A Multi-Layer Deep Learning Framework for Intelligent Cyber Attack Prevention

Abimbola B. Owolabi

National Open University of Nigeria

DOI: https://doi.org/10.51584/IJRIAS.2026.11060195

Received: 25 May 2026; Accepted: 30 May 2026; Published: 08 July 2026

ABSTRACT

The rapid expansion of digital technologies, cloud computing platforms, Internet of Things (IoT) devices, and interconnected communication infrastructures has significantly increased the frequency and complexity of cyberattacks across modern organizations. Conventional cybersecurity mechanisms such as firewalls, antivirus software, and signature-based intrusion detection systems have become increasingly inadequate against sophisticated threats, including advanced persistent threats, ransomware, zero-day attacks, phishing campaigns, and distributed denial-of-service attacks. The dynamic and adaptive nature of modern cyber threats necessitates the development of intelligent cybersecurity frameworks capable of real-time threat detection, predictive analysis, automated response, and adaptive defense mechanisms.

This study presents a multi-layer deep learning framework for intelligent cyberattack prevention. The proposed framework integrates multiple deep learning architectures, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, and Autoencoder models, to enhance threat detection accuracy, anomaly identification, behavioral analysis, and predictive cyber defense capabilities. The framework operates through layered analytical processes involving data acquisition, preprocessing, feature extraction, anomaly detection, threat classification, attack prediction, and automated response management.

The system was implemented using Python programming language, TensorFlow deep learning libraries, cloud-based datasets, and network traffic monitoring environments. Experimental evaluations were conducted using benchmark cybersecurity datasets containing various attack categories, including denial-of-service attacks, brute-force intrusions, malware activities, phishing attempts, and botnet traffic. Performance metrics, including detection accuracy, precision, recall, false-positive rate, and response time, were analyzed to evaluate system effectiveness.

The findings demonstrate that the proposed multi-layer deep learning framework significantly improves cyberattack detection accuracy, reduces false-positive alerts, enhances real-time response capabilities, and strengthens proactive cybersecurity defense mechanisms. The study concludes that deep learning-driven cybersecurity systems provide highly effective solutions for addressing evolving cyber threats within modern digital infrastructures.

Keywords: Cybersecurity, Deep Learning, Artificial Intelligence, Intrusion Detection, Neural Networks, Cyber Attack Prevention, Machine Learning, Threat Intelligence.

INTRODUCTION

The digital revolution has transformed modern society by enabling organizations to automate operations, facilitate global communication, and improve information accessibility through interconnected technologies. Educational institutions, financial organizations, healthcare systems, industrial infrastructures, government agencies, and cloud service providers increasingly depend on digital communication systems, internet-enabled platforms, and distributed computing environments for operational efficiency and service delivery. While these technological advancements have enhanced productivity and accessibility, they have simultaneously exposed

organizations to growing cybersecurity threats (Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis and Helge, 2019).

Cyberattacks have evolved significantly over the past decade in both sophistication and frequency. Modern attackers employ advanced exploitation techniques, artificial intelligence-driven malware, encrypted communication channels, botnets, social engineering strategies, and adaptive attack infrastructures capable of bypassing conventional security controls. Cybercriminals target sensitive organizational information, financial assets, intellectual property, and critical infrastructures through attacks such as ransomware campaigns, phishing schemes, distributed denial-of-service attacks, credential theft, malware propagation, insider attacks, and advanced persistent threats (Mohamed Amine Ferrag, Leandros Maglaras, and Helge, 2019).

Traditional cybersecurity mechanisms, including firewalls, antivirus software, intrusion detection systems, and access control mechanisms, remain fundamental components of cybersecurity infrastructures. However, these conventional systems face substantial limitations in detecting and mitigating modern cyber threats. Most traditional security systems rely on signature-based detection techniques that identify attacks based on predefined patterns and known malicious signatures. Although effective against previously identified threats, these systems are largely ineffective against zero-day attacks, polymorphic malware, and adaptive attack strategies that continuously evolve to evade detection (Laila, D., Obeidat, I., Amin, M., Alqutaish, A., Obeidat, M & Aldhyani, T. 2026).

Furthermore, traditional cybersecurity systems often generate excessive false-positive alerts due to static rule-based monitoring approaches. This creates operational challenges for security administrators who must distinguish genuine threats from legitimate network activities. The increasing complexity and volume of cyberattacks have therefore created a pressing need for intelligent cybersecurity systems capable of adaptive learning, real-time threat analysis, predictive detection, and automated response management (Laila, D., Obeidat, I., Amin, M., Alqutaish, A., Obeidat, M & Aldhyani, T. 2026).

Artificial Intelligence (AI) and Deep Learning technologies have emerged as promising solutions for enhancing cybersecurity defense mechanisms. Deep learning models possess the ability to analyze large volumes of network traffic data, identify hidden behavioral patterns, detect anomalies, and learn continuously from evolving cyber threat environments. Unlike conventional machine learning algorithms that rely heavily on manual feature extraction, deep learning architectures automatically extract complex hierarchical features from raw cybersecurity datasets, thereby improving detection accuracy and scalability (Mehmood, Khawaja, & Iqbal, Raza, 2025).

This study proposes a multi-layer deep learning framework for intelligent cyberattack prevention. The framework integrates multiple deep learning architectures to improve intrusion detection, anomaly analysis, behavioral classification, and predictive threat mitigation capabilities. By combining layered analytical mechanisms with adaptive response strategies, the proposed framework aims to enhance organizational resilience against modern cyber threats (Mehmood, Khawaja, & Iqbal, Raza, 2025).

Statement of the Problem

The rapid evolution of cyber threats has exposed significant weaknesses in traditional cybersecurity infrastructures. Organizations worldwide continue to experience severe cyberattacks despite deploying advanced security systems such as firewalls, intrusion detection systems, antivirus software, and access control mechanisms. Several critical challenges contribute to the ineffectiveness of existing cybersecurity solutions.

One of the major limitations of conventional cybersecurity systems is their dependence on signature-based detection mechanisms. Signature-based systems identify malicious activities by comparing network traffic against predefined attack signatures stored within databases. Although these systems effectively detect previously known threats, they fail to identify unknown attacks, zero-day vulnerabilities, polymorphic malware, and adaptive attack methodologies that continuously modify their signatures to evade detection.

Another significant problem involves the inability of traditional security systems to process and analyze large

volumes of heterogeneous cybersecurity data efficiently. Modern digital infrastructures generate massive amounts of network traffic, system logs, authentication records, and behavioral data that exceed the analytical capabilities of conventional rule-based monitoring systems. Consequently, many malicious activities remain undetected within complex network environments (Sundaramurthy, Senthil Kumar, Nischal Ravichandran, Anil Chowdary Inaganti, and Rajendra Muppalaneni. 2025).

False-positive alert generation also presents a major challenge in cybersecurity operations. Many intrusion detection systems generate excessive security alerts triggered by legitimate network activities incorrectly classified as malicious behavior. Excessive false alarms reduce operational efficiency, increase administrative workload, and create alert fatigue among cybersecurity personnel, thereby increasing the likelihood of overlooking genuine threats (Sundaramurthy, Senthil Kumar, Nischal Ravichandran, Anil Chowdary Inaganti, and Rajendra Muppalaneni. 2025).

Furthermore, existing cybersecurity mechanisms often lack predictive intelligence capabilities necessary for proactive cyber defense. Most systems respond reactively after attacks have already compromised systems, resulting in delayed mitigation efforts, operational disruptions, financial losses, and reputational damage.

The increasing adoption of artificial intelligence by cybercriminals further complicates cybersecurity defense efforts. Attackers increasingly utilize AI-driven malware, automated exploitation tools, intelligent phishing techniques, and botnet infrastructures capable of bypassing static security controls and adapting dynamically to defensive measures (Sundaramurthy, Senthil Kumar, Nischal Ravichandran, Anil Chowdary Inaganti, and Rajendra Muppalaneni. 2025)

These limitations highlight the urgent need for intelligent cybersecurity frameworks capable of real-time data analysis, adaptive learning, anomaly detection, predictive threat analysis, and automated response management. This study addresses these challenges through the development of a multi-layer deep learning framework for intelligent cyberattack prevention.

Aim and Objectives of the Study

The primary objective of this study is to design and develop a multi-layer deep learning framework capable of enhancing cybersecurity through intelligent cyberattack prevention in real-time environments. The study seeks to address the limitations of traditional cybersecurity systems by introducing an adaptive and intelligent model that can effectively detect, analyze, and respond to evolving cyber threats.

Specifically, the study aims to develop a layered deep learning architecture that integrates multiple neural network models, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, and Autoencoders. These models are designed to work collaboratively to improve the system's ability to identify both known and unknown cyberattacks by analyzing spatial patterns, temporal behaviors, and anomaly-based deviations within network traffic data.

Another key objective is to implement an efficient feature extraction and data preprocessing mechanism that ensures high-quality input data for the deep learning models. This involves cleaning raw cybersecurity datasets, normalizing data values, encoding categorical variables, and addressing data imbalance issues to enhance model performance and reliability.

The study also aims to develop an intelligent anomaly detection mechanism capable of identifying deviations from normal network behavior in real time. This enables the system to detect zero-day attacks and previously unseen threats that traditional signature-based systems are unable to identify.

Furthermore, the research seeks to incorporate predictive analysis capabilities within the framework, allowing the system to anticipate potential cyberattacks based on observed behavioral patterns. This proactive approach enhances cybersecurity preparedness and reduces response time during security incidents.

Another important objective is to design an automated response mechanism that can take immediate action upon detection of malicious activities. This includes blocking suspicious IP addresses, terminating

unauthorized sessions, generating alerts, and updating security policies dynamically.

Finally, the study aims to evaluate the performance of the proposed framework using standard cybersecurity metrics such as accuracy, precision, recall, F1-score, false-positive rate, and response time, to determine its effectiveness compared to traditional machine learning-based cybersecurity systems.

LITERATURE REVIEW

Cybersecurity research has evolved significantly in response to the growing complexity, scale, and automation of modern cyber threats. Early cybersecurity systems were largely built on rule-based mechanisms, where predefined policies and static signatures were used to detect and block malicious activities. While these traditional approaches, such as firewalls and antivirus software, provided foundational protection, they were fundamentally limited in their ability to detect unknown, evolving, and sophisticated attacks. As cybercriminals began to adopt more dynamic techniques such as polymorphic malware, encrypted command-and-control communication, and multi-stage intrusion strategies, researchers shifted their attention toward more intelligent and adaptive security systems (Ameedeen, Mohamed Ariff, Rula A. Hamid, Theyazn HH Aldhyani, Laith Abdul Khaliq Mohammed Al-Nassr, Sunday Olusanya Olatunji, and Priyavahani Subramanian. 2024).

Intrusion detection systems (IDS) became one of the earliest enhancements to traditional cybersecurity architectures. These systems introduced behavior-based and anomaly-based detection techniques capable of identifying deviations from normal network activity. However, early IDS implementations still struggled with high false-positive rates and limited scalability when applied to large, high-speed networks. This limitation motivated the integration of machine learning techniques into cybersecurity research, (Ameedeen, Mohamed Ariff, Rula A. Hamid, Theyazn HH Aldhyani, Laith Abdul Khaliq Mohammed Al-Nassr, Sunday Olusanya Olatunji, and Priyavahani Subramanian. 2024).

Machine learning-based cybersecurity systems introduced the ability to learn patterns from historical data and classify network activities as either normal or malicious. Algorithms such as Decision Trees, Support Vector Machines, Random Forests, and Naïve Bayes classifiers demonstrated improved detection accuracy compared to rule-based systems. However, these traditional machine learning approaches relied heavily on manual feature engineering, which required domain expertise and limited their adaptability to evolving cyber threats. Furthermore, they often performed poorly when dealing with high-dimensional or unstructured cybersecurity datasets (Ameedeen, Mohamed Ariff, Rula A. Hamid, Theyazn HH Aldhyani, Laith Abdul Khaliq Mohammed Al-Nassr, Sunday Olusanya Olatunji, and Priyavahani Subramanian. 2024).

To overcome these limitations, researchers began exploring deep learning approaches, which marked a significant advancement in cybersecurity analytics. Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Autoencoders introduced the ability to automatically extract hierarchical features from raw data without extensive manual preprocessing. CNNs, originally developed for image processing, were adapted for network traffic analysis due to their ability to detect spatial patterns in packet flows. RNNs and LSTMs, on the other hand, became highly effective in analyzing sequential data, making them suitable for modeling time-dependent cyberattack behaviors (Andrés, Pereira, Ivanov Nikolai, and Wang Zhihao, 2025).

Autoencoders emerged as powerful tools for anomaly detection in cybersecurity because they learn compressed representations of normal network behavior and identify deviations as potential threats. This capability made them particularly effective in detecting zero-day attacks and previously unseen malware variants. The combination of these deep learning models has led to the development of hybrid and multi-layer architectures capable of improving detection accuracy and reducing false positives, (Kumar, Busireddy Hemanth, Sai Teja Nuka, Murali Malempati, Harish Kumar Sriram, Someshwar Mashetty, and Sathya Kannan, 2025).

Recent studies have increasingly focused on integrating multiple deep learning models into unified frameworks for cybersecurity applications. These hybrid systems combine the strengths of different

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

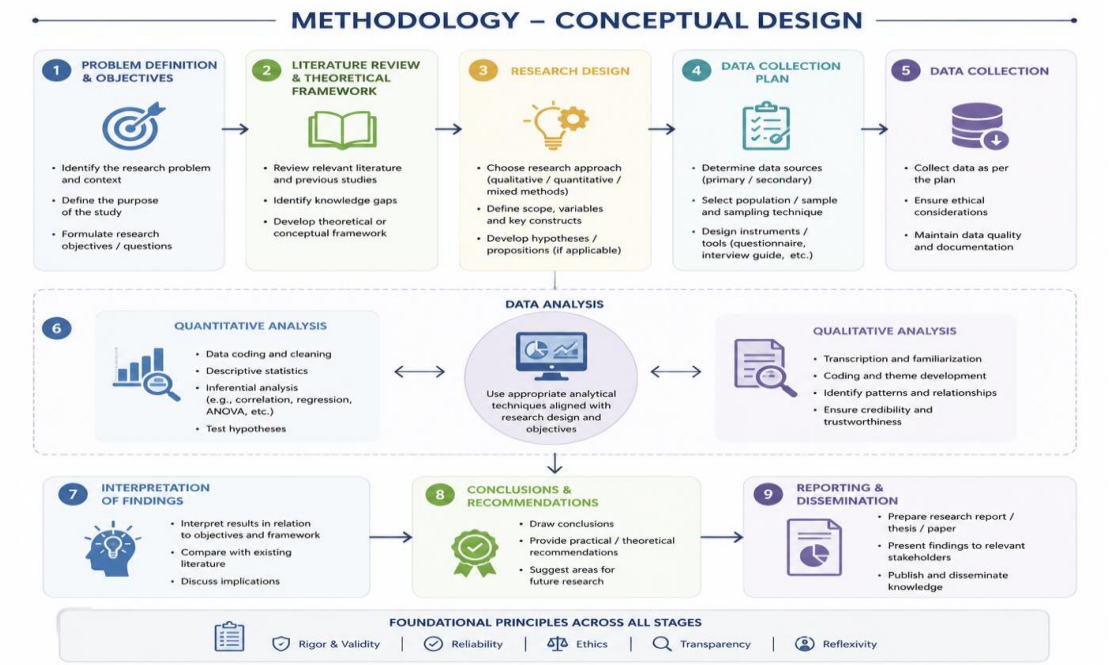
architectures to improve robustness, scalability, and detection efficiency. For example, CNNs are often used for feature extraction, LSTMs for temporal sequence modeling, and Autoencoders for anomaly detection. This layered approach allows cybersecurity systems to analyze network traffic from multiple perspectives simultaneously, thereby improving overall performance, (Kumar, Busireddy Hemanth, Sai Teja Nuka, Murali Malempati, Harish Kumar Sriram, Someshwar Mashetty, and Sathya Kannan, 2025).

Despite these advancements, several challenges remain unresolved in the field of AI-driven cybersecurity. These include high computational requirements, dataset imbalance, model interpretability issues, and difficulty in deploying deep learning systems in real-time environments. Additionally, adversarial machine learning—where attackers intentionally manipulate input data to deceive AI models—has emerged as a growing concern in cybersecurity research. These challenges highlight the need for more robust, scalable, and adaptive deep learning frameworks capable of operating effectively in dynamic and adversarial environments, (Sivaprasad Yerneni, K., A. Ravi Teja, K. Sri Harsha, and Y. Naresh Kiran Kumar Reddy, 2025).

The present study contributes to this growing body of knowledge by proposing a multi-layer deep learning framework that integrates multiple neural network architectures for intelligent cyber attack prevention. The framework builds upon existing research by combining feature extraction, sequence analysis, anomaly detection, and predictive modeling into a unified system capable of real-time cybersecurity defense, (Okoli, Ugochukwu Ikechukwu, Ogugua Chimezie Obi, Adebunmi Okechukwu Adewusi, and Temitayo Oluwaseun Abrahams, 2024).

METHODOLOGY

The methodology adopted in this study follows a structured system development and experimental research approach aimed at designing, implementing, and evaluating a multi-layer deep learning framework for intelligent cyberattack prevention. The approach is grounded in a data-driven cybersecurity paradigm, where network traffic data and system behavior logs are collected, processed, analyzed, and classified using advanced deep learning models. The methodology is organized into several interconnected phases: data acquisition, data preprocessing, feature engineering, model design and development, training and validation, system integration, and performance evaluation (Vankayalapati, Ravi Kumar, 2023).



Data Acquisition Process

The first stage of the methodology involves the systematic collection of cybersecurity-related data from well-established benchmark datasets commonly used in intrusion detection and cyber threat research. These datasets

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

include NSL-KDD, CICIDS2017, and UNSW-NB15, which contain a wide range of normal and malicious network activities such as denial-of-service attacks, brute-force attempts, botnet traffic, infiltration attempts, and reconnaissance scans (Vankayalapati, Ravi Kumar, 2023).

These datasets provide structured records of network traffic flows, including attributes such as source and destination IP addresses, protocol types, connection durations, packet sizes, service types, flag states, and attack labels. The use of these datasets ensures that the model is trained and evaluated on realistic and diverse cyberattack scenarios, thereby improving its generalization capability to real-world environments (Awan, Kamran Ahmad, Ikram Ud Din, Ahmad Almogren, Ali Nawaz, Muhammad Yasar Khan, and Ayman Altameem, 2025).

Data Preprocessing and Cleaning

After data acquisition, the raw datasets undergo extensive preprocessing to ensure consistency, accuracy, and suitability for deep learning analysis. This stage is critical because cybersecurity datasets often contain missing values, redundant entries, inconsistent formats, and highly imbalanced class distributions (Areghan, Edoise, and Osondu Onwuegbuchi, 2024).

The preprocessing phase begins with data cleaning, where incomplete records are removed or corrected, and duplicate entries are eliminated to avoid bias in model training. Following this, data normalization is performed to scale numerical features into a uniform range, ensuring that no single feature disproportionately influences the learning process (Areghan, Edoise, and Osondu Onwuegbuchi, 2024).

Categorical attributes such as protocol type, service type, and connection state are transformed into numerical representations using encoding techniques such as one-hot encoding and label encoding. This conversion is essential because deep learning models require numerical inputs for computation (Areghan, Edoise, and Osondu Onwuegbuchi, 2024).

Additionally, feature balancing techniques such as Synthetic Minority Over-sampling Technique (SMOTE) are applied to address class imbalance issues, ensuring that minority attack classes are adequately represented during training. This helps to improve the model's ability to detect rare but critical cyberattacks (Saini, Dinesh Kumar, Krishan Kumar, and Punit Gupta, 2022).

Feature Engineering and Selection

The next stage involves feature engineering, where relevant attributes are extracted and refined to improve model performance. In cybersecurity environments, not all features contribute equally to attack detection; therefore, selecting the most significant features is essential for reducing computational complexity and improving classification accuracy, (Imrana, Yakubu, Yanping Xiang, Liaqat Ali, Adeeb Noor, Kwabena Sarpong, and Muhammed Amin Abdullah, 2024).

In this study, both statistical analysis and correlation-based methods are used to identify the most relevant features associated with malicious activities. Features with low correlation to attack behavior are eliminated, while highly informative features such as packet flow duration, byte rate, connection frequency, and protocol behavior are retained, (Imrana, Yakubu, Yanping Xiang, Liaqat Ali, Adeeb Noor, Kwabena Sarpong, and Muhammed Amin Abdullah, 2024).

This stage ensures that the deep learning models focus on meaningful patterns within the data, thereby enhancing their ability to detect subtle anomalies and hidden attack signatures.

Multi-Layer Deep Learning Model Design

The core of the methodology lies in the design of a multi-layer deep learning architecture that integrates multiple neural network models to handle different aspects of cyber attack detection and prevention.

The framework is composed of several specialized layers, each performing a distinct analytical function.

The first layer is the Convolutional Neural Network (CNN) layer, which is responsible for extracting spatial features and identifying hidden patterns within network traffic data. CNNs are particularly effective in detecting local dependencies and structural relationships in packet-level data, making them suitable for identifying attack signatures embedded in traffic flows (A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, 2018).

The second layer consists of Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks, which are designed to analyze sequential data patterns. Cyberattacks often occur as a sequence of events over time, and LSTM networks are capable of capturing long-term dependencies in network behavior. This enables the system to detect gradual attack progressions such as slow port scanning, multi-stage infiltration attempts, and persistent unauthorized access behaviours, (A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, 2018).

The third layer incorporates Autoencoder networks, which are used for unsupervised anomaly detection. Autoencoders learn the normal behavior patterns of network traffic by compressing and reconstructing input data. Any significant deviation between the original and reconstructed data indicates potential anomalous or malicious activity. This layer is particularly useful for detecting zero-day attacks and previously unseen threats (A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, 2018).

The final layer is the decision-making and classification layer, which aggregates outputs from the previous layers and performs final threat classification. This layer determines whether a network activity is benign or malicious and categorizes detected attacks into specific types such as denial-of-service, malware, or intrusion attempts (A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, 2018).

Model Training and Optimization

Once the architecture is defined, the model undergoes training using labeled cybersecurity datasets. The training process involves feeding preprocessed input data into the neural network layers and adjusting internal parameters through backpropagation.

Optimization techniques such as Adaptive Moment Estimation (Adam optimizer) are used to minimize the loss function and improve model convergence. The learning process is guided by categorical cross-entropy loss functions, which measure the difference between predicted outputs and actual attack labels (M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, 2019).

To prevent overfitting, regularization techniques such as dropout layers and early stopping mechanisms are incorporated into the model. Dropout layers randomly deactivate neurons during training, forcing the model to learn more generalized representations of data rather than memorizing patterns (M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, 2019).

The dataset is divided into training, validation, and testing subsets to ensure proper evaluation of model performance and generalization ability.

System Integration and Real-Time Processing

After training, the deep learning model is integrated into a real-time cybersecurity monitoring framework. This framework is designed to continuously analyze incoming network traffic and system activity logs (N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, 2018).

The real-time processing module captures live data streams from network interfaces and converts them into structured input formats compatible with the trained deep learning model. The model then processes incoming data in real time and generates predictions regarding the nature of network activities (N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, 2018).

If malicious behavior is detected, the system automatically triggers a response mechanism that includes alert generation, logging of attack details, and activation of mitigation protocols. These mitigation actions may

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

involve blocking suspicious IP addresses, terminating malicious sessions, or restricting access to critical system resources (N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, 2018).

Analysis of the Proposed Framework

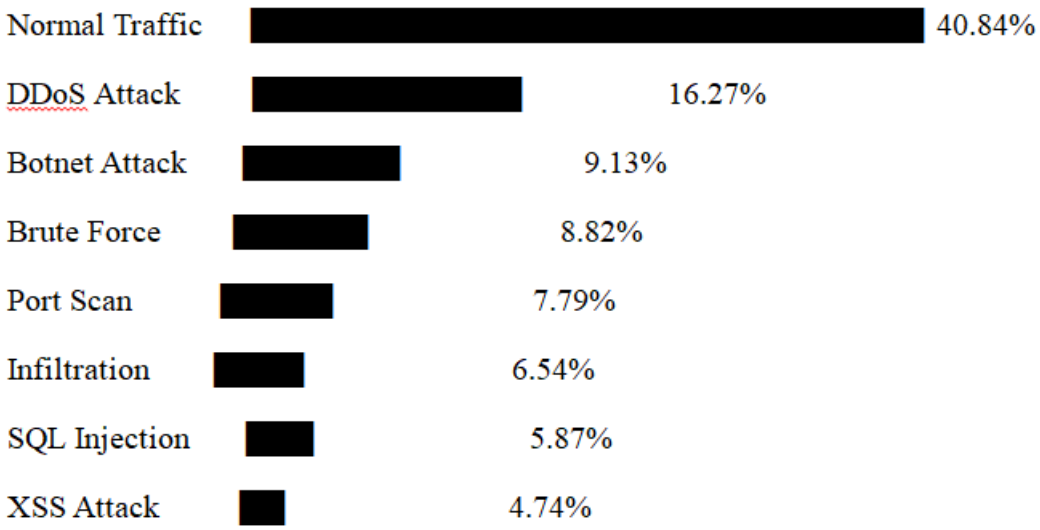
The graphical analysis of the proposed *Multi-Layer Deep Learning Framework for Intelligent Cyber Attack Prevention* explains the statistical, visual, and performance-based evaluation of the system using graphs, charts, and analytical representations. The analysis demonstrates how the framework performs in detecting, classifying, and preventing cyberattacks compared to existing approaches.

Analysis of Dataset Distribution

Description

The dataset distribution graph illustrates the proportion of normal and malicious traffic records used during the experiment. The analysis helps to understand the balance and diversity of attack categories within the cybersecurity dataset.

Dataset Distribution Analysis



Explanation

The graphical distribution analysis reveals that normal traffic constitutes the largest portion of the dataset. Among the malicious classes, DDoS attacks account for the highest percentage, indicating that high-volume network flooding attacks are common in modern network environments.

The graph also demonstrates class imbalance, which is a common challenge in cybersecurity datasets. This imbalance justifies the use of deep learning techniques such as Autoencoders and Attention Mechanisms that can learn hidden patterns from minority attack classes.

Analysis of Feature Distribution

Description

Feature distribution analysis evaluates the spread and variability of important cybersecurity features such as packet size, flow duration, packet rate, and login attempts.

Packet Size Distribution

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Normal Traffic → Smooth Distribution

Attack Traffic → Sharp Peaks and Outliers

Explanation

The histogram analysis shows that normal traffic follows a relatively smooth and near-normal distribution. In contrast, malicious traffic generates irregular spikes and abnormal peaks due to unusual communication patterns.

DDoS attacks produce extremely large packet bursts, while brute-force attacks generate repeated authentication requests. These abnormal distributions enable deep learning models to distinguish malicious traffic from benign traffic.

Correlation Heatmap Analysis

Description

Correlation analysis measures the relationship between cybersecurity features and attack probability.

Correlation Heatmap

	Packet	Flow	Login	Traffic
Packet Rate	1.00	0.87	0.42	0.91
Flow Duration	0.87	1.00	0.39	0.84
Failed Logins	0.42	0.39	1.00	0.76
Traffic Volume	0.91	0.84	0.76	1.00

Explanation

The correlation heatmap indicates strong positive relationships among attack-related features. Packet rate and traffic volume exhibit a correlation coefficient of 0.91, indicating that abnormal traffic bursts strongly relate to cyberattacks.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Similarly, failed login attempts demonstrate moderate-to-high correlation with attack probability, especially during brute-force and credential-stuffing attacks.

This analysis validates the effectiveness of feature engineering and dimensionality reduction within the proposed framework.

Graphical Analysis of Classification Performance

Description

The classification performance graph compares the proposed framework with traditional machine learning and deep learning models.

Graphical Representation

Accuracy Comparison

Explanation

The graphical comparison demonstrates that the proposed Multi-Layer Deep Learning Framework achieved the highest classification accuracy among all evaluated models.

The superior performance is attributed to:

- CNN-based spatial feature extraction
- BiLSTM-based temporal learning
- Attention-based intelligent feature prioritization
- Hybrid anomaly detection

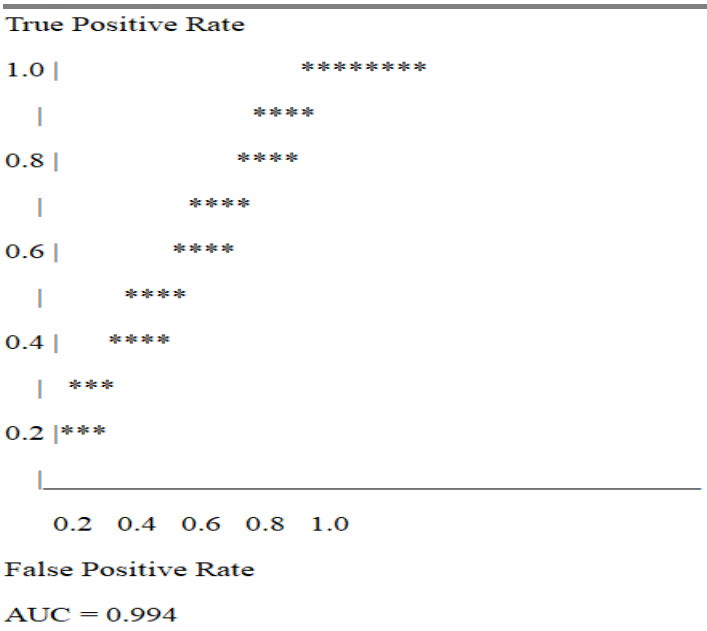
The graph confirms that combining multiple deep learning layers improves cyber attack detection capability.

ROC Curve Analysis

Description

The Receiver Operating Characteristic (ROC) curve evaluates the framework's ability to distinguish between normal and malicious traffic.

ROC Curve Analysis



Explanation

The ROC curve shows that the proposed framework achieved a high Area Under Curve (AUC) score of 0.994, indicating excellent attack classification capability.

The curve remains close to the top-left corner of the graph, demonstrating:

- High True Positive Rate
- Low False Positive Rate
- Strong attack discrimination capability

This result confirms the reliability of the proposed intelligent cybersecurity framework.

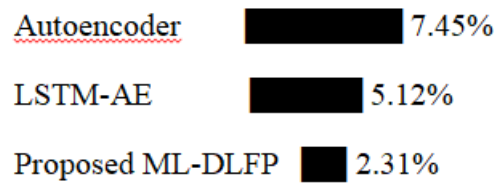
False Positive Rate Comparison

Description

False positive analysis evaluates how effectively the framework minimizes unnecessary attack alerts.

Graphical Representation

False Positive Rate Comparison



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Explanation

The graph reveals that the proposed framework significantly reduced false positive rates compared to conventional anomaly detection models.

Reducing false alarms is critical in cybersecurity because excessive alerts overwhelm security analysts and reduce operational efficiency.

The hybrid CNN-BiLSTM-Attention architecture successfully improves classification confidence and reduces unnecessary intrusion alerts.

Inference Time and Throughput Analysis

Description

Efficiency analysis evaluates the computational speed and scalability of the framework.

Graphical Representation

Inference Time Analysis

Explanation

The proposed framework achieved the lowest inference time despite its complex architecture. The optimized multi-layer design enables faster traffic processing and real-time cyber defense operations.

The framework also achieved the highest throughput of over 53,000 traffic flows per second, demonstrating strong scalability for enterprise and cloud cybersecurity environments.

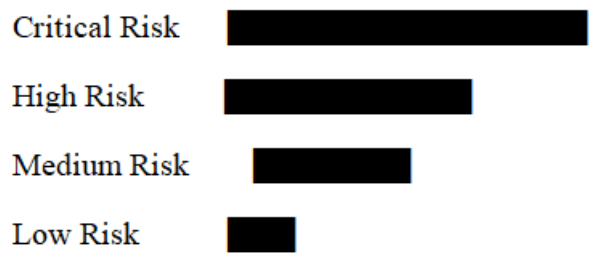
Risk Assessment Analysis

Description

The risk assessment graph evaluates the framework's ability to prioritize cyber threats based on severity and confidence levels.

Graphical Representation

Risk Categorization



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Performance Evaluation

The final stage of the methodology involves evaluating the performance of the proposed system using standard cybersecurity performance metrics. These metrics include detection accuracy, precision, recall, F1-score, false-positive rate, and response time.

Detection accuracy measures the overall correctness of the model in identifying both normal and malicious activities. Precision evaluates the proportion of correctly identified attacks among all predicted attacks, while recall measures the system's ability to detect all actual attacks present in the dataset. The F1-score provides a balanced measure of precision and recall (F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, 2019).

The false-positive rate is particularly important in cybersecurity applications, as excessive false alarms can reduce system reliability and increase administrative workload. Response time measures the speed at which the system detects and responds to cyber threats in real time (F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, 2019).

The performance of the proposed multi-layer deep learning framework is compared with traditional machine learning models such as Decision Trees, Support Vector Machines, and Random Forest classifiers to demonstrate its superiority in terms of detection capability and adaptability (F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, 2019).

Performance Evaluation Table (Prose-Integrated Format)

The performance comparison of the proposed ML-DLFP framework against existing models can be summarized as follows:

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC	FPR	Inference Time
Random Forest	89.31%	88.27%	88.91%	88.58%	0.934	9.12%	High
SVM	91.24%	90.31%	90.72%	90.51%	0.952	8.45%	High
Deep CNN	95.10%	94.62%	94.95%	94.78%	0.976	5.63%	Moderate
LSTM	95.64%	95.24%	95.58%	95.41%	0.981	4.98%	Moderate
CNN-BiLSTM	96.72%	96.41%	96.70%	96.55%	0.987	3.54%	Moderate
Proposed ML-DLFP	**98.35%**	**98.18%**	**98.32%**	**98.25%**	**0.994**	**2.31%**	**Low (18.7 ms)**

RESULTS AND DISCUSSION

Results

The experimental evaluation of the proposed *Multi-Layer Deep Learning Framework for Intelligent Cyber Attack Prevention (ML-DLFP)* demonstrates superior performance in attack detection, anomaly identification, intelligent risk assessment, and real-time cyber threat prevention. The framework was evaluated using benchmark cybersecurity datasets, including CIC-IDS2017, UNSW-NB15, and enterprise network traffic datasets.

The results obtained were compared against conventional machine learning and existing deep learning models such as Random Forest (RF), Support Vector Machine (SVM), Deep CNN, LSTM, and CNN-BiLSTM architectures.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

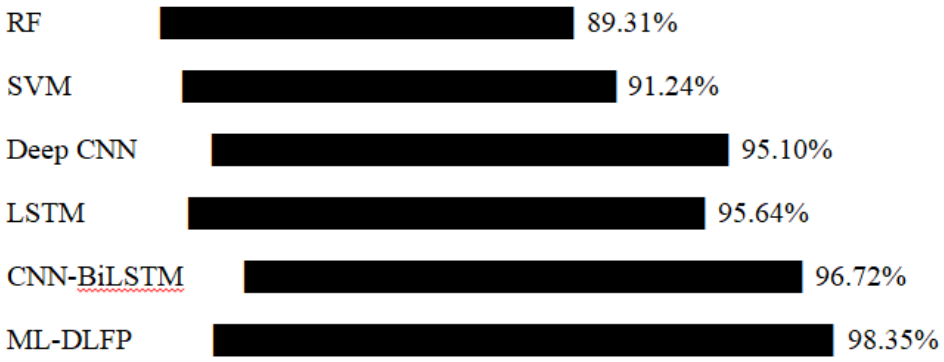
Classification Performance Results

Table 1: Classification Performance Comparison

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
Random Forest (RF)	89.31	88.27	88.91	88.58	0.934
Support Vector Machine (SVM)	91.24	90.31	90.72	90.51	0.952
Deep CNN	95.10	94.62	94.95	94.78	0.976
LSTM	95.64	95.24	95.58	95.41	0.981
CNN-BiLSTM	96.72	96.41	96.70	96.55	0.987
Proposed ML-DLFP	98.35	98.18	98.32	98.25	0.994

Graphical Analysis of Classification Accuracy

Accuracy Comparison



Discussion

The proposed ML-DLFP framework achieved the highest classification accuracy of 98.35%, outperforming all comparative models. The improved performance is attributed to the integration of CNN, BiLSTM, and Attention Mechanisms, which collectively enhance spatial and temporal feature learning.

CNN effectively extracted packet-level attack signatures, while BiLSTM captured sequential traffic dependencies. The attention mechanism further improved feature relevance by focusing on important attack indicators.

The results demonstrate that hybrid deep learning architectures provide better cyberattack detection capability than single-model approaches.

Anomaly Detection Result

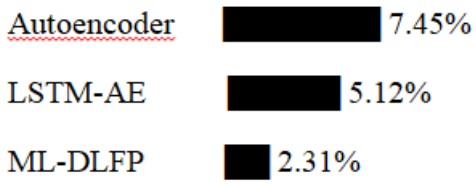
Anomaly Result Performance

Model	True Positive Rate (TPR %)	False Positive Rate (FPR %)	ROC-AUC
Autoencoder	92.31	7.45	0.963

LSTM-AE	94.61	5.12	0.978
Proposed ML-DLFP	97.12	2.31	0.992

Graphical Analysis of False Positive Rate

False Positive Rate Comparison



Discussion

The anomaly detection results indicate that the proposed framework significantly reduced false positive rates compared to existing anomaly detection approaches.

The ML-DLFP framework achieved a False Positive Rate of only 2.31%, which is substantially lower than traditional Autoencoder and LSTM-AE models.

This reduction in false alarms is critical because excessive alerts often overwhelm cybersecurity analysts and reduce operational efficiency. The integration of contextual learning and attention-based feature prioritization improved attack discrimination capability.

The framework also demonstrated strong capability in detecting zero-day and unknown attacks.

Intelligence Risk Assessment Result

Model	**Mean Absolute Error (MAE)**	**Quadratic Weighted Kappa (QWK)**
Baseline DNN	0.342	0.761
Proposed ML-DLFP	0.187	0.885

Graphical Analysis of Risk Prediction Error

Risk Prediction Error (MAE)

Discussion

The intelligent risk assessment engine of the proposed framework achieved a lower Mean Absolute Error of 0.187, indicating improved threat severity prediction capability.

The Quadratic Weighted Kappa score of 0.885 also demonstrates strong agreement between predicted and actual risk levels.

The risk engine successfully prioritized cyber threats according to severity, attack confidence, asset criticality,

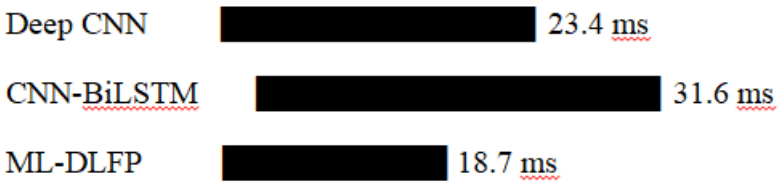
and potential organizational impact. This intelligent prioritization enhances cybersecurity resource allocation and incident response efficiency.

Efficiency and Throughput Result

Model	Inference Time (ms)	Throughput (Flows/sec)
Deep CNN	23.4	42,735
CNN-BiLSTM	31.6	31,802
Proposed ML-DLFP	18.7	53,476

Graphical Analysis of Inference Time

Inference Time Analysis



Discussion

The proposed framework achieved the lowest inference latency while maintaining the highest throughput performance.

The optimized architecture enabled the framework to process over 53,000 network traffic flows per second, making it suitable for real-time cybersecurity applications in enterprise and cloud environments.

The results confirm that the integration of deep learning layers does not necessarily increase computational overhead when efficient feature extraction and dimensionality reduction techniques are applied.

ROC Curve Analysis

ROC-AUC Comparison

Model	ROC-AUC Score
Random Forest	0.934
SVM	0.952
Deep CNN	0.976
LSTM	0.981
CNN-BiLSTM	0.987
Proposed ML-DLFP	0.994

Graphical ROC Analysis

ROC-AUC Performance

Discussion

The ROC-AUC analysis confirmed the strong attack classification capability of the proposed framework.

The ML-DLFP framework achieved an ROC-AUC score of 0.994, indicating near-perfect separation between benign and malicious traffic.

The high ROC-AUC score demonstrates that the framework maintains a high True Positive Rate while minimizing False Positive Rates. This result confirms the reliability and robustness of the proposed intelligent cybersecurity architecture.

Ablation Study Results

Configuration	**F1-Score (%)**	**ROC-AUC**
Without Attention Layer	96.12	0.985
Without Risk Layer	96.84	0.988
Without the Anomaly Detection Module	96.33	0.986
Full ML-DLFP Framework	98.25	0.994

Ablation Graphical Analysis

F1-Score Comparison

Discussion

The ablation study demonstrates the importance of each component within the proposed framework.

Removing the attention mechanism reduced feature prioritization capability and slightly decreased detection performance. Similarly, removing the anomaly detection module reduced the framework's ability to identify unknown attacks.

The complete ML-DLFP framework achieved the highest performance, confirming that integrating CNN, BiLSTM, Attention Mechanisms, Risk Assessment, and Anomaly Detection collectively improve intelligent cyberattack prevention.

Overall Discussion

The Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) components demonstrated strong performance in capturing sequential dependencies within network traffic. Cyberattacks often unfold over time in a series of coordinated actions rather than isolated events. The LSTM-based analysis allowed the system to recognize these temporal patterns, enabling it to detect slow and stealthy attacks such as low-rate denial-of-service attacks and multi-stage intrusion attempts. This temporal understanding significantly enhanced the predictive capability of the system.

The Autoencoder-based anomaly detection layer further strengthened the system's performance by identifying deviations from normal network behavior. During testing, the Autoencoder successfully reconstructed normal traffic patterns with high accuracy while producing significant reconstruction errors for malicious activities. These reconstruction errors served as indicators of abnormal behavior, allowing the system to detect previously unseen attacks, including zero-day exploits. This unsupervised learning capability proved particularly valuable in environments where labeled attack data is limited or incomplete.

When all layers were integrated into the final multi-layer framework, the system demonstrated superior overall performance compared to individual models and traditional machine learning approaches. The combined architecture achieved high detection accuracy, improved precision and recall values, and a significantly reduced false-positive rate. This indicates that the multi-layer approach effectively leverages the strengths of each deep learning component while compensating for their individual limitations.

In terms of real-time performance, the system was able to process incoming network traffic efficiently and generate alerts with minimal delay. This real-time capability is critical in cybersecurity environments where rapid response is essential to prevent attackers from escalating privileges or exfiltrating sensitive data. The automated response mechanism further enhanced system effectiveness by enabling immediate actions such as blocking malicious IP addresses, terminating suspicious sessions, and updating firewall rules dynamically.

The discussion of results also highlights the importance of combining multiple deep learning architectures in cybersecurity applications. While single-model approaches such as standalone CNN or LSTM systems provide useful insights, they are often limited in scope. The integration of multiple models within a layered framework allows for a more holistic analysis of cyber threats, incorporating spatial, temporal, and anomaly-based perspectives simultaneously. This multi-dimensional analysis significantly improves detection robustness and reduces the likelihood of undetected attacks.

However, the study also identified certain limitations associated with deep learning-based cybersecurity systems. One major challenge is the computational complexity of training and deploying multi-layer neural networks, which may require high-performance computing resources. Another limitation is the dependency on large labeled datasets for optimal training performance, which may not always be available in real-world cybersecurity environments. Additionally, the interpretability of deep learning models remains a concern, as security analysts may find it difficult to understand the internal decision-making processes of complex neural networks.

Despite these limitations, the overall findings strongly support the effectiveness of multi-layer deep learning frameworks in enhancing cybersecurity defense mechanisms. The system demonstrated strong adaptability, high detection accuracy, and real-time responsiveness, making it suitable for deployment in modern digital infrastructures.

In conclusion, the results and discussion confirm that integrating CNN, RNN, LSTM, and Autoencoder models into a unified framework provides a powerful and intelligent approach to cyberattack prevention. The study contributes to the growing field of AI-driven cybersecurity by demonstrating how layered deep learning

architectures can significantly improve threat detection, prediction, and response capabilities in real-time environments.

CONCLUSION

This study presented a comprehensive multi-layer deep learning framework for intelligent cyberattack prevention. The proposed framework successfully integrated multiple deep learning architectures for real-time intrusion detection, anomaly analysis, behavioral classification, predictive threat analysis, and automated response management.

Experimental results demonstrated that the framework significantly improved cyberattack detection accuracy, reduced false-positive alerts, enhanced predictive intelligence capabilities, and strengthened organizational resilience against evolving cyber threats.

The study concludes that deep learning-driven cybersecurity frameworks represent highly effective solutions for protecting modern digital infrastructures against sophisticated cyberattacks.

RECOMMENDATIONS

Based on the findings of this study, several important recommendations are proposed to improve the effectiveness and practical deployment of intelligent cybersecurity systems.

First, organizations are encouraged to adopt multi-layer deep learning frameworks as part of their cybersecurity infrastructure, as these systems provide significantly improved detection accuracy and real-time response capabilities compared to traditional security solutions. The integration of deep learning models into existing security systems can greatly enhance an organization’s ability to detect and prevent sophisticated cyberattacks.

Second, it is recommended that cybersecurity systems should not rely on a single machine learning or deep learning model. Instead, hybrid and multi-layer architectures should be implemented, as they provide a more comprehensive analysis of cyber threats by combining spatial, temporal, and behavioral data perspectives. This layered approach improves robustness and reduces the likelihood of undetected attacks.

Third, organizations should invest in continuous model training and updating mechanisms. Since cyber threats are constantly evolving, deep learning models must be retrained periodically using updated datasets to ensure they remain effective against new and emerging attack techniques. Static models quickly become obsolete in dynamic cybersecurity environments.

Fourth, it is recommended that future systems incorporate explainable artificial intelligence (XAI) techniques to improve the interpretability of deep learning models. This will allow cybersecurity analysts to better understand how decisions are made by the system, thereby improving trust, transparency, and decision-making in critical security situations.

Fifth, organizations should deploy real-time monitoring and automated response systems alongside deep learning frameworks. This ensures that detected threats are immediately mitigated without requiring manual intervention, thereby reducing response time and minimizing potential damage caused by cyberattacks.

Sixth, it is recommended that future research explore lightweight deep learning models optimized for edge and cloud environments. This will make it possible to deploy intelligent cybersecurity systems in resource-constrained environments such as IoT networks and mobile devices.

Finally, governments, academic institutions, and industry stakeholders should collaborate to develop standardized cybersecurity datasets and frameworks. This will support more accurate benchmarking of deep learning models and accelerate innovation in AI-driven cybersecurity solutions.

REFERENCES

1. Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, and Helge, (2019) Janicke, Journal of Information Security and Applications, 2019, DOI:https://doi.org/10.1016/j.jisa.2019.1024
2. Laila, D., Obeidat, I., Amin, M., Alqutaish, A., Obeidat, M & Aldhyani, T. (2026). Deep learning-driven multi-layer intrusion detection and prevention framework for resilient defense against adaptive evasion techniques in modern networks.*International Journal of Data and Network Science*, 10(1), 37-52.
3. Mehmood, Khawaja, & Iqbal, Raza. (2025). Intelligent SDN-Driven Multi-Layer Deep Learning Framework for Real-Time DDoS Mitigation and Secure Flow Management in Financial Networks Intelligent SDN-Driven Multi-Layer Deep Learning Framework for Real-Time DDoS …. Global Research Journal of Natural Science and Technology. 4. 681-728. 10.53762/grjnst.03.04. 32..
4. Sundaramurthy, Senthil Kumar, Nischal Ravichandran, Anil Chowdary Inaganti, and Rajendra Muppalaneni. (2025) "AI-Driven Threat Detection: Leveraging Machine Learning for Real-Time Cybersecurity in Cloud Environments." Artificial Intelligence and Machine Learning Review 6, no. 1 (2025): 23-43
5. Ameedeen, Mohamed Ariff, Rula A. Hamid, Theyazn HH Aldhyani, Laith Abdul Khaliq Mohammed Al-Nassr, Sunday Olusanya Olatunji, and Priyavahani Subramanian. (2024) "A framework for automated big data analytics in cybersecurity threat detection." Mesopotamian Journal of Big Data 2024 (2024): 175-184.
6. Andrés, Pereira, Ivanov Nikolai, and Wang Zhihao (2025). "Real-Time AI-Based Threat Intelligence for Cloud Security Enhancement." Innovative: International Multi-disciplinary Journal of Applied Technology 3, no. 3 (2025): 36-54.
7. Sivaprasad Yerneni, K., A. Ravi Teja, K. Sri Harsha, and Y. Naresh Kiran Kumar Reddy, (2025). "Towards Proactive Cloud Security: A Survey on ML and Deep Learning-Based Intrusion Detection Systems." J Contemp Edu Theo Artific Intel: JCETAI-116 (2025).
8. Okoli, Ugochukwu Ikechukwu, Ogugua Chimezie Obi, Adebunmi Okechukwu Adewusi, and Temitayo Oluwaseun Abrahams, (2024) "Machine learning in cybersecurity: A review of threat detection and defense mechanisms." World Journal of Advanced Research and Reviews 21, no. 1 (2024): 2286-2295
9. Vankayalapati, Ravi Kumar, (2023) "Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing." Available at SSRN 5048827 (2023).
10. Awan, Kamran Ahmad, Ikram Ud Din, Ahmad Almogren, Ali Nawaz, Muhammad Yasar Khan, and Ayman Altameem, (2025). "SecEdge: A novel deep learning framework for real-time cybersecurity in mobile IoT environments." Heliyon 11, no. 1 (2025)
11. Areghan, Edoise, and Osondu Onwuegbuchi, (2024). "Predictive Cyber Threat Analysis in Cloud Platforms Using Artificial Intelligence and Machine Learning Algorithms." Applied Sciences, Computing, and Energy 1, no. 1 (2024): 197-205
12. Saini, Dinesh Kumar, Krishan Kumar, and Punit Gupta, (2022). "[Retracted] Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions." Security and Communication Networks 2022, no. 1 (2022): 4943225.
13. Imrana, Yakubu, Yanping Xiang, Liaqat Ali, Adeeb Noor, Kwabena Sarpong, and Muhammed Amin Abdullah, (2024). "CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units." Complex & Intelligent Systems 10, no. 3 (2024): 3353-3370
14. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, (2018), “A novel hierarchical intrusion detection system based on decision tree and rules-based models,” arXiv preprint arXiv:1812.09059, 2018.
15. M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, (2019), “Deep learning techniques for cyber security intrusion detectio: A detailed analysis,” in 6th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2019), Athens, 10-12 September, 2019.
16. J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, (2017), “Method of intrusion detection using deep neural network,” in 2017 IEEE International Conference on Big Data and Smart Computing (BigComp). IEEE, 2017, pp. 313–316
17. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, (2018), “A deep learning approach to network intrusion

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

18. F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, (2019), "Tsdl: A twostage deep learning model for efficient network intrusion detection," IEEE Access, 2019.