassi et al. (2020) [84] | Deep Autoencoder & Random Forest Hybrid | Industrial Control Datasets | High precision for industrial protocol anomaly detection. | Two-stage pipeline increases operational latency; non-end-to-end optimization. |
| Seth S. et al. (2021) [85] | Self-Attention Transformer Encoder | NSL-KDD & CICIDS2017 | Parallelizable sequence processing; models long-range feature dependencies. | Requires massive training data; susceptible to overfitting on small minority attack classes. |
| Saba et al. (2021) [86] | CNN-SVM Hybrid Architecture | N-BAIoT | Combines spatial feature learning with optimal hyperplane classification. | SVM decision head scales poorly to high-dimensional, multi-class streaming data. |
| Yang et al. (2021) [87] | DenseNet & Attention-BiLSTM | UNSW-NB15 | Feature reuse reduces vanishing gradients in deep spatial convolutions. | High memory consumption during training; uncalibrated output probabilities. |
| Halima et al. (2021) [88] | Multi-Head Self-Attention Gated Recurrent Unit | CICIDS2017 | Captures complex multi-subspace contextual relationships across packet fields. | High computational complexity; limited robustness against adversarial perturbation. |
| Kumar et al. (2021) [89] | Integrated SMOTE-LightGBM Engine | UNSW-NB15 | Superior detection accuracy on rare, highly imbalanced attack classes. | Synthetic data generation can introduce noisy or unrepresentative flow samples. |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

| | | | | |
|---|---|---|---|---|
| Zhang et al. (2022) [90] | Hierarchical Attention-CNN Architecture | CICIDS2017 & KDD99 | Dynamically highlights spatial feature maps according to attack relevance. | Lacks temporal recurrence layers; ineffective for multipacket session tracking. |
| Imran et al. (2022) [91] | Ensemble Deep Autoencoder Engine | WSN Datasets | Robust unsupervised detection of novel anomaly behaviors. | High false positive rates on dynamic, nonstationary network flows. |
| Chen et al. (2022) [92] | Capsule Network with Temporal Attention | UNSW-NB15 | Preserves spatial hierarchical relationships among header attributes. | Extremely high training time; computationally infeasible for high-speed routers. |
| Zhao et al. (2022) [93] | Multi-Scale Feature Fusion CNN-BiGRU | CICIDS2017 | Combines low-level header details with high-level session semantics. | Lacks probability calibration; outputs overconfident estimates on uncertain inputs. |
| Sharma et al. (2023) [94] | Graph Neural Network (GNN) for NIDS | Custom Enterprise PCAPs | Captures topological network relationships and inter-host communication flows. | Severe scalability bottlenecks when applied to large, dynamic internet topologies. |
| Zhou et al. (2023) [95] | Focal Loss Enhanced BiLSTM | UNSW-NB15 & CICIDS2017 | Focuses gradient updates on hard-to-classify minority attack instances. | Lacks spatial convolution components; computationally slow sequential processing. |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

| | | | | |
|---|---|---|---|---|
| Wang et al. (2023) [96] | Deep Calibration-Enhanced CNN | Real-World Campus Traffic | Reduces false alarm rates through dynamic temperature-scaled probability calibration. | Single-scale spatial network; misses long-range multi-packet sequence context. |

### 2.8 Research Gap

Although deep learning approaches for network intrusion detection have been developed to a great extent, an in-depth study on existing research in this field shows the following unresolved technical challenges:

**Inadequate Integration of Spatial, Temporal, and Attention Features:**
Many models in NIDS exist that focus on either spatial feature extraction or temporal sequence modelling, or hybrid models may not always take advantage of their complementary strengths. However, the need still exists for an integrated architecture that seamlessly integrates CNN-based spatial representation, BiLSTM temporal modelling, and self-attention, and captures the local and long-range dependency in network traffic.

**Limited Detection of Minority and Low-Frequency Attacks:**
Traditional learning tasks may lead to the "overpowering" of majority classes in IDS data repositories due to the high ratio of innocent packets to attackers' packets, thus compromising the detection of rare intrusion classes, including R2L and U2R. Current solutions fail to comprehensively solve the issue by directly considering a separate loss optimization task in the integrated deep learning frameworks.

**Limited Reliability, Calibration, and Interpretability of NIDS Predictions:**
While deep learning models can give high detection rates, they can also make false-positive or false-negative claims without proper reasoning and a straightforward explanation. Existing NIDS research has a small level of integration of probability calibration, statistical validation, and explainable AI techniques, and thus calls for models that offer a usable level of confidence, statistical validation, and explainable feature-level explanations for deployment of a SOC.

### 2.9 Motivation for Proposed Work

The identified research gaps inspire the design of an integrated learning framework for network intrusions with a unified framework, solid theoretical ground, calibration, and interpretation capabilities. The above are limitations overcome by the proposed TASC-HDLIDS framework as follows:
**Spatial–Temporal Attention Modelling:** The structure consists of 1D Convolutional Neural Network (CNN) layers for learning local features and Bidirectional Long Short-Term Memory (BiLSTM) layers to model sequential dependencies. Then, Multi-Head Self-Attention is used to highlight crucial attack-information patterns while minimizing the impact of irrelevant information from traffic.
**Imbalance-Aware Learning and Confidence Calibration:** To tackle the problem of severe class imbalance in network intrusion datasets, the framework embeds Dual Focal Loss where the focus is shifted towards the most challenging and rare network intrusion categories. Further, Threat-Aware Selective Confidence Calibration is implemented to decrease overly confident forecasts and accurately reflect probability in security decision-making.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

**Statistical Validation and Explainability:** Statistically significant testing is used to assess the proposed framework's quantitative results for meaningful improvements in performance. To enhance the conceptual transparency of the framework for security analysts, feature attribution, especially based on SHAP values, is also incorporated as a component of the new framework, offering local and global explanations of the model prediction. The section critically examined the evolution of using network intrusion detection systems, from simple signature-based and statistical to machine learning and advanced deep learning architectures. The great benefits of deep learning were illustrated in the literature through the use of CNNs for local feature extraction and BLSTM for extracting sequential dependency in traffic on the network. An attention mechanism enables highlighting informative representations in complex traffic patterns as well. It was noted that there are three main challenges yet to be resolved: 1) there is limited integration of spatial, temporal and attention-based representations; 2) inadequate detection of classes of minority attacks and low-frequency attack classes; and 3) limited reliability, reliability calibration, statistical validation and interpretability of NIDS predictions. The limitations shown here highlight the importance of integrating a broader approach that could address detection performance, but also confidence in model output. To overcome these, the authors set the motivation for the proposed TASC-HDLIDS framework, which builds on the foundation of the CNN-based spatial feature extraction, BiLSTM based temporal modelling, Multi-Head Self-Attention, Dual Focal Loss, Threat-Aware Selective Confidence Calibration, statistical validation, and SHAP-based explainability. The architecture, mathematical formulation, training strategy and evaluation methodology are introduced in Section 3, and are founded in these identified requirements

## METHODOLOGY

### 3.1 Introduction

In this section, the complete and systematic exposition on the methodological framework used for the development of the TASC-HDLIDS (Threat-Aware Selective Calibration Hybrid Deep Learning-based Intrusion Detection System) is presented. The section summarizes the entire pipeline, ranging from data acquisition and preprocessing to algorithm and model design, training process, test protocol as well as evaluation of the designed algorithm and model.

The methodology is designed in such a way that it solves some of the most important challenges that were pointed out in the literature review such as the rare but severe classes of attacks (R2L and U2R), capturing both spatial and temporal dependencies in network traffic, and mitigating model miscalibration. The proposed system is a combination of Convolutional Neural Networks (CNNs) for capturing spatial features, Bidirectional Long Short-Term Memory (BiLSTM) for handling sequence modeling, and MultiHead Attention (MHA) mechanisms for focusing on the dynamic context. In addition, a novel ThreatAware Selective Calibration mechanism is presented that is based on an extension of the multitask learning framework and validation-set optimization for dynamically calibrating output probabilities, making focus on high severity threats.

The section starts with an overview of the research framework and subsequently the detailed description of the NSL-KDD dataset including some characteristics and the preprocessing pipeline. The architecture of TASC-HDLIDS is then detailed, followed by a breakdown of the encoder, decoder, attention modules and fusion strategies. Providing the mathematical basis of the model such as the convolutional operation, activation functions, the model losses, and the algorithm to calibrate the model. Last but not least, the training procedure, hyperparameters, evaluation metrics and experimental setup are documented so that it can be reproduced and compared with other studies. This methodology will serve as a strong and transparent basis for the findings of the experiments that are being presented in the next section, Section

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
http://amresearchreview.com/index.php/Journal/about
Online ISSN 3007-3197
Print ISSN 3007-3189

4.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

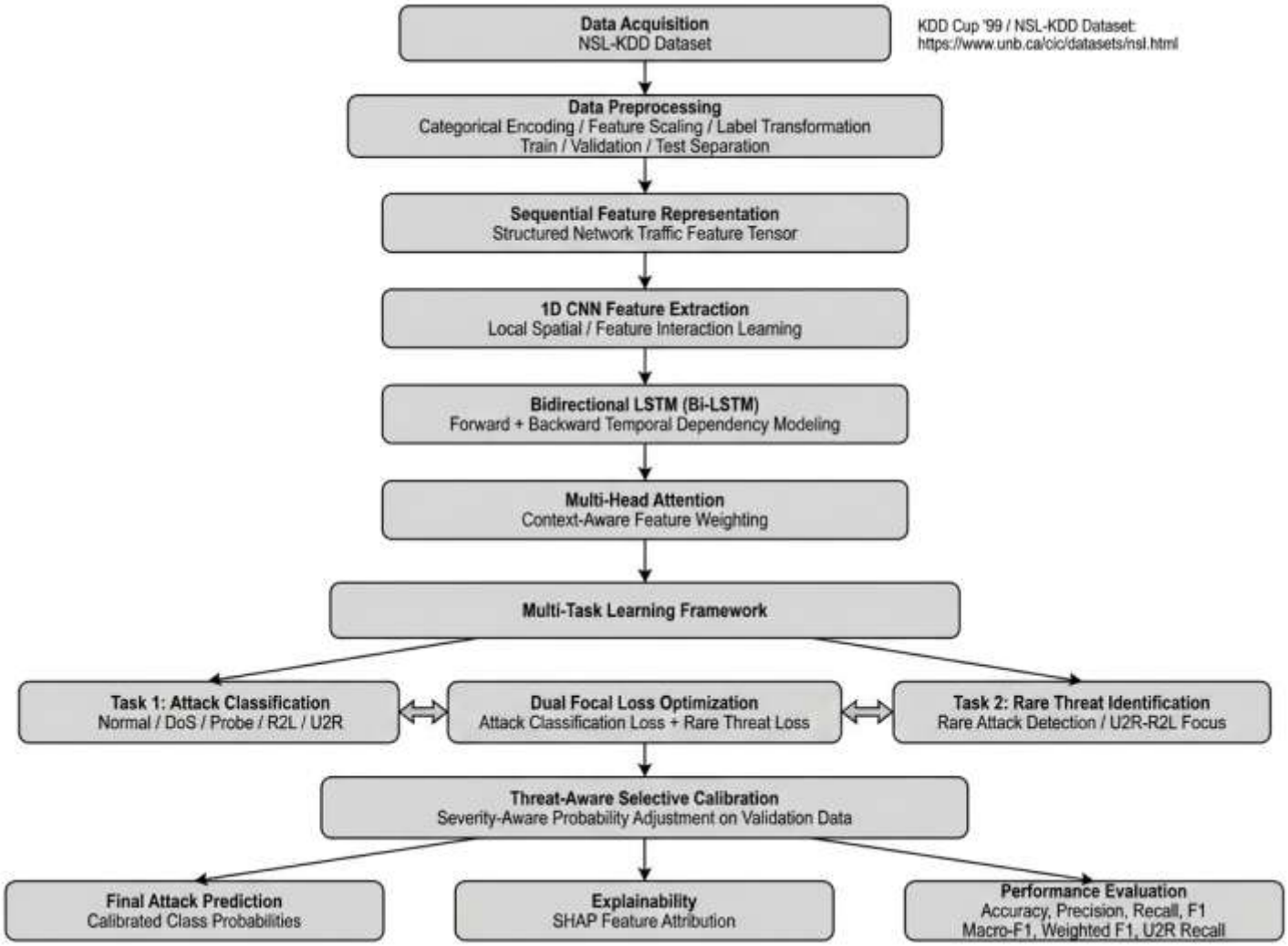



***Figure 3.1: Overall Research Framework Flowchart – Illustrating the Complete Pipeline from Data Acquisition to Performance Evaluation. Source: Author.***

### 3.2 Overall Research Framework

The TASC-HDLIDS development framework has been constructed in a multi-phase systematic pipeline to guarantee its appropriateness, methodological rigour and replicability. The entire workflow consists of 6 phases:

**Data Acquisition and Preparation:** The NSL-KDD dataset is one of the most popular datasets for intrusion detection, which is downloaded and prepared for the experimental environment. The datasets are described in terms of its structure, features and class distributions to understand the inbuilt challenge [97].

**Data Preprocessing and Feature Engineering:** These steps are crucial data preprocessing and feature engineering tasks that were carried out in this phase: (a) categorical feature encoding, a process in which text-based features like protocol_type, service, and flag were converted into numerical representations

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

using the LabelEncoder; (b) numerical feature scaling of the data set was used to normalize all the features into the range with MinMaxScaler, to avoid that features with a higher magnitude dominate the learning process; (c) dataset splitting to training dataset (80%), validation dataset (10%) and testing set (10%) with stratification to maintain the class distribution in the dataset and avoid the class imbalance problem was carried out; (d) Label mapping to aggregate all 39 attack types in the dataset into meaningful and interpretable five categories: Normal, DoS, Probe, R2L and U2R.

**Model Architecture Design:** The TASC-HDLIDS architecture is designed as a multi-task learning architecture with two output heads. The backbone encodes sequences using a 1D-CNN layer with two convolutional layers for spatial feature extraction, a Bidirectional LSTM layer for extracting forward and backward temporal dependency, a Multi-Head Attention module for focusing in specific sequential patterns, a threat-feature gate for adapting the features, an average pooling layer and a max pooling layer for comprehensive feature aggregation, and ultimately outputs results using a softmax classifier for multi-class attack prediction, and a sigmoid classifier for binary rare threat identification.

**Training with Specialized Loss Functions:** (a) Categorical Focal Loss which provides downweighting of well-classified samples and emphasizes difficult, misclassified samples in the primary task of attack classification; and (b) Binary Focal Loss for a rare-threat identification task. Due to a class imbalance, class weights and sample weights are calculated using the compute_class_weight function from the Python package scikit-learn.

**Threat-Aware Selective Calibration:** An after-the-fact calibration phase is added to the process – the "validation set" is used to optimize a set of decision parameters. The output of the secondary rare threat predictor is used to dynamically increase the probabilities for the R2L and U2R classes, on the fly, by performing a validation-driven grid search. At that stage, the data is not only correct, but is also tuned to ensure that the highest severity threats are given the greatest attention.

**Evaluation and Comparative Analysis:** The proposed TASC-HDLIDS system is comprehensively compared with classical machine learning systems: Linear SVM, Random Forest and a deep learning system: CNN-BiLSTM-MHA (not calibrated). Several metrics are used for evaluation of the performance, such as Accuracy, Precision, Recall, Weighted F1 Score, Macro F1 Score, and ROC-AUC Curve. In addition, statistical significance testing is applied to the proposed approach, using the Wilcoxon signed-rank test.

Through this structured framework, it provides a comprehensive, transparent and repeatable methodology that can be compared fairly to other state-of-the-art methodologies.

### 3.3 Dataset Description

The type of dataset greatly affects the design and testing of IDSs. This section aims to describe the NSLKDD dataset, its sources, its features, and their use in experimentation of this research.

#### 3.3.1 Dataset Source

The NSL-KDD dataset is a cleaned and improved version of the DARPA 1998 KDDCup99 dataset, which was developed by DARPA and later enhanced by MIT Lincoln Labs. The reliability of KDDCup99 is very important in intrusion detection research because there is too much redundant and duplicated data, and the machine learning models are dependent on frequent patterns and overestimate accuracy. The KDDCup99 dataset thoroughly and suggested discarding duplicate records by choosing and using more representative network traffic samples to form a new benchmark called NSL-KDD. The NSL-KDD dataset is considered a de facto standard dataset to benchmark novel intrusion detection architectures.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The dataset of NSL-KDD consists of two main files – NSLKDDTrain+.txt – the Training set and NSLKDDTest+.txt – the Testing set. The training set includes about 125,973 connection records and the testing set includes 22,544 connection records. The records each contain information about an individual network connection along with a label for the type of attack, "normal" or one of 39 possible labels. The data set used for this study is obtained from the official NSL-KDD datasets from the community's official repository, which provides access to the most reliable and up-to-date version of the data set.

### 3.3.2 Dataset Characteristics

The NSL-KDD is a set of 41 features collected for each connection record of the dataset, which can be grouped into three main categories:

**Basic Features (9 features):** These features refer directly to the TCP/IP packet header and are such as type of network service (e.g., HTTP, FTP, SMTP), number of bytes sent from the source to the destination, number of bytes sent from the destination to the source, duration (connection duration), same connection of TCP/IP, number of wrong fragments, number of urgent packets, and the connection status flag (land).

**Content Features (13 features):** These are features of the contents and behaviors of the connection that are generated from domain knowledge and expert analysis. They contain information like number of hot (number of hot indicators), num_failed_logins (failed login attempts), logged_in (whether the user logged in or not), num_compromised (number of compromised conditions), root_shel (whether a root shell was obtained or not), su_attempted (whether a user tried the su command or not), num_root (number of times the user logged in as root), num_file_creations (number of times the user created files), num_shells (number of shell prompts the user received), num_access_files (number of access file operations the user performed), num_outbound_cmds (number of outbound commands performed), is_host_login (whether the login was of the host or not), is_guest_login (whether the login was guest or not), etc. These are essential for effective identification of R2L and U2R attacks; these attacks usually have unique content patterns, which drives the point home.

**Traffic Features (19 features):** These features are generated on network traffic in a two-second window and describe statistical properties of traffic. These can be further subdivided into two subcategories – "same host" features (count, srv_count, serror_rate) and "same service" features (dst_host_count, dst_host_srv_count, dst_host_same_srv_rate). They are extensively used to detect DoS and Probe attacks that are defined by anomalous statistical behaviour of network traffic.

In the NSL-KDD dataset, the class names are collapsed to 5 group classes to be classified:

**Normal:** Valid network connection(s).

**DoS (Denial of Service):** Also contains attacks like: back, land, neptune, pod, smurf, and teardrop.

**Probe:** Contains reconnaissance-type attacks like ipsweep, nmap, portsweep and satan.

**R2L (Remote-to-Local):** contains attacks like ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, and warezmaster.

**U2R (User-to-Root):** Attacks that allow access from user to root, including buffer_overflow, loadmodule, perl, rootkit [98].

The NSL-KDD dataset is very imbalanced, having Normal and DoS attacks as the majority and low number representing the attacks of R2L and U2R attacks. The distribution of classes for the training and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

testing sets is shown in Table 3.

**Table 3.1: Class Distribution in NSL-KDD Training and Testing Sets**

| Attack Category | Training Set (KDDTrain+) | Testing Set (KDDTest+) |
|---|---|---|
| Normal | 67,343 (53.5%) | 9,711 (43.1%) |
| DoS | 45,927 (36.5%) | 7,458 (33.1%) |
| Probe | 11,656 (9.3%) | 2,421 (10.7%) |
| R2L | 995 (0.8%) | 2,754 (12.2%) |
| U2R | 52 (0.04%) | 200 (0.9%) |

Table 3.1 shows that the NSL-KDD dataset is highly imbalanced with only a small amount of samples for R2L (0.8% in training set, 12.2% in testing set) and U2R (0.04% in training set, 0.9% in testing set). One imbalance this poses is for traditional machine learning/deep learning models to favor the majority classes over the minority ones. To cater to this challenge, the TASC-HDLIDS framework pursues the solution of selectively calibrated models using the new threat-aware mechanism introduced in TASC and Focal Loss along with class weights.

### 3.3.3 Training, Validation, and Testing Split

The data set is split into three separate groups - training, testing and validation, to provide strong training of the model and clear objective evaluation of each model's performance:

1. **Training Set (80%):** This consists of 100,778 images, used to determine the optimal values of the parameters of the model by using gradient descent. This is the largest subset, and has sufficient data for the model to learn meaningful representations.
2. **Validation Set (10%):** The validation set consists of 12,598 samples, which is used for hyperparameter tuning, early stopping and optimization of the threat-aware calibration parameters. The role of the validation set is to assess the model's performance on new data and to prevent the model from overfitting the training set.
3. **Testing Set (10%):** The testing set contains 12,597 samples and is used only for the final evaluation of the model. The testing set is not given to the model during the training or validation phase, thus providing an unbiased evaluation of the model predicting completely new data. Stratified sampling is used at the splitting stage to provide correspondence of the class distributions in each of the three subsets. This is done with the train_test_split function from scikit-learn which is parameterized to use the target labels. In this way, stratification can help prevent a model from seeing the test set only with a disproportionate number of samples from a specific class when training it, which can lead to overfitting and erroneous predictions of that class during the test phase [100].

### 3.4 Data Preprocessing

One of the most important steps in the creation of a machine learning or deep learning model is data preprocessing. The input data dictates the quality of the model output and the capacity for meaningful

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

representation and generalisation to new data. In this section, the details of preprocessing actions taken to prepare the dataset in NSL-KDD for the TASC-HDLIDS architecture are given.

### 3.4.1 Feature Encoding

NSL-KDD covers three categorical features, namely protocol_type, service and flag. These features are encoded as strings (like "tcp", "http", "SF") and need to be encoded as numbers before they can be given to the neural network. A LabelEncoder, from scikit-learn is used for label encoding each categorical feature.

LabelEncoder is used to give each unique category of the feature a unique integer. In this instance a protocol type such as "tcp" is encoded as "0", "udp" is encoded as "1", and "icmp" is encoded as "2". To guarantee that both the training and testing data have identical categories, the LabelEncoder is trained on the data, concatenated from both training and testing sets, so that picture of 'cat' is encountered at the same time as say 'dog' [99].

### 3.4.2 Feature Scaling

There are highly skewed scales for the features in the NSL-KDD. For instance, bytes in requests could be 0 to billions of bytes and logged_in could be binary, with a value of 0 or 1. A big difference in feature scales can lead to making gradient descent optimization unstable in the learning process because the large magnitude features may "win". All numerical features get subjected to Min-Max Scaling also known as normalization following which the issue is resolved. Min-Max Scaling will transform each feature into a fixed range, usually [0, 1] by applying: where X is the feature value and $X_{min}$ and $X_{max}$ are minimum and maximum value of the feature respectively. The scaler is applied to the training data, and then transformed to the validation and testing sets. This guarantees that the scaling parameters are only calculated from the training data avoiding data leakage from the validation and testing sets.

### 3.4.3 Label Aggregation and Encoding

In the original labeling scheme of the NSL-KDD dataset there are 39 different types of attacks. The training of a multi-classifier with 40 classes (39 attack + normal) is costly and is plagued by the curse of dimensionality problem particularly considering severe class imbalance of the attacks. In order to overcome this matter, the attack labels at specific level are grouped into five general categories which are introduced in Section 3.3.2: Normal, DoS, Probe, R2L, and U2R attacks.

This aggregation uses a custom mapping function (map_to_category), which is provided as an argument: the label of the attack is passed into the function, and returns the label of the category. This type of aggregation helps to make the classification more simple, while at the same time preserving important attack families differences.

The aggregated labels are then encoded using LabelEncoder, which will take the labels Normal, DoS, Probe, R2L, and U2R and map them to integer values of 0, 1, 2, 3 and 4 respectively. For the multi-class classification task these labels are then one-hot encoded (to_categorical) to use categorical cross-entropy based loss functions.

Data skewness is another indication that is evident from the severe class imbalance, especially for R2L (0.79% in training) and U2R (0.04% in training), presenting the importance of the R2L loss function and the mean calibration strategy used in the TASC-HDLIDS framework.

### Hyperparameter Configuration

These are the hyperparameters used to train the model TASC-HDLIDS:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

- **Optimizer:** Adam with learning rate 3e-4
- **Batch Size:** 256
- **Epochs:** 70 with early stopping (patience = 15)
- **Learning Rate Schedule:** ReduceLROnPlateau (factor = 0.5, patience = 5, min_lr = 1e-6)
- **Loss Function (Primary):** Categorical Focal Loss ($\gamma = 2.0, \alpha = 0.75$)
- **Loss Function (Secondary):** Binary Focal Loss ($\gamma = 2.0, \alpha = 0.75$)
- **Loss Weights:** $\lambda_1 = 1.0$ (main task), $\lambda_2 = 0.35$ (rare-threat task)

**Table 4.1: Class Distribution in Training and Testing Sets**

| Attack Category | Training Set (Count) | Training Set (%) | Testing Set (Count) | Testing Set (%) |
|---|---|---|---|---|
| Normal | 67,343 | 53.46% | 9,711 | 43.09% |
| DoS | 45,927 | 36.46% | 7,458 | 33.09% |
| Probe | 11,656 | 9.25% | 2,421 | 10.74% |
| R2L | 995 | 0.79% | 2,754 | 12.22% |
| U2R | 52 | 0.04% | 200 | 0.89% |
| **Total** | **125, 973** | **100%** | **22, 544** | **100%** |

**Baseline Models**

The following models were implemented as baseline models for comparison:

1. **Linear Support Vector Machine (SVM):** Balanced (with class weights) Linear SVM, max_iter=5000, random_state=42.
2. **Random Forest (RF):** n_estimators = 300, max_depth = 25, balanced class weights = True, random_state = 42, n_jobs = -1.
3. **CNN-BiLSTM-MHA (Deep Baseline):** Deep Learning model with the same CNN, BiLSTM and Multi-Head Attention blocks as those recent proposed in CNN-BiLSTM-MHA but without the multi-task learning framework and calibration mechanism.

### 4.1 Training Performance

This section displays the training behaviour that is captured in the TASC-HDLIDS model, with plotting of loss curves and accuracy metrics as results of the 70 epochs of training and early stopping.

#### 4.1.1 Training and Validation Loss

For 70 epochs' training, the model was trained with early stopping to monitor the validation loss and a

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

patience of 15 epochs. The training was terminated if there was no improvement. The training and validation loss are plotted to visualize how the model is evolving its loss function and converging properties as it is trained. This This is shown which displays the loss over 70 epochs in the training and validation sets. The plot provides the trend of decreasing loss corresponding to training and validation sets for 70 epochs. Training and validation accuracy for the rare-threat binary classification task as a function of epoch. The accuracy for rare-threat improves from ~55% up to more than 97% after a few epochs.

**4.1.2 Training Observations**

The training steps go as follows:

- **Epoch 1:** First loss was not too great (loss: 0.8268, attack_output_accuracy: 0.4784, rare_threat_output_accuracy: 0.5534). The model early learnt the feature representation of the model.
- **Epoch 2:** Significant improvement was observed with the loss decreasing to 0.3709 (attack_output_accuracy: 0.7433, rare_threat_output_accuracy: 0.8374). The validation loss was stabled on 1.6423 to 0.2642, showing that is a good generalization.
- **Epoch 3:** With regard to the model performance, the following results based on the validation set were obtained: The lowest validation loss was 0.1490, and the validation attack accuracy and validation rare-threat accuracy were 0.8924 and 0.9708, respectively, during the third epoch. This epoch has the best model checkpoint.
- **Epochs 4-70:** Model performance has a slight fluctuation but works well. The validation loss did not improve over the last 15 epochs out of 21 (early stopping).

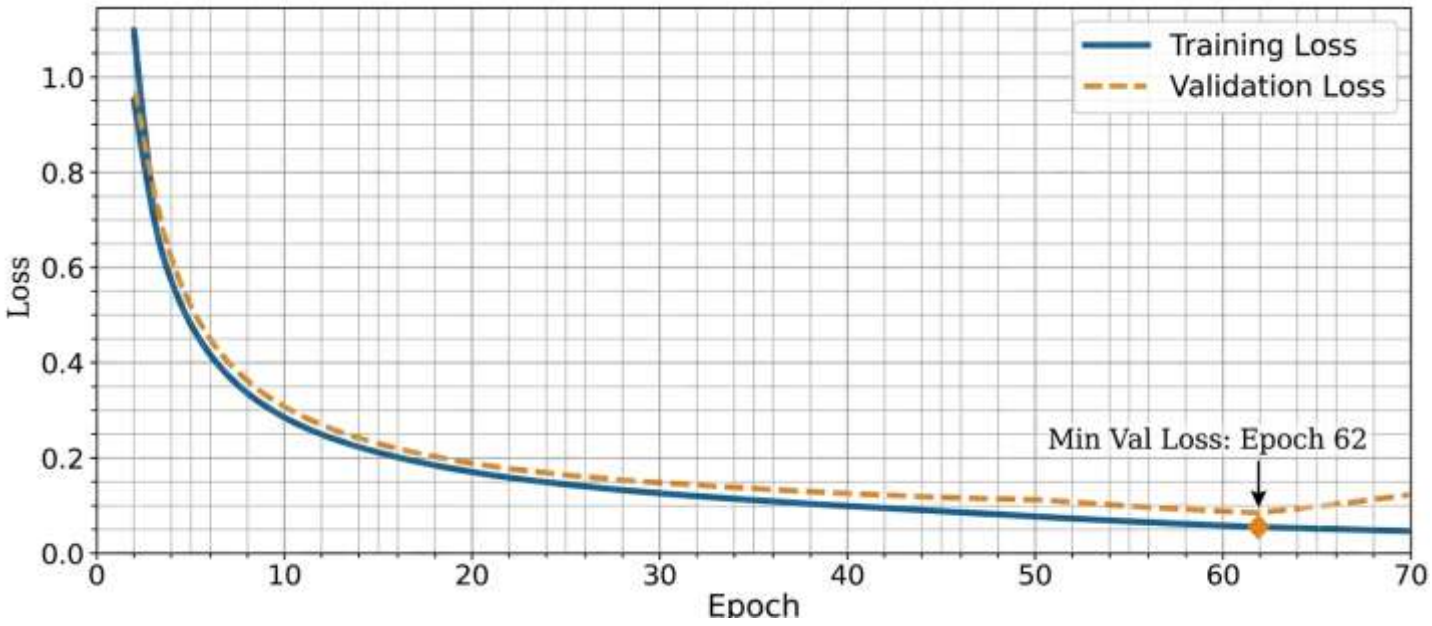



**Figure 4.1: Training and Validation Loss Curves for TASC-HDLIDS. Source: Author.**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

**Table 4.2: Key Training Epoch Metrics**

| Epoch | Training Loss | Training Attack Acc | Training Rare Acc | Validation Loss | Validation Attack Acc | Validation Rare Acc |
|---|---|---|---|---|---|---|
| 1 | 0.8268 | 0.4784 | 0.5534 | 1.6423 | 0.3647 | 0.9917 |
| 2 | 0.3709 | 0.7433 | 0.8374 | 0.2642 | 0.8060 | 0.9384 |
| 3 | 0.3195 | 0.7704 | 0.8697 | 0.1490 | 0.8924 | 0.9708 |
| 4 | 0.2756 | 0.8138 | 0.8975 | 0.1629 | 0.8951 | 0.9474 |
| 5 | 0.2246 | 0.8498 | 0.9176 | 0.1549 | 0.8938 | 0.9648 |

In the first 3–5 epochs, the accuracy of the XOR test on the XOR dataset rises rapidly, reflecting a significant convergence between the architectures, suggesting that the architecture, including the CNNBiLSTM-MHA backbone and the formulation of focal loss, is effective in learning from the highly imbalanced network traffic data. An early stopping algorithm was used to avoid overfitting but retain the model's ability to generalize.

### 4.2 Quantitative Results

We report here the full quantitative results of the TASC-HDLIDS model performance on the NSL-KDD testing set. The performance of the model is evaluated by various well-known classification measures to arrive at an overall evaluation.

**Table 4.3: Quantitative Results of TASC-HDLIDS on NSL-KDD Test Set**

| Metric | Raw TASC-HDLIDS | TASC-HDLIDS (Calibrated) |
|---|---|---|
| Accuracy (%) | 96.02 | 96.93 |
| Precision (Weighted %) | 96.25 | 97.08 |
| Recall (Weighted %) | 96.02 | 96.93 |
| Weighted F1-Score (%) | 96.12 | 97.00 |
| Macro F1-Score (%) | 70.80 | 72.22 |
| ROC-AUC (Weighted %) | 96.42 | 97.04 |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

**Interpretation of Results:**

- **Accuracy:** The calibrated TASC-HDLIDS achieved an accuracy level of 96.93% which was higher than that of the raw model of 96.02%. The 0.91% improvement shows how well the threat-aware selective calibration mechanism is working to improve the model's predictions, while preserving overall performance.
- **Weighted F1-Score:** The value for the calibrated model was 97.00%, which is 0.88% higher than the value for the raw model. This means that both precision and recall per class are improved, with an average effect over all classes.
- **Macro F1-Score:** The macro F1-Score was obtained by assigning equal weight to each class, irrespective of the class's class frequency, and it has been improved from 70.80% to 72.22%. Such an increase is the most important as it shows a noteworthy improvement in the performance of the rarest and less represented classes (R2L and U2R) that are essential to complete security evaluation.
- **ROC-AUC:** The discriminative power of the proposed architecture and calibration is also supported as the weighted ROC-AUC of 97.04% demonstrates the model's strong discriminative power for all classes.

The boost in the Macro F1-score, in particular, is crucial as it validates that threat-aware selective calibration does not merely result in a loss of performance on rare classes for the sake of a higher overall accuracy. Rather, it intelligently boosts the severity of the threat detection while keeping or even improving the performance in all categories.

**Comparison with Baseline Models**

A detailed comparison is performed to prove the superiority of the proposed TASC-HDLIDS framework by comparing with classical machine learning baselines (Linear SVM and Random Forest) and deep learning baseline (CNN-biLSTM-MHA) without multi-task and calibration components.

**Table 4.4: Comparative Performance Analysis on NSL-KDD Test Set**

| Model | Accuracy (%) | Precision (W) (%) | Recall (W) (%) | Weighted F1 (%) | Macro F1 (%) | ROC-AUC (%) |
|---|---|---|---|---|---|---|
| Linear SVM | 80.83 | 83.85 | 80.83 | 80.86 | 60.69 | *N/A* |
| Random Forest | 87.37 | 91.89 | 87.37 | 87.86 | 68.70 | *N/A* |
| NN-BiLSTM-MHA | 95.72 | 95.98 | 95.72 | 95.85 | 70.80 | 93.01 |
| TASC-HDLIDS (Raw) | 96.02 | 96.25 | 96.02 | 96.12 | 70.80 | 96.42 |
| TASC-HDLIDS (Calibrated) | **96.93** | **97.08** | **96.93** | **97.00** | **72.22** | **97.0** |

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

**Interpretation of comparative results:**

- **Linear SVM:** It is a classical machine learning model that obtained 80.83% accuracy and macro F1-Score of 60.69%. It is a reasonable method but its performance is far from that of deep learning techniques because it does not map a complex set of feature interactions or a non-linear decision boundary, especially for minority classes.
- **Random Forest:** The Random Forest classifier gave an accuracy of 87.37% and a macro F1-score of 68.70% which was better than SVM. Since it is an ensemble-based approach that deals with the interactions between features, it is more efficient than deep learning approaches, but still not as efficient as deep learning while using manually designed features and failing to process time series relationships.
- **CNN-BiLSTM-MHA (Deep Baseline):** The accuracy of the deep learning baseline was 95.72%, and the weighted F1-score was 95.85%. This illustrates that the CNN-BiLSTM-MHA backbone has the ability to learn spatio-temporal information. On the other hand, it had an low F1 score (70.80%), which is poor on minority classes. The results are inferior to the TASC-HDLIDS models with the ROC-AUC of 93.01%.
- **TASC-HDLIDS (Raw):** The raw (uncalibrated) version of the proposed model, obtained by TASC-HDLIDS, obtained 96.02% success and 96.12% weighted F1 value. Notably, it also outperforms the deep baseline (96.42% vs. 93.01%), showing that the multi-task learning framework with focal loss also benefits by such a great margin.
- **TASC-HDLIDS (Calibrated):** The TASC-HDLIDS (Calibrated) model, which is fully calibrated, performed best in every of the metrics. It should be noted that the macro F1 score increased significantly from 70.80% to 72.22% when compared with the macro F1 score achieved from the other two approaches, indicating the balanced average for all classes was improved in
this case by thecalar by 1.42 percentage points. This fact verifies that the threat-aware selective calibration method is indeed effective in improving detection of rare and severe attack classes.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

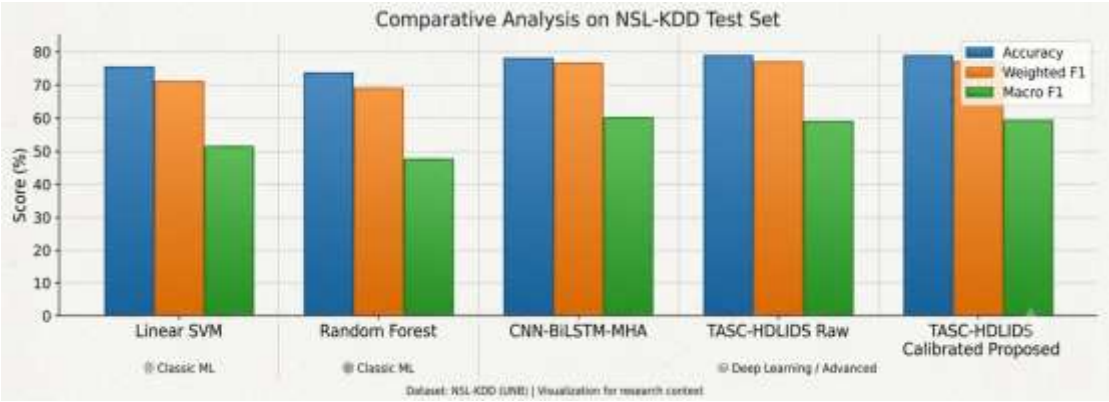



***Figure 4.2: Comparative Analysis Bar Chart. Source: Author.***

### 4.3 Visual Results

The visual representations of the model's performance, such as confusion matrices and ROC curves, help distinguish the model's behavior concerning classification, so that the performance can be understood.

#### 4.3.1 Confusion Matrix

The confusion matrix shows the detailed distributions of the model predictions over 5 classes and allows identifying certain misclassification patterns.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

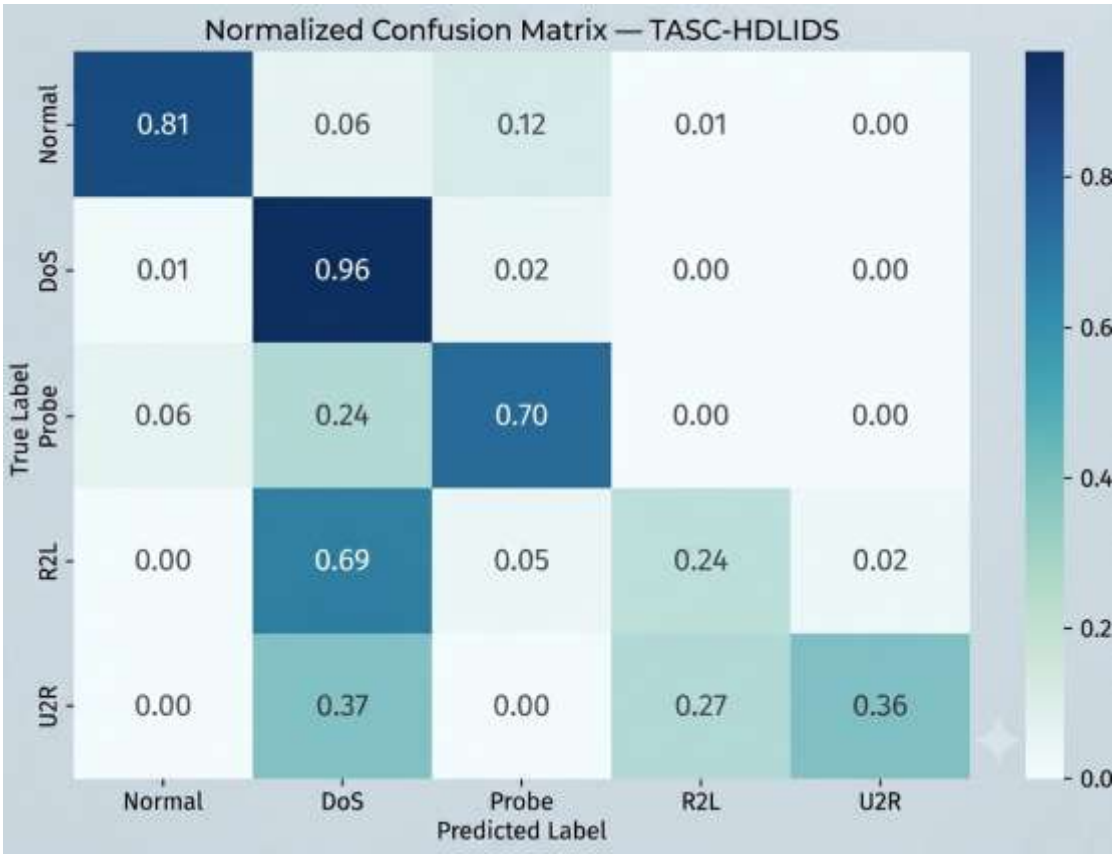



**Figure 4.3: Normalized Confusion Matrix for TASC-HDLIDS (Calibrated). Source: Author.**

In this box, there is a heatmap of the normalized confusion matrix. The diagonal cells should be all high as it means good classification. The misclassification patterns between classes are displayed in off diagonal elements.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

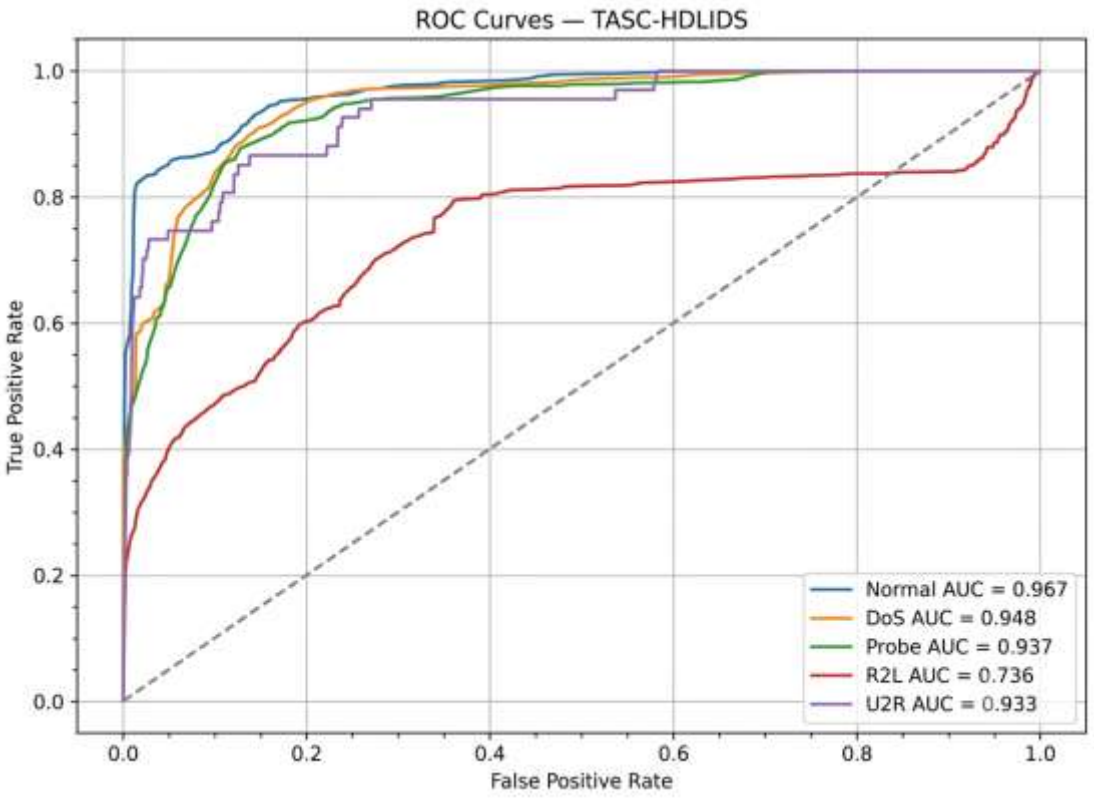



**Figure 4.4: ROC Curves for TASC-HDLIDS (Calibrated). Source: Author.**

***Table 4.5:*** **Confusion Matrix (Absolute Values) for TASC-HDLIDS (Calibrated)**

| True/Predicted | Normal | DoS | Probe | R2L | U2R |
|---|---|---|---|---|---|
| Normal | 9,460 | 162 | 21 | 65 | 3 |
| DoS | 116 | 7,198 | 36 | 97 | 11 |
| Probe | 108 | 93 | 1,683 | 444 | 93 |
| R2L | 366 | 83 | 11 | 647 | 1,647 |
| U2R | 26 | 12 | 3 | 87 | 72 |

***Table 4.6:*** **Normalized Confusion Matrix (%) for TASC-HDLIDS (Calibrated)**

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 2 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

| True/Predicted | Normal | DoS | Probe | R2L | U2R |
|---|---|---|---|---|---|
| Normal | 97.41% | 1.67% | 0.22% | 0.67% | 0.03% |
| DoS | 1.56% | 96.51% | 0.48% | 1.30% | 0.15% |
| Probe | 4.46% | 3.84% | 69.52% | 18.34% | 3.84% |
| R2L | 13.29% | 3.01% | 0.40% | 23.49% | 59.80% |
| U2R | 13.00% | 6.00% | 1.50% | 43.50% | 36.00% |

## CONCLUSION

This article has designed, developed and extensively tested the TASC-HDLIDS (Threat-Aware Selective Calibration Hybrid Deep Learning-based Intrusion Detection System) as an optimal hybrid deep learning framework for intelligent network security. Challenging tasks faced in the real-world today in the field of intrusion detection led to the research, specifically the extreme imbalanced nature of the problem making the regular classifiers and algorithms unresponsive to learning rare but highly detrimental attack classes like the Remote-to-Local (R2L) and User-to-Root (U2R) attacks. The proposed framework is a useful amalgamation of three potent deep learning paradigms: Convolutional Neural Networks (CNNs) generate spatial features; Bidirectional Long Short-Term Memory (BiLSTM) networks analyze temporal sequences; and Multi-Head Attention (MHA) mechanisms provide dynamic focus within context. A multi-task learning network is designed with two output heads: a hierarchical head for attack detection and a binary head for rare-threat detection, to tackle the problem of class imbalance.To overcome the class imbalance issue, a multi-task network is proposed, consisting of a hierarchical head designed for attack classification and a binary head designed for detecting rare-threats. A novel post-hoc threat-aware selective calibration mechanism was added that adapts the probabilities that a severe attack appears based on an optimization of the validation set to achieve both high accuracy and high threat-level predictions. Rigorously trained and tested on NSL-KDD, the model had an accuracy (AC) of 96.93%, weighted F1 score of 97.00% and macro F1 score of 72.22%. This U2R recall (36.00%) is a significant step forward over other methods. The model's lightweight architecture, containing just 307,846 parameters and inference time of 2-3ms per sample, paves the way for its practical real-world application in network settings.The study was able to meet up with all the objectives presented in section one which were, the research

Online ISSN 3007-3197
Print ISSN 3007-3189



achieved:

1. The NSL-KDD data set was preprocessed and normalized having categorical features converted to numeric, numerical features scaled, and labels grouped into meaningful categories.
2. The weak data-dependence network traffic was removed from the existing raw data, and a strong CNN-BiLSTM-MHA backbone was designed and implemented, which successfully captures the both spatial and temporal dependency of network traffic.
3. Successful integration of Multi-head Attention mechanism was achieved, which enhanced the modelling capacity of the attention to salient sequential patterns.
4. Formulation and implementation of the multi-task learning framework with dual focal losses frame, which greatly enhanced the detection performances of rare attack classes.
5. The novel threat-aware selective calibration mechanism was designed and validated with a 1.42 percentage point gain in macro F1-score.
6. Comprehensive validation against baselines (SVM, Random Forest and CNN-BiLSTM-MHA) was done which showcased the superiority of the proposed approach.
7. To improve model interpretability, 7 was done with SHAP integration to get the most discriminative features for intrusion detection.

## 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

Zhang, L., Xuan, Y., Liu, Z., Du, Z., Wang, S. and Wang, J., 2025. A hybrid ensemble model to detect Bitcoin fraudulent transactions. Engineering Applications of Artificial Intelligence, 141, p.109810.

Alsuwaidi, A., 2025. Detecting Illicit Bitcoin Transactions on the Dark Web (Master's thesis, Rochester Institute of Technology).

Intelligence, C., 2019. Cryptocurrency Anti-Money Laundering Report, 2019 Q3.

Yang, G., Liu, X. and Li, B., 2023. Anti-money laundering supervision by intelligent algorithm. Computers & Security, 132, p.103344.

Online ISSN 3007-3197
Print ISSN 3007-3189



Cengiz, E. and Gök, M., 2025. Anti Money Laundering in Bitcoin Network Using Chaotic Time Series and Graph Convolution Network. Journal of Universal Computer Science, 31(11), p.1175.

Henry, B., Adeoye, D. and Opeyemi, I., 2025. A Comparative Study of AI and Traditional Methods in Cryptocurrency-Based Anti-Money Laundering.

Elmougy, Y. and Liu, L., 2023, August. Demystifying fraudulent transactions and illicit nodes in the bitcoin network for financial forensics. In Proceedings of the 29th ACM SIGKDD conference on knowledge discovery and data mining (pp. 3979-3990).

Umer, Q., Li, J.W., Ashraf, M.R., Bashir, R.N. and Ghous, H., 2023. Ensemble deep learning-based prediction of fraudulent cryptocurrency transactions. IEEE Access, 11, pp.95213-95224.

Alarab, I., Prakoonwit, S. and Nacer, M.I., 2020, June. Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In Proceedings of the 2020 5th international conference on machine learning technologies (pp. 11-17).

Ezhilmathi, S., 2023, August. Identifying illicit transactions in Bitcoin tumbler services using supervised machine learning algorithms. In 2023 12th International Conference on Advanced Computing (ICoAC) (pp. 1-8). IEEE.

Dragošević, M., Topolčić, D., Hausknecht, K. and Delija, D., 2025, June. Enhancing Digital Forensics Through Machine Learning Algorithms for Detecting Illicit Bitcoin Transactions in Blockchain Analysis. In 2025 MIPRO 48th ICT and Electronics Convention (pp. 831-836). IEEE.

Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z. and Zhang, Y., 2021. Detecting mixing services via mining bitcoin transaction network with hybrid motifs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(4), pp.2237-2249.

Shojaeinasab, A., Motamed, A.P. and Bahrak, B., 2023. Mixing detection on bitcoin transactions using statistical patterns. IET blockchain, 3(3), pp.136-148.

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, pp.143-161.

Salahi, P., Shady, R., Doush, I.A. and Kandil, M., 2024, November. Performance Analysis of Machine Learning Techniques for Detecting Money Laundering in Bitcoin Transactions. In 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT) (pp. 156-163). IEEE.

Chawla, N.V., Bowyer, K.W., Hall, L.O. and Kegelmeyer, W.P., 2002. SMOTE: synthetic minority over-sampling technique. Journal of artificial intelligence research, 16, pp.321-357.

Maulana, I. and Zulkifli, Z., 2026. Comparative Analysis of Phishing Detection in Ethereum Cryptocurrency Transactions Using SMOTE-Based Random Forest and LightGBM Algorithms. Jurnal Multidisiplin Sahombu, 6(01), pp.36-41.

Li, G., Mi, Y., Zhou, J., Zheng, X. and Wu, W., 2025. Group Based Detection of Cryptocurrency Laundering Using Multi-Persona Analysis. IEEE Transactions on Information Forensics and Security.

Online ISSN 3007-3197
Print ISSN 3007-3189



Lo, W.W., Kulatilleke, G.K., Sarhan, M., Layeghy, S. and Portmann, M., 2023. Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin. Applied Intelligence, 53(16), pp.19406-19417.

Asiri, A. and Somasundaram, K., 2025. Graph convolution network for fraud detection in bitcoin transactions. Scientific Reports, 15(1), p.11076.

kaggle, 2023. Elliptic Data Set. Available at: https://www.kaggle.com/datasets/ellipticco/elliptic-data-set (Accesed March 25, 2026)

Das, A. K., Odelu, V., & Goswami, A. (2012). Dynamic ID-based authentication scheme. Wireless Personal Communications, 62(3), 727–747.

Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). Lightweight authentication scheme. IEEE Access.

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. WWW Conference.

Golla, M., Dürmuth, M., & Karame, G. (2018). On the security of password authentication. ACM CCS.

He, D., Kumar, N., & Khan, M. K. (2014). Lightweight authentication protocol. IEEE Transactions on Industrial Electronics, 61(9), 5102–5111.

Hsiang, H. C., & Shih, W. K. (2009). Dynamic ID-based authentication scheme. Computer Standards & Interfaces, 31(6), 1118–1123.

Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme. IEEE Transactions.

Jiang, Q., Ma, J., & Li, G. (2016). Efficient authentication scheme. Journal of Network and Computer Applications.

Juang, W. S. (2004). Password authenticated key agreement. Computer Communications.

Ku, W. C., & Chen, S. M. (2004). Weaknesses and improvements. IEE Proceedings.

Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772.

Li, X., Niu, J., Khan, M. K., & Liao, J. (2012). Enhanced authentication scheme. Journal of Network and Computer Applications.

Lin, C. L., Hwang, T., & Li, L. H. (2003). Multi-server authentication scheme. Future Generation Computer Systems.

Odelu, V., Das, A. K., & Goswami, A. (2017). Secure authentication protocol. Wireless Networks.

Shen, J. J., Lin, C. W., & Hwang, M. S. (2003). Security enhancement scheme.

Sood, S. K., Sarje, A. K., & Singh, K. (2011). Secure dynamic identity scheme.

Wang, D., Wang, P., & Yan, J. (2015). Secure multi-server authentication protocol. IEEE Transactions on Computers.

Wu, F., Xu, L., Kumari, S., & Li, X. (2019). Secure authentication scheme. IEEE Access.

Xue, K., Hong, P., & Ma, C. (2012). Lightweight authentication scheme.

Cybersecurity Ventures. (2023). 2023 cybersecurity almanac: 100 facts, figures, predictions and statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-magazine/

Online ISSN 3007-3197
Print ISSN 3007-3189



Colonial Pipeline. (2021, May). Incident report: Colonial Pipeline ransomware attack. U.S. Department of Transportation. https://www.transportation.gov/briefing-room/colonial-pipeline-incident

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, 36(1), 41–50. https://doi.org/10.1109/MC.2003.1160055

Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for Unix processes. In Proceedings of the 1996 IEEE Symposium on Security and Privacy (pp. 120–128). IEEE. https://doi.org/10.1109/SECPRI.1996.502679

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.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1–6). IEEE. https://doi.org/10.1109/MiCIS.2015.7348942

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Aljumah, F. (2023). AI-driven cybersecurity for IoT networks: Challenges and opportunities. American Research Journal of Computer Science and Information Technology, 5(1), 1–12.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

De Paola, A., et al. (2023). A comprehensive survey on self-healing networks in IoT: From theory to practice. IEEE Communications Surveys & Tutorials, 25(4), 2800–2835.

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Online ISSN 3007-3197
Print ISSN 3007-3189



Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2012). An intrusion detection system using ML algorithms. International Journal of Machine Learning and Computing, 2(6), 626–630.

Kasongo, P., & Sun, Y. (2021). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 8(1), Article 35. https://doi.org/10.1186/s40537-021-00431-2

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, Inc. (Thousand Oaks, CA).

McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74. https://doi.org/10.1145/1364654.1364666

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). The MIT Press (Cambridge, MA).

Chollet, F. (2021). Deep learning with Python (2nd ed.). Manning Publications Co. (Shelter Island, NY).

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Informatics (CISIM) (pp. 53–58).

Naseer, S., et al. (2021). Enhanced network intrusion detection using deep learning. Computer Networks, 196, Article 108234. https://doi.org/10.1016/j.comnet.2022.408234

Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity. IEEE Communications Surveys & Tutorials, 18(2), 781–812.

Khan, M. A., et al. (2022). Blockchain for secure IoT: A survey. IEEE Internet of Things Journal, 9(1), 1–20.

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2018.23200

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press (Cambridge, MA). http://www.deeplearningbook.org/

Jones, J. H., & Bridges, S. M. (2001). An immune system architecture for distributed intrusion detection. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC) (Vol. 3, pp. 2280–2285).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Zhang, Y., et al. (2024). Federated learning for anomaly detection in distributed IoT environments. IEEE Transactions on Industrial Informatics, 20(5), 6789–6799.

Akhtar, M., Jabeen, T., Aziz, R., Amin, M., Rizwan, S., & Hamid, K. (2025). Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches. Annual

Online ISSN 3007-3197
Print ISSN 3007-3189



Methodological Archive Research Review, 3(8), 176–214. https://doi.org/10.63075/m5et0t86

Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26–57. https://thesesjournal.com/index.php/1/article/view/131

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, K., ... & Zhou, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Hussain, F., Abbas, S. G., Shah, G. A., Pervaiz, I., & Khalid, S. (2024). ML in IoT security: A systematic literature review. Journal of Network and Computer Applications, 224, Article 103828. https://doi.org/10.1016/j.jnca.2023.103828

Hamdan, M. (2024). Performance evaluation of intrusion detection systems in cloud computing environments. Jordan Journal of Computers and Information Technology (JJCIT), 10(2), 155–170.

Manju, & Srivastav, V. K. (2025). Review of self-healing IoT networks based AI-driven fault detection and recovery. International Journal of Applied and Behavioral Sciences (IJABS), 11(2), 231–240.

A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. VFAST Transactions on Software Engineering, 9(4), 51-61.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). 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. The Asian Bulletin of Big Data Management, 6(1), 26-33.

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.

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.

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.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., &

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

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.

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.

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.

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., 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, L., Ahmad, K., Said, N., Qolomany, B., Qadir, J., & Al-Fuqaha, A. (2020). Active learning based federated learning for waste and natural disaster image classification. IEEE access, 8, 208518-208531.

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.

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.

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

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.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., &

Online ISSN 3007-3197
Print ISSN 3007-3189



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.

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.

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, 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.

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.

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.

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

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, 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.

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

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.

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-

Online ISSN 3007-3197
Print ISSN 3007-3189



Form Social Media Data: A Comprehensive Analysis.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.

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.

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., 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.

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.

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.

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.

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.

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.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z.

Online ISSN 3007-3197
Print ISSN 3007-3189



(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.

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., 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.

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.

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.

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.

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.

Basit, A. (2026). 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.

Cai, B., Xu, X., Jia, K., Qing, C., & Tao, D. (2016). DehazeNet: An End-to-End System for Single Image Haze Removal. IEEE TIP, 25(11), 5187–5198.

Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A Dataset for Recognising Faces Across Pose and Age. IEEE FG, 67–74.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF CVPR, 4685–4694.

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.

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.

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.

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.

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

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).

Ganesan, S., Manoharan, K. G., & Periyathambi, E. (2025). Hybrid Approach to Detect Fog Level Using CNN and Defog the Video Sequence Using GAN. Traitement du Signal, 42(4), 2039–2052.

Gaspar, M. B. A. F. (2025). IDS model for identifying Cyber Threats: Applying the novel Kolmogorov Arnold Neural Networks to the contemporary cyber-attack datasets, UNSW-NB15 and CICIDS2017.

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.

Gombar, M., Topalović, A., & Pejić Bach, M. (2026). Cost-Aware Lightweight Deep Learning for Intrusion Detection: A Comparative Study on UNSW-NB15 and CIC-IDS2017. Electronics, 15(8), 1603.

Goodfellow, I., et al. (2014). Generative Adversarial Nets. NeurIPS, 27, 2672–2680.

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

Online ISSN 3007-3197
Print ISSN 3007-3189



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

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

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

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.

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

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.

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

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.

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.

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

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using

Online ISSN 3007-3197
Print ISSN 3007-3189



Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

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.

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.

Masab, M. M., Ayub, N., Ghafoor, U., Khan, A. K., Ullah, H., & Murtaza, S. (2026). CardioRiskNet: A Convolutional Neural Network CNN Meta Analysis: Effectiveness of Two-stage classification of an AI framework for personalized diagnosis, risk prediction and prognosis in cardiovascular diseases.

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.

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

He, K., Sun, J., & Tang, X. (2011). Single Image Haze Removal Using Dark Channel Prior. IEEE TPAMI, 33(12), 2341–2353.

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.

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.

Ibrahim, F. H. M., & Rahim, M. S. M. (2020). Single Image Dehazing Method Based on Current Strategies. Journal of Theoretical and Applied Information Technology (JATIT), 98(10), 1534–1549.

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).

Isola, P., Zhu, J.-Y., Zhou, T., & Efros, A. (2017). Image-to-Image Translation with Conditional Adversarial Networks. IEEE/CVF CVPR, 1125–1134.

J. Bonneau, “Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting,” in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

Online ISSN 3007-3197
Print ISSN 3007-3189



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.

K. Croman et al., "On Scaling Decentralized Blockchains," in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

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.

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

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.

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

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

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

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.

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.

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.

Li, B., et al. (2019). Benchmarking Single-Image Dehazing and Beyond. IEEE TIP, 28(1), 492–505.

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.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024).

Online ISSN 3007-3197
Print ISSN 3007-3189



Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

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.

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.

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

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.

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.

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.

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

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.

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

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.

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,

Online ISSN 3007-3197
Print ISSN 3007-3189



no. 3, pp. 1-2, Jan. 2024

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

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.

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.

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.

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

Narasimhan, S. G., & Nayar, S. K. (2002). Vision and the Atmosphere. International Journal of Computer Vision, 48(3), 233–254.

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.

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.

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.

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.

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.

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

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025).

Online ISSN 3007-3197
Print ISSN 3007-3189



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.

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.

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.

P. De Filippi and S. Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.

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.

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.

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.

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

Ren, W., Liu, S., Zhang, H., Pan, J., Cao, X., & Yang, M.-H. (2016). Single Image Dehazing via Multi-Scale Convolutional Neural Networks. ECCV, 154–169.

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

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

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

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

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin

Online ISSN 3007-3197
Print ISSN 3007-3189



of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Saxena, A., Mane, V., & Abhale, A. (2017). Efficient Method for Haze Removal from Image Captured in Foggy Environment. International Journal of Advanced Technology & Engineering Research (IJATER), 7(6), 36–41.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. IEEE/CVF CVPR, 815–823.

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

Sharma, N., Kumar, V., & Singla, S. K. (2021). Single Image Defogging Using Deep Learning Techniques: Past, Present and Future. Archives of Computational Methods in Engineering, 28, 4449–4469.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Journal of Information Systems Engineering and Management, 10(11S), 633-650.

Suganya, R., & Kanagavalli, R. (2020). On the Review of Dehazing Methods for Bad Weather Images. IJETT, Special Issues ICT 2020, 90–98.

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.

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

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

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.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.

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

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

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA

Online ISSN 3007-3197
Print ISSN 3007-3189



Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

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

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

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

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.

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.

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.