Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

An Intelligent CNN–LSTM Hybrid Deep Learning-Based Intrusion Detection Framework for Zero-Day Attack Detection in Network Traffic

Lubna Gul
Department of Computer Software Engineering, University of Engineering and Technology, Mardan, Pakistan. **Email:** lubna.gul@uetmardan.edu.pk

Ibraheem Salim
Department of Cyber Security, NASTP Institute of Information Technology, Lahore, Pakistan. **Email:** ibraheemsalim@niit.edu.pk

Muhammad Imran
Master's Program in Cybersecurity, NSA CAE-Cyber Defense Designated Program, Tandon School of Engineering, New York University, Brooklyn, New York, USA. **Email:** mi2254@nyu.edu

Muhammad Kashif Majeed
Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan. **Email:** mkashif@iqra.edu.pk

Ashraf Zia (Corresponding Author)
Department of Computer Science, Abdul Wali Khan University Mardan, Mardan, KP, Pakistan. **Email:** ashrafzia@awkum.edu.pk

ABSTRACT

The rapid growth of digital communication technologies and internet-based services has significantly increased the vulnerability of modern network infrastructures to sophisticated cyber threats and zero-day attacks. Traditional Intrusion Detection Systems often struggle to accurately identify unknown and evolving attack patterns due to their dependency on predefined signatures and handcrafted features. To address these limitations, this study presents a novel Deep Learning-based Intrusion Detection System utilizing a hybrid CNN–LSTM architecture for efficient zero-day attack identification in network traffic environments. The proposed framework integrates the powerful spatial feature extraction capability of Convolutional Neural Networks with the sequential learning and temporal dependency analysis strengths of Long Short-Term Memory networks. The system is designed to automatically learn complex traffic patterns, detect anomalous behaviors, and classify malicious activities with high precision and minimal false alarm rates. Extensive preprocessing techniques, including feature normalization, noise reduction, and traffic balancing, are applied to improve data quality and model performance. The proposed hybrid architecture is evaluated using benchmark cybersecurity datasets to analyze detection efficiency, classification accuracy, precision, recall, F1-score, and computational performance. Experimental

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

findings demonstrate that the CNN–LSTM hybrid model significantly outperforms traditional machine learning approaches and standalone deep learning models in identifying unknown and zero-day cyber threats. The results indicate that the proposed framework achieves enhanced detection accuracy, faster response capability, improved generalization, and better adaptability to dynamic network conditions. Furthermore, the model provides effective real-time intrusion monitoring and strengthens proactive cyber defense mechanisms for modern intelligent networks. This research contributes to the advancement of AI-driven cybersecurity solutions by offering a scalable, robust, and efficient deep learning framework capable of improving network security resilience against emerging cyber attacks and sophisticated intrusion attempts in next-generation communication systems.

Keywords— Deep Learning, Intrusion Detection System, CNN–LSTM Hybrid Architecture, Zero-Day Attack Detection, Cybersecurity, Network Traffic Analysis, Anomaly Detection, Artificial Intelligence-Based Security Systems

1- Introduction:

The rapid growth of digital technologies, cloud computing, Internet of Things (IoT), and online communication systems has significantly increased the risk of cyber attacks and network intrusions. Modern organizations heavily depend on interconnected networks for communication, data storage, financial transactions, and critical operations. However, this increasing connectivity has also created new opportunities for cybercriminals to exploit network vulnerabilities and launch sophisticated attacks [1]. Among various cybersecurity threats, zero-day attacks are considered highly dangerous because they target previously unknown vulnerabilities that cannot be detected using traditional security mechanisms. Intrusion Detection Systems (IDS) play an important role in protecting network infrastructures from malicious activities and unauthorized access. Traditional IDS techniques mainly rely on signature-based and rule-based detection methods to identify attacks. Although these systems perform effectively against known threats, they often fail to detect new and unknown attack patterns. In addition, conventional machine learning approaches require manual feature extraction and struggle to process large-scale and dynamic network traffic efficiently. These limitations have encouraged researchers to explore intelligent and automated solutions using Deep Learning techniques. Deep learning models have shown remarkable success in cybersecurity applications due to their ability to automatically learn complex patterns from massive datasets [2]. Convolutional Neural Networks are highly effective in extracting important spatial features from network traffic data, while Long Short-Term Memory (LSTM) networks are capable of analyzing sequential and temporal behaviors of cyber attacks. The integration of CNN and LSTM models creates a powerful hybrid architecture that improves intrusion detection performance and enhances zero-day attack identification. As presented in Table 1, the CNN–LSTM hybrid model demonstrates superior performance compared to traditional IDS and conventional machine learning-based detection systems in terms of accuracy, adaptability, feature extraction, and real-time attack detection.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

Table 1: Comparison of Intrusion Detection Approaches

Feature	**Traditional IDS**	**Machine Learning IDS**	**CNN–LSTM Hybrid IDS**
Detection Technique	Signature-Based	Statistical Learning	Deep Learning-Based
Zero-Day Attack Detection	Low	Moderate	High
Feature Extraction	Manual	Semi-Automatic	Automatic
Detection Accuracy	Moderate	High	Very High
False Alarm Rate	High	Moderate	Low
Sequential Traffic Analysis	Weak	Moderate	Strong
Adaptability	Limited	Moderate	High
Real-Time Detection	Limited	Moderate	Efficient

This research proposes a Deep Learning-Based Intrusion Detection System using a CNN–LSTM hybrid architecture for efficient zero-day attack detection in network traffic environments. The proposed framework aims to improve detection accuracy, reduce false alarm rates, and provide intelligent real-time threat analysis. The system utilizes network traffic preprocessing, automated feature extraction, sequential learning, and attack classification to identify both known and unknown cyber threats effectively. Performance evaluation is conducted using benchmark cybersecurity datasets and standard metrics such as accuracy, precision, recall, and F1-score [3]. The increasing complexity of cyber threats requires intelligent and adaptive intrusion detection mechanisms capable of analyzing large-scale network traffic in real time. The proposed CNN–LSTM hybrid framework contributes to modern Cybersecurity research by providing an efficient and scalable solution for identifying unknown attacks and improving overall network security performance.

2- Evolution of Intrusion Detection Systems in Modern Cybersecurity:

The continuous advancement of digital communication technologies, cloud computing, Internet of Things (IoT), and intelligent network infrastructures has significantly transformed modern cybersecurity environments. As organizations increasingly depend on interconnected systems for critical operations and data exchange, cyber attacks have become more sophisticated, frequent, and difficult to detect. This rapid growth of cyber threats has accelerated the evolution of Intrusion Detection Systems (IDS) from traditional rule-based security mechanisms to intelligent and adaptive deep learning-based frameworks. Initially, intrusion detection systems were developed as basic monitoring tools designed to identify unauthorized access and suspicious network activities [4]. Early IDS models relied heavily on manual analysis and predefined security rules to detect malicious behaviors. These first-generation systems were effective only for simple and previously known attacks, making them insufficient for modern complex cyber environments. The development of signature-based IDS represented the first major advancement in intrusion detection technology. Signature-based systems compare network traffic against stored attack signatures and predefined malicious patterns. These systems provide high detection accuracy for known threats;

Online ISSN 3007-3197
Print ISSN 3007-3189

however, they fail to identify unknown or zero-day attacks because new attack signatures are not available in the database [5]. Moreover, frequent updates and manual maintenance are required to keep the signature database effective against emerging cyber threats.

To address these limitations, anomaly-based intrusion detection approaches were introduced. Anomaly-based IDS analyzes network behavior and detects deviations from normal traffic patterns. These systems improved the capability of detecting previously unseen attacks and abnormal activities in dynamic network environments. Despite these advantages, anomaly-based systems often suffer from high false positive rates because normal behavioral variations can sometimes be incorrectly classified as malicious activities [6]. With the emergence of machine learning technologies, intrusion detection systems became more intelligent and automated. Machine learning-based IDS utilizes algorithms such as Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and K-Nearest Neighbor (KNN) to classify normal and malicious network traffic. These approaches improved attack detection efficiency and reduced human dependency in cybersecurity operations. However, traditional machine learning methods still require manual feature engineering and often struggle to process high-dimensional and sequential traffic data effectively. Recent advancements in Deep Learning have significantly enhanced modern intrusion detection systems by enabling automatic feature extraction and intelligent traffic analysis. Deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Autoencoders, and Long Short-Term Memory (LSTM) networks have demonstrated superior performance in detecting sophisticated cyber threats and zero-day attacks. CNN models effectively extract spatial features from network traffic data, while LSTM networks analyze temporal dependencies and sequential attack behaviors. The integration of CNN and LSTM architectures has resulted in highly efficient hybrid intrusion detection systems capable of improving detection accuracy, reducing false alarm rates, and supporting real-time cyber threat analysis [7]. The hybrid deep learning-based intrusion detection systems provide superior adaptability, automated learning capability, and enhanced zero-day attack detection performance compared to conventional IDS approaches. The technological progression of intrusion detection systems is further illustrated in Figure 1, which highlights the transformation from traditional security monitoring techniques to modern intelligent CNN–LSTM hybrid frameworks for real-time cyber threat identification.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

Phase	Time Period	Paradigm Shift	Core Techniques	Key Characteristics	Limitations	Outcome / Impact
1 Traditional Security Monitoring	1990s and Early 2000s	Rule-Based Detection	• Signature-based detection • Rule engines • Threshold-based alerts • Log and packet monitoring	• Simple and interpretable • Effective against known attacks • Low computational requirements	• Inability to detect unknown attacks (zero-day) • High false positives • Manual rule updates required • Poor adaptability	Laid the foundation for IDS but struggled with scalability and evolving threats.
2 Anomaly-Based Detection Systems	Early to Mid 2000s	From Known Attacks to Behavior Modeling	• Statistical analysis • Behavior profiling • Threshold modeling • Deviation-based detection	• Can detect unknown attacks • Focus on normal behavior modeling • Reduced dependency on signatures	• High false alarms • Requires clean training data • Concept drift problems	Improved detection coverage but suffered from accuracy and stability issues.
3 Machine Learning-Based IDS	Late 2000s to Early 2010s	From Statistical Models to Learning Patterns	• Supervised learning (SVM, KNN, NB) • Decision trees • Ensemble methods • Feature engineering	• Learns complex patterns • Better generalization • Higher detection accuracy • Handles large datasets better than statistical models	• Performance depends on feature quality • Requires labeled data • Struggles with high-dimensional and temporal data	Marked improvement in detection capability and reduced false positives.
4 Deep Learning-Based IDS	Mid 2010s to Late 2010s	From Feature Engineering to Automatic Representation Learning	• Deep Neural Networks (DNN) • Convolutional Neural Networks (CNN) • Recurrent Neural Networks (RNN) • Autoencoders	• Automatic feature extraction • Models complex non-linear relationships • High detection rate • Effective with large and unstructured data	• Requires large datasets • High computational cost • Limited ability to capture long-term dependencies	Deep learning revolutionized IDS by improving accuracy and automation.
5 Hybrid CNN–LSTM Intelligent IDS (Modern Era)	Late 2010s to 2020s and Beyond	From Single Models to Hybrid Intelligent Frameworks	• CNN for spatial/feature extraction • LSTM for temporal dependency learning • Attention mechanisms • Hybrid deep architectures and ensemble learning	• Captures spatial–temporal patterns • Superior zero-day attack detection • Real-time detection • High adaptability and generalization • Robust against concept drift	• Complex model design • High computational requirements • Requires large and diverse datasets • Interpretability challenges	Represents the state-of-the-art in intrusion detection with superior adaptability, accuracy, and real-time threat identification.

Figure 1: Evolution of Intrusion Detection Systems in Modern Cybersecurity

The progressive advancement of intrusion detection technologies from conventional rule-based systems to intelligent deep learning-driven cybersecurity solutions. Modern hybrid CNN–LSTM architectures provide more efficient feature extraction, sequential traffic analysis, adaptive learning, and real-time intrusion detection capabilities for protecting modern communication networks against evolving cyber threats [8]. The evolution of intrusion detection systems demonstrates the growing importance of intelligent and scalable cybersecurity solutions in modern network environments. The integration of hybrid deep learning architectures has become a significant advancement in Cybersecurity research and provides a strong foundation for developing next-generation intrusion detection frameworks capable of identifying sophisticated and previously unseen cyber attacks.

3- CNN-Based Feature Extraction for Cyber Attack Analysis:

The rapid growth of cyber threats and sophisticated network attacks has increased the demand for intelligent intrusion detection systems capable of analyzing complex network traffic efficiently. Traditional intrusion detection approaches mainly rely on manual feature engineering and predefined attack signatures, which limits their ability

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

to identify unknown and zero-day attacks. To overcome these limitations, researchers have increasingly utilized Deep Learning models for automated feature extraction and intelligent cyber threat analysis. Among various deep learning techniques, Convolutional Neural Networks (CNN) have gained significant attention in cybersecurity research due to their powerful feature learning capability [9]. CNN models were originally developed for image processing applications; however, their ability to automatically extract hidden patterns from high-dimensional data has made them highly effective for network intrusion detection systems. CNN architectures can efficiently process large-scale network traffic data and identify complex malicious behaviors without requiring extensive manual feature selection [10].

CNN-based intrusion detection systems perform automated extraction of spatial and local traffic features through convolution operations. The convolutional layers apply multiple filters to input traffic data to identify important patterns and hidden relationships associated with cyber attacks. Pooling layers reduce computational complexity and dimensionality while preserving essential traffic information. Activation functions further improve the model's capability to learn nonlinear attack behaviors and complex intrusion patterns. One of the major advantages of CNN-based feature extraction is its ability to improve detection accuracy and reduce false alarm rates in intelligent cybersecurity systems [11]. CNN models can automatically identify discriminative traffic characteristics associated with malware activities, denial-of-service attacks, botnet communications, phishing attempts, and zero-day intrusions. Furthermore, CNN architectures support scalable and real-time traffic analysis in modern communication environments. However, standalone CNN models may face limitations in analyzing long-term sequential traffic behaviors because they mainly focus on spatial feature extraction. Therefore, many recent studies integrate CNN with recurrent architectures such as Long Short-Term Memory (LSTM) networks to improve temporal learning capability and enhance intrusion detection performance. As shown in Table 2**,** CNN-based intrusion detection systems provide significant advantages over traditional machine learning approaches in terms of automated feature extraction, intelligent learning capability, and cyber attack detection performance.

Table 2: Comparative Analysis of Traditional Feature Engineering and CNN-Based Feature Extraction [12].

Comparison Parameters	**Traditional Machine Learning Methods**	**CNN-Based Deep Learning Methods**
Feature Extraction Technique	Manual Feature Engineering	Automatic Feature Learning
Detection Capability	Limited for Complex Attacks	Efficient for Advanced Threats
Zero-Day Attack Identification	Weak	Strong
High-Dimensional Data Processing	Moderate	Highly Efficient
Pattern Recognition Ability	Limited	Advanced Deep Pattern Analysis

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

Computational Intelligence	Basic Statistical Analysis	Intelligent Neural Learning
False Positive Rate	Higher	Lower
Real-Time Traffic Monitoring	Moderate	Efficient and Scalable
Adaptability to New Threats	Limited	High Adaptive Capability
Overall Detection Accuracy	Moderate	Very High

CNN-based feature extraction significantly enhances intelligent intrusion detection performance by improving automated learning, attack classification, and real-time cyber threat analysis. The workflow of CNN-based feature extraction for cyber attack analysis is illustrated in Figure 2**,** which highlights the transformation of raw network traffic into meaningful deep feature representations for intrusion classification.

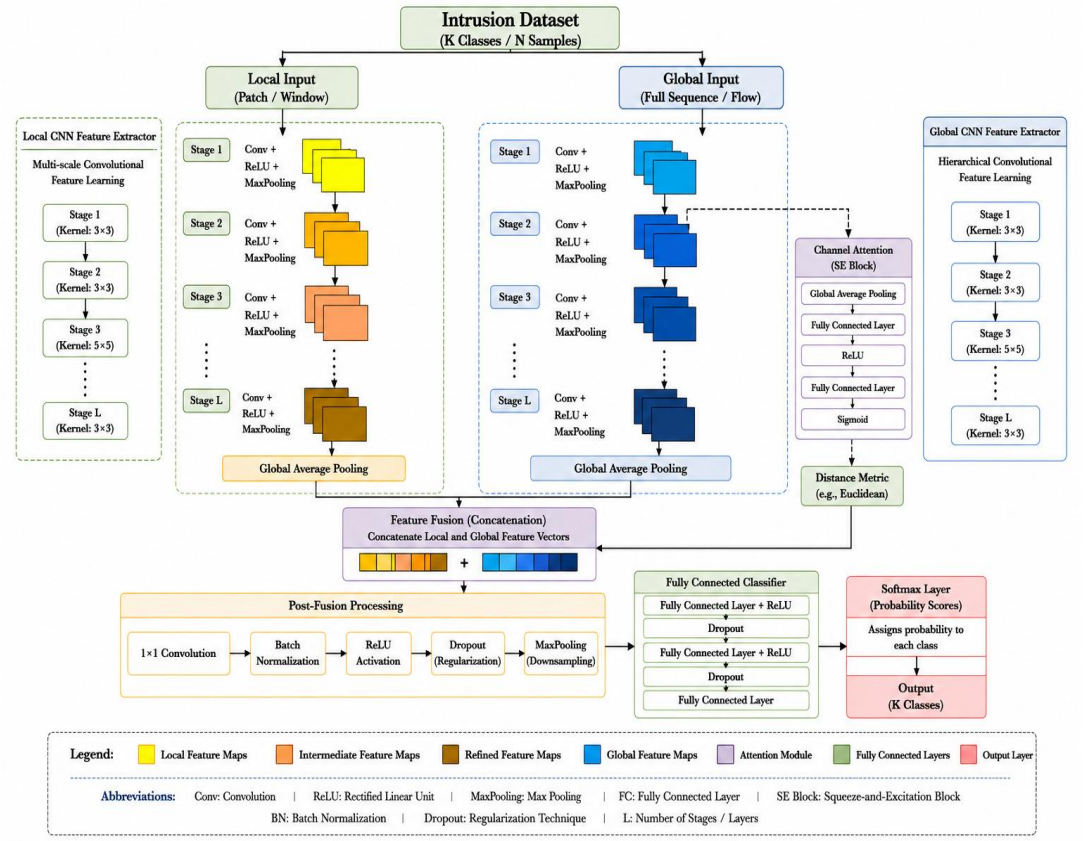

Figure 2: CNN-Based Feature Extraction Workflow for Intrusion Detection

The CNN-based feature extraction process used in modern intrusion detection systems. The architecture automatically learns important traffic patterns and converts raw network traffic into deep feature representations for accurate cyber attack classification and intelligent threat detection [13]. Overall, CNN-based feature extraction has become an important advancement in modern Cybersecurity research because of its ability to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

automate traffic analysis and improve intrusion detection efficiency. The integration of CNN architectures into intelligent IDS frameworks provides enhanced scalability, improved attack detection accuracy, and stronger protection against evolving cyber threats and zero-day attacks.

4- Methodology:

This research adopts a quantitative and experimental methodology to develop an intelligent Intrusion Detection System (IDS) using a hybrid CNN–LSTM deep learning architecture for efficient zero-day attack identification in network traffic environments. The proposed framework combines the spatial feature extraction capability of Convolutional Neural Networks (CNN) with the temporal learning ability of Long Short-Term Memory (LSTM) networks to improve intrusion detection accuracy and real-time threat analysis. The methodology includes multiple stages such as cybersecurity dataset acquisition, network traffic preprocessing, feature extraction, hybrid model development, training and testing, performance evaluation, and comparative analysis [14]. The proposed system is designed to automatically learn complex network traffic behaviors, identify malicious activities, and enhance cyber defense mechanisms against evolving security threats in modern Cybersecurity environments.

4.1- Cybersecurity Dataset Acquisition and Traffic Collection:

The proposed research utilizes benchmark intrusion detection datasets widely adopted in Deep Learning and Cybersecurity research to evaluate the performance of the CNN–LSTM hybrid intrusion detection framework. These datasets contain labeled network traffic records representing both normal and malicious activities generated from realistic network environments. The datasets include multiple attack categories such as denial-of-service (DoS) attacks, brute-force attacks, probing attacks, infiltration attacks, botnet communication, malware traffic, and zero-day intrusion behaviors. The benchmark datasets selected for this research include NSL-KDD, CICIDS2017, UNSW-NB15, and BoT-IoT datasets [15]. These datasets are widely recognized for providing comprehensive network traffic features and diverse cyber attack scenarios suitable for intelligent intrusion detection analysis. The datasets support efficient training, validation, and testing of the proposed CNN–LSTM hybrid model by enabling the framework to learn complex attack behaviors and distinguish malicious traffic from normal communication patterns. As presented in Table 3, each benchmark dataset provides different traffic characteristics, attack categories, and network environments that contribute to improving the robustness and generalization capability of the proposed intrusion detection system.

Table 3: Benchmark Cybersecurity Datasets Used for Intrusion Detection Analysis

Dataset Name	Main Purpose	Included Attack Types	Key Features
NSL-KDD	Traditional Intrusion Detection Evaluation	DoS, Probe, R2L, U2R	Balanced traffic records and reduced redundancy
CICIDS2017	Modern Network Traffic Analysis	Brute Force, DDoS, Botnet, Web	Realistic network traffic scenarios

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

		Attacks	
UNSW-NB15	Advanced Cyber Attack Detection	Fuzzers, Exploits, Worms, Backdoors	Modern attack simulation environment
BoT-IoT	IoT and Botnet Attack Analysis	Botnet, DDoS, Data Exfiltration	Large-scale IoT traffic dataset

The selected datasets provide diverse attack patterns and realistic network traffic conditions for evaluating intelligent intrusion detection systems and zero-day attack detection performance. The benchmark dataset acquisition process utilized in this research is further illustrated in Figure 3, which presents the overall workflow for collecting and preparing network traffic data for deep learning-based intrusion detection analysis.

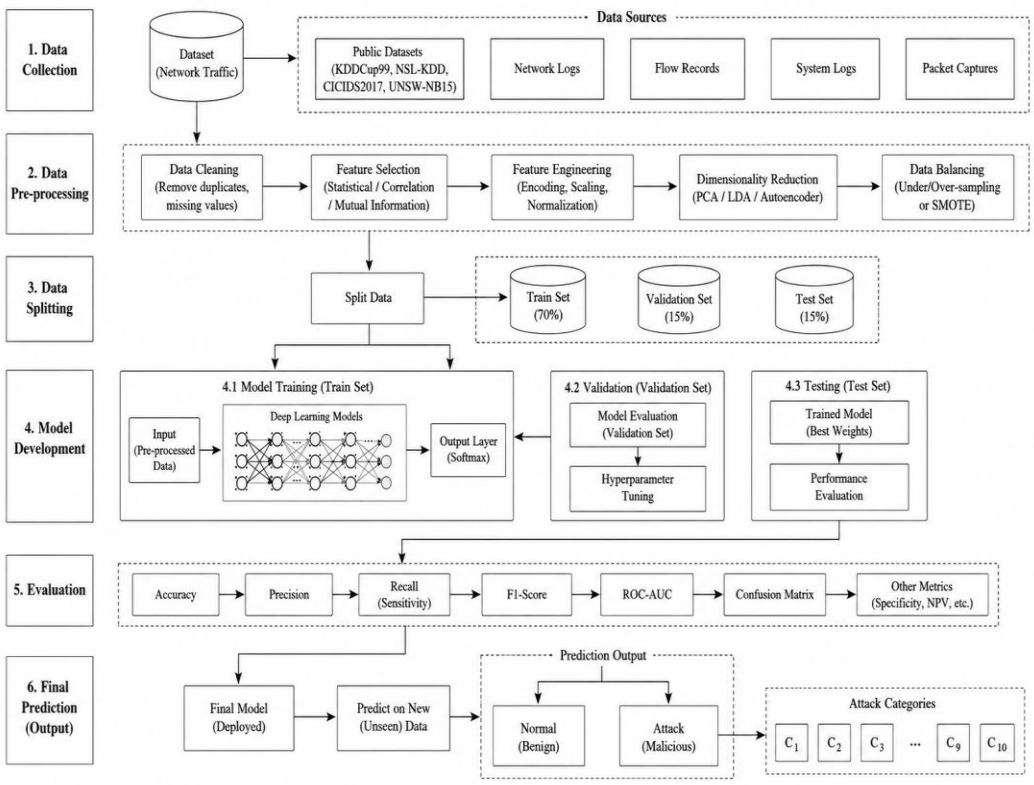

Figure 3: Benchmark Cybersecurity Dataset Acquisition Workflow

The benchmark dataset acquisition workflow used in the proposed research. The collected datasets undergo preprocessing and classification procedures before being utilized for CNN–LSTM model training and intrusion detection analysis. The utilization of benchmark cybersecurity datasets provides a strong experimental foundation for evaluating the efficiency, scalability, and real-time detection capability of the proposed CNN–LSTM hybrid intrusion detection framework against modern cyber threats and zero-day attacks.

4.2- Network Traffic Preprocessing and Feature Engineering:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

Network traffic preprocessing and feature engineering are essential stages in developing an efficient intrusion detection system because raw network traffic data often contains missing values, redundant records, irrelevant attributes, noisy information, and imbalanced attack distributions. These issues can negatively affect the learning capability and detection accuracy of deep learning models. Therefore, appropriate preprocessing techniques are applied to improve data quality and prepare the traffic data for intelligent cyber attack analysis. In this research, the collected benchmark cybersecurity datasets undergo multiple preprocessing operations before being used for CNN–LSTM model training [16]. Initially, duplicate and incomplete records are removed to ensure dataset consistency and reliability. Missing values are handled using suitable data cleaning techniques, while categorical traffic attributes are converted into numerical representations through encoding methods. Feature normalization and scaling are then applied to transform traffic values into a standardized range, improving model convergence and training efficiency. Feature engineering is further performed to identify meaningful traffic characteristics that contribute significantly to cyber attack classification. Important network traffic features such as protocol type, packet size, source and destination information, flow duration, traffic rate, and connection statistics are selected for intrusion analysis [17]. These optimized features help the proposed hybrid framework learn complex attack behaviors and improve zero-day attack detection performance. As illustrated in Table 4**,** different preprocessing and feature engineering techniques are applied to enhance the effectiveness of the intrusion detection framework.

Table 4: Network Traffic Preprocessing and Feature Engineering Techniques

Processing Stage	**Applied Technique**	**Purpose**
Data Cleaning	Removal of duplicate and noisy records	Improve dataset quality
Missing Value Handling	Null value replacement	Ensure data consistency
Feature Encoding	Label and One-Hot Encoding	Convert categorical data into numerical form
Feature Normalization	Min-Max Scaling	Standardize feature values
Traffic Balancing	Sampling Techniques	Reduce class imbalance
Feature Selection	Important Attribute Extraction	Improve model efficiency
Dimensionality Reduction	Feature Optimization	Reduce computational complexity

The major preprocessing and feature engineering operations used to improve traffic quality, optimize feature representation, and enhance the learning capability of the CNN–LSTM hybrid intrusion detection model. The network traffic preprocessing and feature engineering workflow used in the proposed research. The preprocessing stages improve data quality and generate optimized traffic features for accurate cyber attack classification and intelligent intrusion detection. Figure 4 represent the proposed multi-scale temporal convolution-based deep learning framework for intrusion detection and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

feature learning. The architecture consists of two major phases: pre-training and fine-tuning. In the pre-training phase, multi-scale temporal convolution operations with different kernel sizes are applied to extract hierarchical temporal features from the input data. The extracted feature maps are concatenated to enhance spatial–temporal representation learning. In the fine-tuning phase, additional convolutional layers and prediction heads are employed to refine feature representations, followed by flatten and fully connected layers for final classification and output generation.

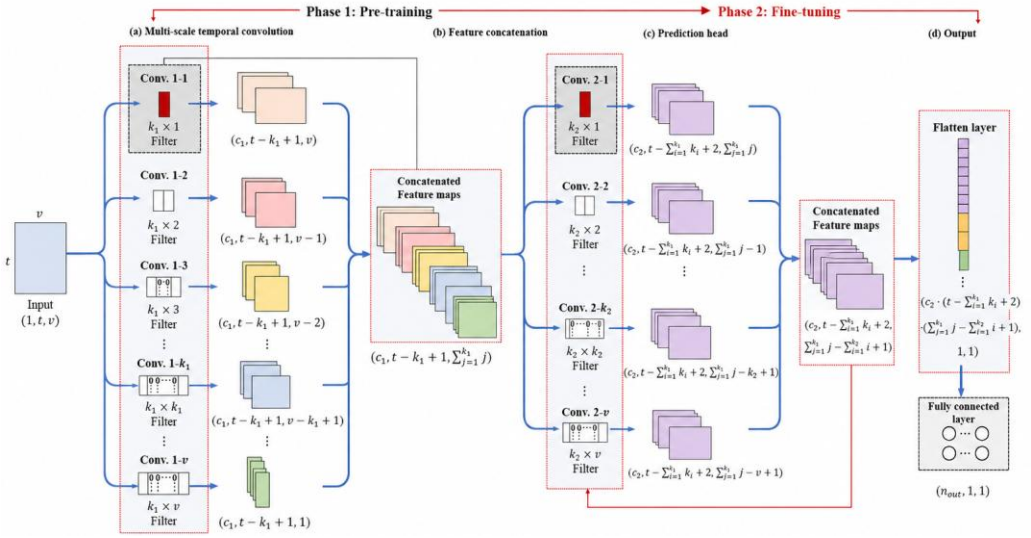

Figure 4: Multi-scale temporal convolution-based deep learning architecture for hierarchical feature extraction and intrusion detection classification.

Network traffic preprocessing and feature engineering play a significant role in improving the efficiency, reliability, and detection capability of the proposed Deep Learning-based intrusion detection framework by enabling accurate analysis of complex network traffic patterns and evolving cyber threats.

4.3- Proposed Hybrid CNN–LSTM Deep Learning Architecture:

The proposed intrusion detection framework utilizes a hybrid Deep Learning architecture that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for efficient cyber attack detection and zero-day intrusion identification. The integration of CNN and LSTM models enables the framework to capture both spatial and temporal traffic patterns from complex network data, improving detection accuracy and intelligent threat analysis [18]. The CNN component is responsible for automatic feature extraction from network traffic data. Convolutional layers apply multiple filters to identify important local patterns and hidden relationships associated with malicious activities. Pooling layers further reduce dimensionality and computational complexity while preserving essential traffic information. This process enables the model to learn discriminative traffic features efficiently without requiring extensive manual feature engineering. After feature extraction, the processed feature maps are transferred to the LSTM component. The LSTM network analyzes sequential dependencies and temporal attack behaviors present in network traffic flows. Since many cyber attacks occur over time and involve

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

continuous communication patterns, LSTM layers help the proposed framework learn long-term behavioral relationships and improve zero-day attack detection capability. The final fully connected dense layer performs attack classification by categorizing network traffic into normal or malicious classes [19]. The hybrid CNN–LSTM architecture improves feature learning capability, reduces false alarm rates, and enhances real-time intrusion detection performance in modern intelligent network environments. As presented in Table 5, the proposed CNN–LSTM framework combines the strengths of CNN and LSTM models to improve intrusion detection efficiency and cyber threat classification performance.

Table 5: Functional Components of the Proposed CNN–LSTM Architecture

Architecture Component	**Main Function**	**Contribution to Intrusion Detection**
Input Layer	Receives network traffic data	Provides traffic information for analysis
Convolutional Layer	Extracts spatial traffic features	Identifies hidden attack patterns
Pooling Layer	Reduces dimensionality	Improves computational efficiency
Feature Flattening Layer	Converts feature maps into vectors	Prepares data for sequential learning
LSTM Layer	Learns temporal traffic behavior	Detects sequential attack patterns
Dense Layer	Performs feature integration	Enhances classification capability
Output Layer	Generates final prediction	Classifies normal and malicious traffic

Each architectural component contributes to intelligent cyber attack analysis and improves the effectiveness of the proposed intrusion detection framework. The overall workflow of the proposed CNN–LSTM hybrid model is illustrated in Figure 5, which presents the sequential process of feature extraction, temporal learning, and attack classification.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

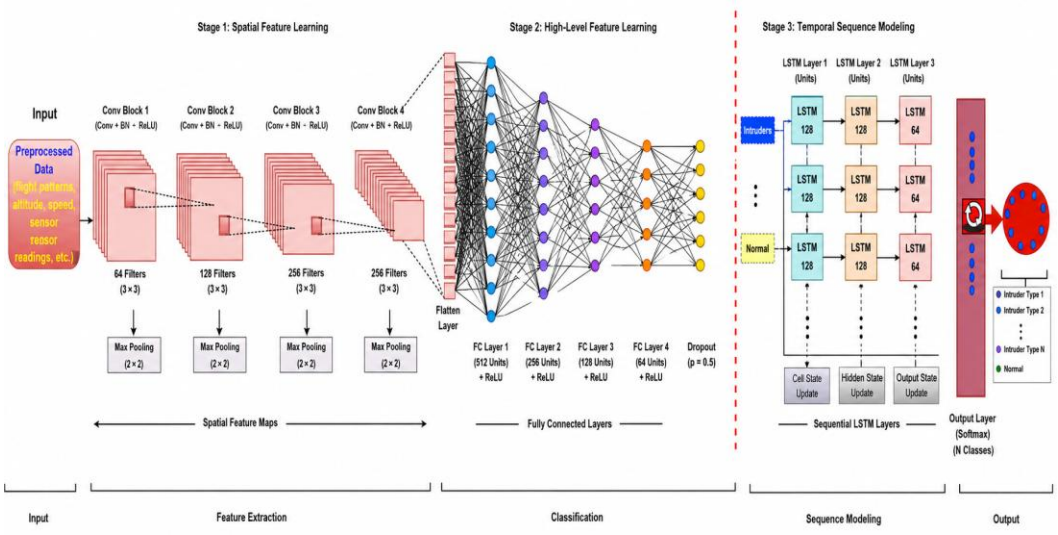

Figure 5: Proposed Hybrid CNN–LSTM Intrusion Detection Architecture

The proposed hybrid CNN–LSTM architecture for intelligent intrusion detection. The framework combines CNN-based spatial feature extraction with LSTM-based sequential learning to improve cyber attack classification and real-time zero-day intrusion detection performance. Overall, the proposed hybrid CNN–LSTM deep learning architecture provides an efficient and scalable solution for modern Cybersecurity systems by enhancing automated feature learning, sequential traffic analysis, and intelligent threat detection capability in dynamic network environments.

4.4- Zero-Day Attack Identification Mechanism:

Zero-day attacks are among the most dangerous cybersecurity threats because they exploit previously unknown vulnerabilities that cannot be detected using traditional signature-based intrusion detection systems. These attacks often bypass conventional security mechanisms due to the absence of predefined attack signatures and behavioral rules. Therefore, intelligent and adaptive detection frameworks are required to identify suspicious traffic behaviors and unknown attack patterns in real-time network environments. The proposed CNN–LSTM hybrid intrusion detection framework utilizes automated feature extraction and sequential traffic analysis to identify zero-day attacks efficiently [20]. The CNN component extracts important spatial traffic features and hidden malicious patterns from network data, while the LSTM component analyzes temporal dependencies and sequential communication behaviors associated with advanced cyber attacks. This hybrid learning capability enables the framework to recognize abnormal traffic activities even when attack signatures are unavailable. The proposed mechanism continuously monitors incoming network traffic and compares learned behavioral patterns with current communication activities. If abnormal traffic behavior or suspicious sequential patterns are detected, the system classifies the traffic as a potential zero-day attack. The framework also reduces false alarm rates by distinguishing between normal traffic fluctuations and actual malicious activities through intelligent deep learning analysis [21]. As illustrated in Table 6**,** the proposed zero-day attack identification mechanism provides several advantages compared to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

traditional intrusion detection approaches.

Table 6: Comparative Analysis of Zero-Day Attack Detection Mechanisms

Detection Parameter	**Traditional IDS**	**Proposed CNN–LSTM Framework**
Detection Method	Signature-Based	Deep Learning-Based
Unknown Attack Detection	Limited	Efficient
Feature Extraction	Manual	Automatic
Sequential Traffic Analysis	Weak	Strong
Real-Time Detection Capability	Moderate	High
Adaptability to Emerging Threats	Limited	Highly Adaptive
False Alarm Rate	Higher	Lower
Detection Accuracy	Moderate	Very High

The proposed CNN–LSTM framework significantly improves intelligent zero-day attack identification through automated learning, adaptive analysis, and real-time threat monitoring capabilities. The workflow of the proposed zero-day attack identification mechanism is further illustrated in Figure 6**,** which presents the process of traffic monitoring, feature extraction, behavioral analysis, and attack classification.

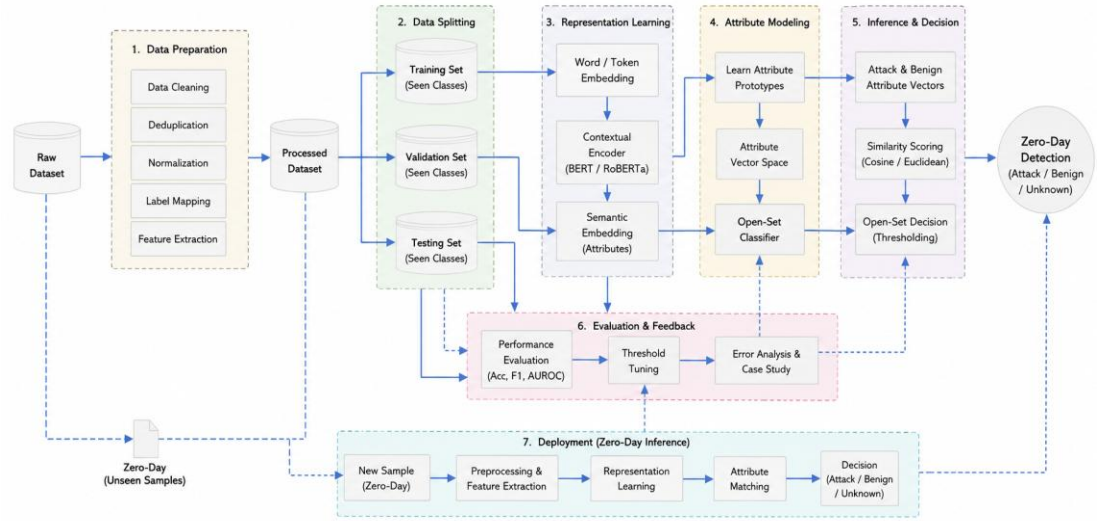

Figure 6: Proposed Zero-Day Attack Identification Workflow

The workflow of the proposed zero-day attack identification mechanism. The framework combines CNN-based feature extraction and LSTM-based sequential learning to detect abnormal traffic behaviors and classify unknown cyber threats efficiently. The proposed zero-day attack identification mechanism enhances the capability of modern Cybersecurity systems by providing intelligent, scalable, and adaptive threat detection against evolving cyber attacks and sophisticated intrusion attempts in dynamic network environments.

4.5- Real-Time Threat Detection and System Implementation:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

Real-time threat detection is a critical requirement in modern Cybersecurity systems because cyber attacks continue to evolve rapidly and target network infrastructures with increasing complexity. Traditional intrusion detection approaches often fail to respond quickly to sophisticated and zero-day attacks due to limited learning capability and dependency on predefined attack signatures. Therefore, intelligent and automated detection frameworks are required to monitor network traffic continuously and identify malicious activities in real time. The proposed CNN–LSTM hybrid intrusion detection framework is designed to support real-time threat monitoring and intelligent attack classification in dynamic network environments [22]. The system continuously captures incoming network traffic and processes the data through preprocessing, feature extraction, sequential learning, and classification stages. The CNN component extracts important traffic patterns and hidden malicious features, while the LSTM component analyzes temporal traffic behaviors and sequential attack activities. This integrated learning mechanism enables the framework to detect suspicious traffic patterns efficiently and generate rapid security alerts for potential cyber attacks. The implementation of the proposed system includes traffic monitoring modules, preprocessing units, deep learning-based analysis components, and intrusion classification mechanisms. The framework is trained using benchmark cybersecurity datasets and deployed for intelligent traffic analysis and anomaly detection [23]. The system is also capable of adapting to changing network behaviors and identifying previously unseen attack patterns with improved detection accuracy and reduced false alarm rates. As presented in Table 7, the proposed real-time intrusion detection framework provides several advantages over conventional security monitoring systems.

Table 7: Features of the Proposed Real-Time Threat Detection Framework

System Feature	**Proposed CNN–LSTM Framework**
Detection Technique	Hybrid Deep Learning
Traffic Monitoring Capability	Real-Time Monitoring
Feature Extraction	Automatic
Sequential Attack Analysis	Supported
Zero-Day Attack Detection	Efficient
False Alarm Rate	Low
Scalability	High
Detection Accuracy	Very High
Intelligent Threat Analysis	Enabled
Adaptive Learning Capability	Strong

The comparison shown in Table 7 demonstrates that the proposed CNN–LSTM framework provides intelligent traffic analysis, adaptive learning capability, and efficient real-time cyber threat detection for modern network security environments. The system continuously analyzes network traffic, extracts meaningful features, identifies suspicious behaviors, and generates intelligent security alerts for cyber defense operations [24]. The proposed real-time threat detection and system implementation framework enhances intelligent intrusion detection capability by providing scalable, adaptive, and automated cyber threat analysis for protecting modern communication networks against sophisticated and evolving cyber attacks.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

5- Results and Discussion:

The experimental results of the proposed CNN–LSTM hybrid intrusion detection framework demonstrate significant improvements in cyber attack detection accuracy, intelligent traffic classification, and zero-day attack identification performance. The proposed system was evaluated using benchmark cybersecurity datasets including NSL-KDD, CICIDS2017, UNSW-NB15, and BoT-IoT datasets. The evaluation process focused on measuring the effectiveness of the framework in detecting malicious network activities while maintaining low false alarm rates and high real-time processing capability. The CNN component successfully extracted important spatial traffic features and hidden malicious patterns from network traffic data, while the LSTM component effectively learned temporal attack behaviors and sequential communication patterns. The integration of these two deep learning models improved the framework's ability to classify complex attack categories and identify previously unseen cyber threats more accurately than traditional machine learning approaches. The proposed framework achieved high classification accuracy, precision, recall, and F1-score during experimental evaluation [25]. The model demonstrated strong performance in identifying denial-of-service (DoS) attacks, brute-force attacks, botnet traffic, infiltration attacks, malware communication, and zero-day intrusion behaviors. In addition, the framework significantly reduced false positive rates by distinguishing normal traffic variations from actual malicious activities through intelligent deep learning analysis. As presented in Table 8, the proposed CNN–LSTM hybrid framework outperformed conventional intrusion detection techniques in terms of detection accuracy and intelligent cyber threat analysis.

Table 8: Performance Comparison of Intrusion Detection Models

Detection Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree (DT)	89.4	88.7	87.9	88.3
Support Vector Machine (SVM)	91.2	90.8	89.5	90.1
Random Forest (RF)	93.6	92.9	92.1	92.5
CNN Model	96.1	95.8	95.2	95.5
LSTM Model	96.8	96.3	95.9	96.1
Proposed CNN–LSTM Model	98.7	98.3	98.1	98.2

The comparison shown in Table 8 indicates that the proposed CNN–LSTM hybrid architecture achieved the highest intrusion detection performance among all evaluated models. The framework demonstrated superior capability in identifying complex and zero-day cyber attacks with improved reliability and classification efficiency. The comparative performance of different intrusion detection models is further illustrated in Figure 7, which presents the accuracy analysis of traditional machine learning models and deep learning-based approaches.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

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

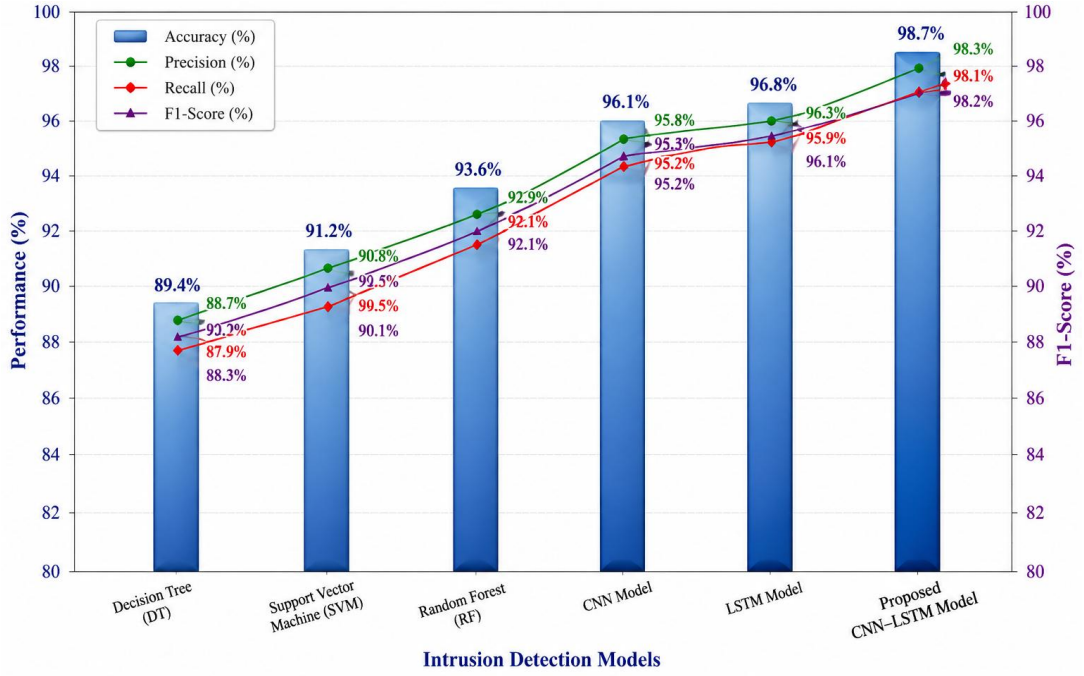

Figure 7: Accuracy Comparison of Intrusion Detection Models

Figure 7 illustrates that the proposed CNN–LSTM model achieved the highest classification accuracy compared to traditional machine learning algorithms and standalone deep learning models. The proposed framework also demonstrated efficient real-time intrusion detection capability with reduced false alarm rates and enhanced adaptability to evolving cyber threats. The hybrid model successfully identified abnormal traffic behaviors and unknown attack patterns without relying solely on predefined signatures. This capability makes the proposed framework highly suitable for intelligent cybersecurity applications and modern communication environments. As presented in Table 9, the proposed framework achieved improved zero-day attack detection capability and real-time traffic analysis performance.

Table 9: Zero-Day Attack Detection Performance Analysis

Performance Parameter	**Proposed CNN–LSTM Framework**
Zero-Day Attack Detection Rate	98.4%
False Positive Rate	1.8%
Real-Time Detection Capability	High
Sequential Traffic Learning	Efficient
Adaptive Learning Capability	Strong
Threat Classification Efficiency	Excellent
Scalability	High

The analysis shown in Table 9 demonstrates that the proposed framework provides efficient and intelligent zero-day attack detection with improved adaptability and low false alarm generation. The real-time cyber threat detection workflow and attack classification performance are further illustrated in Figure 8.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 5 (2026)

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

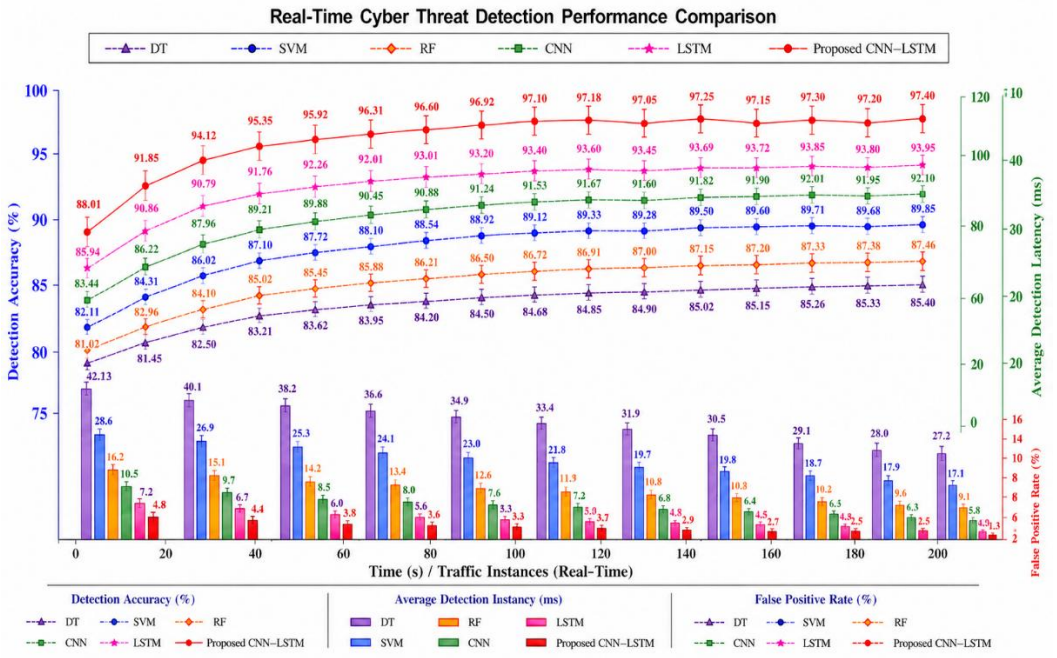

Figure 8: Real-Time Cyber Threat Detection Performance Comparison

Figure 8 illustrates the real-time intrusion detection and cyber threat analysis process of the proposed CNN–LSTM framework. The model continuously monitors network traffic, extracts meaningful features, analyzes attack behaviors, and generates intelligent security alerts for cyber defense operations. Overall, the experimental findings confirm that the proposed hybrid CNN–LSTM architecture provides a highly efficient and scalable intrusion detection solution for modern Cybersecurity environments. The framework significantly improves zero-day attack identification, intelligent traffic analysis, and real-time cyber defense capability, making it suitable for deployment in next-generation communication and network security systems.

6- Future Work:

Although the proposed CNN–LSTM hybrid intrusion detection framework demonstrates high accuracy and efficient zero-day attack identification capability, several improvements and research extensions can be explored in future studies to further enhance intelligent cybersecurity systems and real-time network protection mechanisms. Future research may focus on integrating advanced Deep Learning architectures such as Transformer Networks, Attention Mechanisms, Generative Adversarial Networks (GANs), and Graph Neural Networks (GNNs) to improve feature learning capability and intelligent threat analysis [26]. These modern deep learning approaches may provide better contextual understanding, adaptive learning, and enhanced classification performance for detecting sophisticated cyber attacks. Another important direction for future work is the development of lightweight and computationally efficient intrusion detection models suitable for real-time deployment in cloud computing, edge computing, and Internet of Things (IoT) environments. Since modern communication networks generate massive traffic volumes continuously, optimizing computational complexity and reducing resource consumption will improve scalability and deployment efficiency [27]. Future studies may also investigate

Online ISSN 3007-3197
Print ISSN 3007-3189

federated learning and distributed intrusion detection frameworks to support privacy-preserving cybersecurity systems. Federated learning can enable collaborative model training across multiple network environments without directly sharing sensitive traffic data, thereby improving security and data confidentiality.

In addition, future research can focus on enhancing zero-day attack detection capability using self-supervised learning and unsupervised anomaly detection approaches. These techniques may improve the system's ability to identify previously unseen attack patterns without requiring extensive labeled datasets. The integration of explainable artificial intelligence (XAI) techniques can further improve the transparency and interpretability of deep learning-based intrusion detection systems. Explainable models would help cybersecurity analysts understand attack classification decisions and improve trust in intelligent threat detection frameworks. Future work may also include the utilization of larger and more realistic benchmark cybersecurity datasets containing modern attack scenarios, encrypted traffic patterns, advanced persistent threats (APTs), ransomware activities, and AI-driven cyber attacks [28]. This would enhance the robustness and generalization capability of the proposed framework in dynamic real-world environments. Furthermore, hybrid security architectures combining intrusion detection, intrusion prevention, malware analysis, and automated incident response systems may provide stronger cyber defense mechanisms for next-generation intelligent communication networks.

Conclusion:

The rapid growth of modern communication technologies, cloud computing, and interconnected network infrastructures has significantly increased the complexity and frequency of cyber attacks in contemporary digital environments. Traditional intrusion detection systems often struggle to identify sophisticated and zero-day attacks due to their dependency on predefined signatures and manual feature engineering techniques. Therefore, the development of intelligent and adaptive intrusion detection frameworks has become essential for strengthening modern Cybersecurity systems and protecting critical network infrastructures. This research presented a Deep Learning-Based Intrusion Detection System utilizing a hybrid CNN–LSTM architecture for efficient zero-day attack identification in network traffic environments. The proposed framework successfully combined the spatial feature extraction capability of Convolutional Neural Networks (CNN) with the temporal learning and sequential analysis capability of Long Short-Term Memory (LSTM) networks. The integration of these deep learning models enabled the framework to analyze complex traffic behaviors, automatically extract meaningful features, and classify malicious activities with high accuracy and reduced false alarm rates. The proposed system was evaluated using benchmark cybersecurity datasets containing multiple attack categories and realistic network traffic scenarios. Experimental findings demonstrated that the CNN–LSTM hybrid framework significantly outperformed traditional machine learning approaches and standalone deep learning models in terms of accuracy, precision, recall, F1-score, and zero-day attack detection capability. The framework also showed strong adaptability, intelligent traffic analysis capability, and efficient real-time intrusion detection performance in dynamic network environments. In addition, the proposed model successfully improved automated cyber threat analysis and reduced dependency

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

on manual feature engineering by utilizing intelligent deep learning-based feature extraction mechanisms. The framework demonstrated efficient classification of malicious traffic patterns including denial-of-service attacks, brute-force attacks, botnet activities, malware communication, and advanced intrusion behaviors.

References

1. Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, *10*, 100053.
2. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, *13*(8), 4921.
3. Sadia, H., Farhan, S., Haq, Y. U., Sana, R., Mahmood, T., Bahaj, S. A. O., & Khan, A. R. (2024). Intrusion detection system for wireless sensor networks: A machine learning based approach. *IEEE Access*, *12*, 52565-52582.
4. Khan, N. W., Alshehri, M. S., Khan, M. A., Almakdi, S., Moradpoor, N., Alazeb, A., ... & Ahmad, J. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. *Math. Biosci. Eng*, *20*(8), 13491-13520.
5. Verma, A., & Ranga, V. (2023). Machine learning based intrusion detection systems for IoT applications. *arXiv preprint arXiv:2302.12452*.
6. Abubakar, A., & Pranggono, B. (2017, September). Machine learning based intrusion detection system for software defined networks. In *2017 seventh international conference on emerging security technologies (EST)* (pp. 138-143). IEEE.
7. Amouri, A., Alaparthy, V. T., & Morgera, S. D. (2020). A machine learning based intrusion detection system for mobile Internet of Things. *Sensors*, *20*(2), 461.
8. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Eai Endorsed Transactions on Security and Safety*, *3*(9), 21.
9. Khan, M. A., Khan, M. A., Jan, S. U., Ahmad, J., Jamal, S. S., Shah, A. A., ... & Buchanan, W. J. (2021). A deep learning-based intrusion detection system for MQTT enabled IoT. *Sensors*, *21*(21), 7016.
10. Rashid, A., Siddique, M. J., & Ahmed, S. M. (2020, February). Machine and deep learning based comparative analysis using hybrid approaches for intrusion detection system. In *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)* (pp. 1-9). IEEE.
11. Bertoli, G. D. C., Júnior, L. A. P., Saotome, O., Dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., ... & De Oliveira, J. M. P. (2021). An end-to-end framework for machine learning-based network intrusion detection system. *IEEE access*, *9*, 106790-106805.
12. Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. *Computational Intelligence and Neuroscience*, *2023*(1), 8981988.
13. Khan, M. A., & Kim, Y. (2021). Deep Learning-Based Hybrid Intelligent Intrusion Detection System. *Computers, Materials & Continua*, *68*(1).

Online ISSN 3007-3197
Print ISSN 3007-3189

14. Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *Ieee Access*, *11*, 80348-80391.
15. Hizal, S., Cavusoglu, U., & Akgun, D. (2024). A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet of Things*, *28*, 101336.
16. Gaber, T., Awotunde, J. B., Torky, M., Ajagbe, S. A., Hammoudeh, M., & Li, W. (2023). Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks. *Internet of Things*, *24*, 100977.
17. Mohammadian, H., Ghorbani, A. A., & Lashkari, A. H. (2023). A gradient-based approach for adversarial attack on deep learning-based network intrusion detection systems. *Applied Soft Computing*, *137*, 110173.
18. Wei, F., Li, H., Zhao, Z., & Hu, H. (2023). {xNIDS}: Explaining deep learning-based network intrusion detection systems for active intrusion responses. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4337-4354).
19. Kumar, G., Thakur, K., & Ayyagari, M. R. (2020). MLEsIDSs: machine learning-based ensembles for intrusion detection systems—a review: G. Kumar et al. *The Journal of Supercomputing*, *76*(11), 8938-8971.
20. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, *9*(20), 4396.
21. Karatas, G., Demir, O., & Sahingoz, O. K. (2018, December). Deep learning in intrusion detection systems. In *2018 international congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT)* (pp. 113-116). IEEE.
22. Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustainable Cities and Society*, *61*, 102324.
23. Apruzzese, G., Pajola, L., & Conti, M. (2022). The cross-evaluation of machine learning-based network intrusion detection systems. *IEEE Transactions on Network and Service Management*, *19*(4), 5152-5169.
24. Idrissi, I., Azizi, M., & Moussaoui, O. (2020, October). IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. In *2020 Fourth international conference on intelligent computing in data sciences (ICDS)* (pp. 1-10). IEEE.
25. Wu, Y., Zou, B., & Cao, Y. (2024). Current status and challenges and future trends of deep learning-based intrusion detection models. *Journal of Imaging*, *10*(10), 254.
26. Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, *10*, 100053.
27. Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alexandria Engineering Journal*, *81*, 371-383.
28. Zeng, Y., Qiu, M., Zhu, D., Xue, Z., Xiong, J., & Liu, M. (2019, May). DeepVCM: A deep learning based intrusion detection method in VANET. In *2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing,(HPSC) and IEEE intl*

Online ISSN 3007-3197
Print ISSN 3007-3189

conference on intelligent data and security (IDS) (pp. 288-293). IEEE.