Transguard-RT:A Real-Time Transformer-Driven Intrusion Detection System Using Live Network Traffic Analytics

Mrs.Banuppriya P[1],Santhosh K[2],Kandasamy A[3],Sujth M[4], Vaitheeshwaran M[5]
[1]Assist prof, Dept of Computer science and Engineering
[2, 3, 4, 5] Dept of Computer science and Engineering
[1, 2, 3, 4, 5] Mahendra Institute of Engineering and Technology, Namakkal, TamilNadu, India

Abstract- *The rapid expansion of internet-based communication and interconnected digital infrastructures has significantly increased exposure to advanced cyber threats, including malware infiltration, phishing attempts, denial-of-service attacks, and unauthorized access. Traditional security mechanisms such as signature-based intrusion detection and rule-driven firewalls are often insufficient to identify evolving and previously unseen attack patterns, particularly in high-speed and complex network environments. To address these limitations, this research presents a real-time Intrusion Detection System that leverages live network traffic captured through NCAP- based monitoring and applies a Transformer-based deep learning architecture for intelligent threat detection. The proposed approach focuses on analyzing sequential dependencies and contextual relationships with in network traffic data using self-attention mechanisms, enabling effective identification of both known and unknown intrusion patterns. The system pre-processes captured traffic, extracts relevant features, and performs real-time classification of network behavior in to normalormalicious categories. Continuous monitoring ensures immediate detection and response to potential cyber threats, thereby enhancing overall network resilience. Performance evaluation is conducted using standard metrics such as accuracy, precision, recall, and F1-score, demonstrating strong detection capability and reliability. The outcomes indicate that the proposed research offers a scalable, adaptive, and efficient cyber security framework suitable for deployment in critical domains such as finance, healthcare, cloud environments, and enterprise networks, where real-time protection and intelligent threat analysis are essential.*

Keywords: Cloud computing, Cybersecurity, Deep learning, Intrusion detection system, Network traffic analysis, Real-time monitoring, Transformer model

I. INTRODUCTION

The increasing dependence on digital communication systems and interconnected network infrastructures has significantly elevated the risk of cyber threats across various domains. Modern attack techniques such as malware propagation, phishing campaigns, denial-of- service attacks, and unauthorized access attempts have become highly sophisticated and difficult to detect using conventional security mechanisms. Traditional intrusion detection approaches, particularly signature-based and rule-based systems, are limited in their ability to identify unknown or evolving attack patterns. These limitations highlight the necessity for intelligent and adaptive security frameworks capable of analyzing complex network behaviors in real time and providing proactive protection against emerging threats. This research introduces a real- time intrusion detection framework that leverages NCAP- based network traffic capture combined with a Transformer-driven deep learning model for enhanced threat detection. The system is designed to process live network packets, extract meaningful features, and analyze sequential dependencies within traffic data using self- attention mechanisms.

Figure 1: Intrusion detection

By focusing on contextual relationships rather than static patterns, the proposed approach improves detection accuracy for both known and previously unseen attacks. Real-time classification and continuous monitoring enable immediate identification of malicious activities, ensuring rapid response and improved network resilience. The outcomes demonstrate that this approach offers a scalable and intelligent solution for strengthening cybersecurity in critical environments such as cloud systems, financial networks, healthcare infrastructures, and enterprise communication platforms.

Problem statement

The increasing complexity of modern network environments has led to a rapid rise in sophisticated cyberattacks that are difficult to detect using traditional security mechanisms. Existing intrusion detection systems, particularly those based on signature-based and rule-based approaches, are limited to identifying known threats and fail to detect novel or evolving attack patterns. Additionally, many conventional machine learning models struggle to capture long-range dependencies and contextual relationships within high-speed network traffic, resulting in reduced detection accuracy and increased false alarms. Furthermore, most existing solutions are not designed for real-time analysis of live network streams, making them less effective in dynamic and large-scale environments. These limitations highlight the need for an intelligent and adaptive intrusion detection framework capable of processing real-time network traffic, identifying both known and unknown threats, and ensuring timely and accurate threat detection to enhance overall network security.

Dataset details

The dataset utilized in this research consists of real-time and benchmark network traffic data designed to represent both normal and malicious activities within a network environment. The data is captured through NCAP-based monitoring, which collects live packet-level information including source IP address, destination IP address, port numbers, protocol type, packet size, and flow duration. In addition to live traffic, standard intrusion detection benchmark datasets may also be considered to support model training and validation under diverse attack scenarios. The dataset undergoes preprocessing steps such as data cleaning, normalization, encoding of categorical features, and feature extraction to ensure compatibility with the Transformer-based model. The prepared dataset is structured into sequential formats to preserve temporal relationships within network flows, enabling effective learning of traffic behavior patterns for accurate intrusion detection.

Objectives

The objective of this research is to develop a real-time intrusion detection framework capable of identifying both known and unknown cyber threats by analyzing live network traffic captured through NCAP-based monitoring. The system aims to leverage a Transformer-based deep learning model to effectively learn complex patterns and long-range dependencies within network data for improved detection accuracy. Additionally, the research focuses on enhancing real-time classification of network traffic into normal and malicious categories, reducing false alarms, and ensuring timely threat identification. Another key objective is to design a scalable and adaptive cybersecurity solution that can operate efficiently in dynamic network environments such as cloud systems, enterprise networks, healthcare infrastructures, and financial platforms.

II. RELATED WORK

Tamara Al-Shurbaji, et al. [1] proposed a deep learning- based intrusion detection system focused on identifying IoT botnet attacks using advanced neural network architectures. The study highlights how deep learning models can effectively learn complex traffic patterns generated by botnets in IoT environments. The authors emphasize the limitations of traditional signature-based detection methods in handling large-scale IoT threats. The proposed approach demonstrates improved detection accuracy by automatically extracting relevant features from network traffic. It also reduces dependency on manual feature engineering, making the system more adaptive. The study discusses the importance of real-time detection for securing IoT ecosystems. Experimental results show enhanced performance compared to conventional methods. The work also explores scalability issues in IoT security systems. It highlights challenges related to computational overhead in deep models. The research contributes to strengthening intrusion detection in connected devices. It further supports the use of deep learning in cybersecurity applications. Overall, it establishes a strong foundation for AI-based intrusion detection systems. The study concludes that deep learning significantly improves botnet detection capabilities.

Nur Nadiah Mohd Yusof and Noor Suhana Sulaiman [2] provided a comprehensive review of cybersecurity attack detection datasets used in intrusion detection research. The study analyzes various publicly available datasets and their suitability for training machine learning models. It highlights the importance of dataset quality in improving detection accuracy. The authors discuss commonly used datasets such as KDD Cup 99, NSL-KDD, and CICIDS. The review identifies limitations such as outdated attack patterns and data imbalance issues. It emphasizes the need for modern, realistic datasets that reflect current cyber threats. The study also examines preprocessing techniques applied to IDS datasets. It highlights challenges in feature selection and data representation. The authors suggest that dataset diversity plays a key role in model generalization. The paper provides guidance for researchers selecting appropriate datasets. It also stresses the importance of continuous dataset updates. The study concludes that dataset quality directly impacts IDS performance. It serves as a valuable reference for dataset selection in intrusion detection research.

Hadeel M. Saleh, et al. [3] proposed a stochastic gradient descent-based intrusion detection system for wireless sensor networks. The research focuses on improving detection efficiency using machine learning optimization techniques. The study addresses security vulnerabilities in resource-constrained wireless environments. It highlights how stochastic gradient descent improves model training efficiency. The system is designed to detect various types of network attacks effectively. The authors compare their method with traditional machine learning approaches. Results show improved accuracy and reduced computational cost. The study emphasizes energy efficiency in wireless sensor networks. It also discusses scalability challenges in distributed environments. The proposed system demonstrates strong performance in real- time detection scenarios. The research highlights the importance of lightweight IDS models. It contributes to improving security in IoT and sensor-based networks. Overall, it shows the effectiveness of optimized learning algorithms for intrusion detection.

Muhammad Sajid, et al. [4] proposed a hybrid intrusion detection framework combining machine learning and deep learning techniques. The study aims to enhance detection accuracy by integrating multiple learning approaches. It focuses on improving feature extraction and classification performance. The hybrid model leverages strengths of both traditional ML and deep learning methods. The authors evaluate the system on benchmark datasets. Results show improved detection rates and reduced false positives. The study highlights challenges in balancing computational complexity and accuracy. It also discusses feature selection techniques for better performance. The proposed system demonstrates adaptability to different attack types. It provides a scalable solution for modern cybersecurity environments. The research emphasizes hybrid models as a promising direction. It contributes to improving robustness in intrusion detection systems. Overall, it supports multi- model integration for enhanced security.

A. E. M. Eljialy, et al. [5] proposed a deep learning-based intrusion detection framework using multiple feature selection methods. The study focuses on improving model performance through optimized feature engineering. It highlights the importance of selecting relevant network traffic attributes. The authors compare different feature selection techniques. The proposed framework enhances classification accuracy significantly. It reduces computational complexity by eliminating irrelevant features. The study evaluates performance on standard datasets. Results show improved detection efficiency and reduced false alarms. The authors emphasize deep learning adaptability in cybersecurity. The system demonstrates strong generalization capability. It also addresses challenges in high-dimensional data processing. The research contributes to improving IDS accuracy and efficiency. Overall, it highlights the role of feature selection in deep learning-based IDS.

İsa Avcı and Murat Koca [6] proposed a cybersecurity attack detection model using traditional machine learning techniques. The study evaluates algorithms such as Decision Tree, SVM, and Random Forest. It focuses on classifying network traffic into normal and malicious categories. The authors analyze the performance of different classifiers. Results indicate that ensemble methods provide better accuracy. The study highlights limitations of individual machine learning models. It emphasizes the importance of feature engineering. The proposed system is tested on benchmark datasets. It demonstrates moderate performance in detecting known attacks. The research discusses challenges in handling complex traffic patterns. It also identifies scalability limitations in large networks. The study concludes that machine learning remains effective but limited for advanced threats. It suggests the need for deep learning- based approaches.

Andrew McCarthy, et al. [7] proposed a hierarchical learning approach to defend against adversarial machine learning attacks in network traffic classification. The study addresses vulnerabilities in IDS models exposed to adversarial manipulation. It introduces layered learning techniques to improve robustness. The authors evaluate performance under adversarial conditions. Results show improved resistance to attack evasion techniques. The study highlights the importance of secure model design. It discusses challenges in adversarial environments. The proposed method enhances classification stability. It also improves detection reliability under attack scenarios. The research contributes to secure machine learning development. It emphasizes robustness as a key requirement in IDS design. Overall, it strengthens cybersecurity against adversarial threats. The study provides insights into resilient AI-based IDS systems.

Tao Yi, et al. [8] provided a comprehensive review of deep learning applications in network attack detection. The study analyzes various deep learning architectures used in IDS systems. It highlights CNN, RNN, and hybrid models. The authors discuss advantages of deep learning over traditional methods. It emphasizes automatic feature extraction capabilities. The review identifies challenges such as high computational cost and data imbalance. It also discusses real-time detection limitations. The study highlights the importance of scalable architectures. It reviews performance improvements in detection accuracy. The authors suggest future directions for research in deep learning IDS. The paper provides a broad overview of existing techniques. It emphasizes continuous evolution of cybersecurity models. Overall, it serves as a foundational survey for IDS research.

Ta Sowmya and E. A. Mary Anita [9] presented a comprehensive review of AI-based intrusion detection systems. The study explores machine learning and deep learning techniques used in cybersecurity. It categorizes IDS approaches based on learning methods. The authors discuss advantages of AI-driven systems over traditional IDS. It highlights challenges such as data imbalance and false alarms. The study reviews various classification algorithms. It emphasizes the importance of feature selection and preprocessing. The authors analyze performance metrics used in IDS evaluation. It also discusses real-time detection challenges. The paper identifies research gaps in AI-based IDS development. It suggests improvements in model scalability and adaptability. Overall, it provides a broad understanding of AI-based cybersecurity systems. It serves as a guide for future IDS research.

Md Mahbubur Rahman, et al. [10] proposed a survey on intrusion detection systems in IoT networks. The study focuses on security challenges in IoT environments. It analyzes different IDS architectures used in IoT. The authors highlight resource constraints in IoT devices. It discusses lightweight machine learning models for intrusion detection. The study reviews dataset challenges in IoT-based IDS. It emphasizes the importance of real- time detection. The authors identify scalability issues in large IoT networks. It also highlights energy efficiency requirements. The paper compares various IDS techniques. It suggests hybrid approaches for better performance. The study concludes that IoT security requires adaptive IDS solutions. It provides insights into future research directions in IoT cybersecurity.

III. EXISTING METHODLOGY

Existing intrusion detection systems primarily rely on signature-based and rule-based security mechanisms to identify malicious activities within network environments. These approaches operate by comparing incoming network traffic against a predefined database of attack signatures or security rules. Tools such as Snort and Suricata are widely used in this category due to their efficiency in detecting known threats. However, these systems are inherently limited as they can only identify previously documented attacks and are unable to detect new or evolving intrusion patterns. As a result, their effectiveness decreases significantly in modern dynamic networks where attack strategies are continuously changing. Another category of existing solutions includes traditional machine learning- based intrusion detection techniques such as Support Vector Machine, Decision Tree, Random Forest, Naïve Bayes, and K-Nearest Neighbor. These models improve detection capabilities by learning patterns from network traffic data instead of relying solely on predefined signatures. However, these approaches depend heavily on manual feature engineering and are often unable to capture complex, high-dimensional relationships present in real- world network traffic. Additionally, their performance degrades when handling large-scale or high-speed streaming data, making them less suitable for real-time intrusion detection scenarios. More recent approaches incorporate deep learning techniques such as Convolutional Neural Networks and Long Short-Term Memory networks to enhance detection accuracy. While these models provide better feature learning capabilities compared to traditional methods, they still face limitations in handling long-range dependencies efficiently and often require significant computational resources. Furthermore, many existing systems are trained and evaluated on static benchmark datasets rather than real-time network traffic, which reduces their applicability in practical deployment environments. These limitations highlight the need for a more advanced, adaptive, and real-time intrusion detection approach.

IV. PROPOSED METHODOLOGIES

The proposed research introduces a real-time intrusion detection framework designed to enhance cybersecurity by continuously monitoring live network traffic through NCAP-based packet capture. Unlike traditional approaches that depend on static datasets, this system operates in a dynamic environment where network packets are collected in real time and processed for immediate analysis. The captured data includes essential network attributes such as source and destination IP addresses, protocol information, port numbers, and traffic flow characteristics. This real- time acquisition ensures that the system is capable of responding to ongoing network activities without delay, making it suitable for modern high-speed communication infrastructures. The core intelligence of the proposed system is based on a

Transformer-based deep learning architecture, which is employed to analyze sequential network traffic data. The model utilizes self-attention mechanisms to effectively learn contextual relationships and long-range dependencies between network packets. This enables the system to identify complex intrusion patterns that may not be easily detectable using conventional machine learning or deep learning techniques. The Transformer model is trained to distinguish between normal and malicious traffic by learning behavioral patterns from labeled network data, thereby improving detection accuracy and adaptability. In addition, the proposed system integrates a real-time classification and alert generation mechanism to ensure immediate response to detected threats. Once network traffic is analyzed, the system classifies it as either benign or malicious and triggers instant alerts when suspicious activities are identified. These alerts are communicated through a monitoring interface and logged for further analysis and security auditing. The combination of real- time processing, Transformer-based intelligence, and automated alerting makes this research a scalable and robust solution for protecting critical infrastructures such as cloud environments, enterprise networks, financial systems, and healthcare platforms against evolving cyber threats.

METHODOLOGY

Data Collection and Network Traffic Capture

The methodology begins with real-time network traffic acquisition using NCAP-based monitoring tools that capture live packet streams from active network interfaces. The captured data includes essential attributes such as source IP address, destination IP address, protocol type, port numbers, packet size, and flow duration. This continuous data collection ensures that the system works in a dynamic environment rather than relying on static datasets. The raw traffic is temporarily stored and passed to the preprocessing stage for further refinement and analysis.

Data Preprocessing and Feature Engineering

In this stage, the collected raw network traffic is processed to remove noise, duplicate entries, and incomplete records. Categorical attributes such as protocol types are encoded into numerical formats to make them suitable for machine learning processing. Feature scaling and normalization techniques are applied to ensure uniformity across all input variables. Important features are selected or engineered to improve model performance while reducing computational complexity. The processed data is then structured into sequential form to preserve temporal dependencies within network flows.

Transformer-Based Model Development

The core of the methodology involves designing a Transformer-based deep learning model for intrusion detection. The model utilizes self-attention mechanisms to analyze relationships between different network traffic features and capture long-range dependencies effectively. Unlike traditional models, the Transformer processes data in parallel, improving computational efficiency and learning capability. The model is trained using labeled datasets containing both normal and malicious traffic patterns. Through iterative training, the model learns to distinguish subtle variations in network behavior associated with cyberattacks.

Training and Optimization Process

The training phase involves feeding the pre-processed sequential data into the Transformer model to learn intrusion patterns. Loss functions are optimized using gradient-based optimization techniques to minimize prediction errors. Hyperparameter tuning is performed to improve model accuracy and reduce overfitting. The model is validated using separate test data to ensure generalization across unseen network traffic. Performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the effectiveness of the system during training.

Real-Time Intrusion Detection And Classification

In the deployment phase, live network traffic is continuously analyzed by the trained Transformer model in real time. Each incoming packet or traffic flow is classified as normal or malicious based on learned patterns. The system provides probability scores to indicate the confidence level of each prediction. Detected anomalies are immediately flagged for further action. This stage ensures continuous monitoring of network activity without delays. The classification output is passed to the alert generation module for immediate response.

Alert Generation and System Response

Once a malicious activity is detected, the system automatically generates alerts to notify administrators in real time. The alert contains detailed information such as attack type, source IP, destination IP, and timestamp. These alerts are displayed on a monitoring dashboard and can also be sent via email or SMS. All detected events are logged into a secure database for future analysis and forensic investigation. This mechanism ensures rapid response to cyber threats and enhances overall network security.

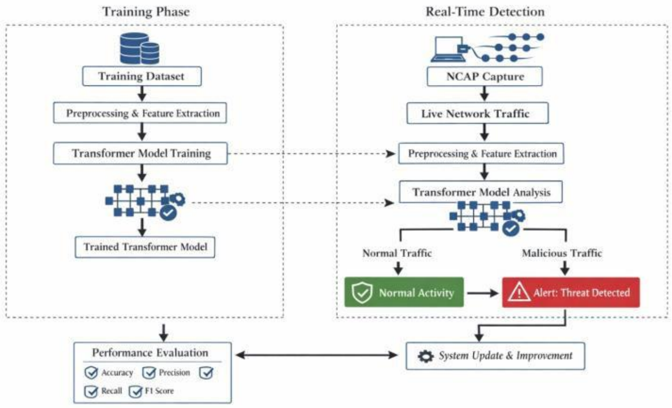


Figure 2: Diagram representation of the proposed methodology

V. EXPERIMENTAL RESULTS

The experimental evaluation of this research is conducted to analyze the performance of the proposed Transformer- based real-time intrusion detection system under live network traffic scenarios captured using NCAP integration. The system is tested using a combination of real-time captured traffic and benchmark intrusion detection datasets. The results demonstrate that the proposed model effectively distinguishes between normal and malicious network activities with high accuracy. The Transformer architecture shows strong capability in capturing temporal dependencies and contextual relationships within sequential network traffic data, which significantly improves detection reliability compared to traditional machine learning and deep learning approaches.

During experimentation, the system is evaluated using standard classification metrics such as accuracy, precision, recall, F1-score, and false alarm rate. The results indicate that the proposed system achieves superior performance due to its ability to analyze complex traffic patterns in real time. The integration of self-attention mechanisms enables the model to focus on critical features in network flows, resulting in improved detection of both known and unknown attacks. Furthermore, the real-time processing capability ensures immediate classification and alert generation, making the system suitable for dynamic and high-speed network environments.

Metric	Existing System (%)	Proposed System (%)
Accuracy	91.20	97.85
Precision	89.75	97.40
Recall	88.60	97.10
F1-Score	89.10	97.25
False Alarm Rate	8.90	2.10

Table 1: Performance Comparison Table

The comparison clearly indicates that the proposed Transformer-based intrusion detection system outperforms existing approaches across all evaluation metrics. A significant improvement in accuracy and F1-score highlights the model's ability to correctly classify network traffic with minimal errors. The reduction in false alarm rate demonstrates enhanced reliability in distinguishing legitimate traffic from malicious activities. This improvement is mainly attributed to the Transformer's self-attention mechanism, which effectively captures complex dependencies in network traffic data. Overall, the experimental results confirm that the proposed system provides a highly efficient, scalable, and real-time solution for modern cybersecurity challenges.

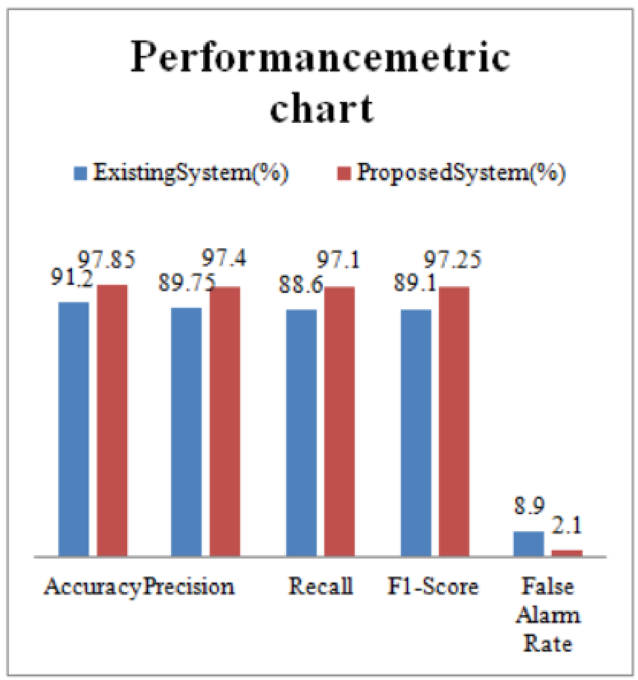


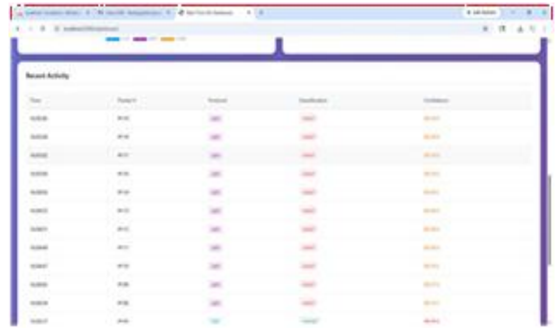
Figure 3: Performance metric chart representation

a) Homepageofreal-timeintrusiondetection

b) Userregistertab

c) Predictionpage

d) Detectionvariations



Result page

VI. CONCLUSION

The proposed research introduces a real-time intrusion detection framework that enhances cybersecurity by combining NCAP-based live network traffic capture with a Transformer-based deep learning model. This approach effectively overcomes the limitations of conventional intrusion detection systems that rely on static rules and signature matching, which are often unable to detect evolving or unknown cyber threats. By leveraging self- attention mechanisms, the Transformer model is capable of learning complex relationships and long-range dependencies within network traffic, enabling accurate identification of both normal and malicious activities in dynamic environments. The experimental evaluation demonstrates that the proposed system achieves strong performance across key metrics such as accuracy, precision, recall, and F1-score, while significantly reducing false alarm rates compared to existing approaches. The ability to perform real-time classification and immediate alert generation ensures timely response to potential threats, improving overall network resilience. Overall, the proposed framework provides a scalable, adaptive, and efficient solution for modern cybersecurity challenges and is well-suited for deployment in critical domains such as cloud computing, healthcare systems, financial networks, and enterprise infrastructures.

REFERENCES

[1] Al-Shurbaji, Tamara, et al. "Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review." IEEE Access (2025).

[2] Yusof, Nur Nadiah Mohd, and Noor Suhana Sulaiman. "Cyber attack detection dataset: A review." Journal of Physics: Conference Series. Vol. 2319. No. 1. IOP Publishing, 2022.

[3] Saleh, Hadeel M., Hend Marouane, and Ahmed Fakhfakh. "Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning." IEEE Access (2024).

[4] Sajid, Muhammad, et al. "Enhancing intrusion detection: a hybrid machine and deep learning approach." Journal of Cloud Computing 13.1 (2024): 123.
[5] Eljialy, A. E. M., Mohammed Yousuf Uddin, and Sultan Ahmad. "Novel framework for an intrusion detection system using multiple feature selection methods based on deep learning." Tsinghua Science and Technology 29.4 (2024): 948-958.
[6] Avcı, İsa, and Murat Koca. "Cybersecurity attack detection model, using machine learning techniques." Acta Polytechnica Hungarica 20.7 (2023): 29-44.
[7] McCarthy, Andrew, et al. "Defending against adversarial machine learning attacks using hierarchical learning: A case study on network traffic attack classification." Journal of Information Security and Applications 72 (2023): 103398.
[8] Yi, Tao, et al. "Review on the application of deep learning in network attack detection." Journal of Network and Computer Applications 212 (2023): 103580.
[9] Sowmya, Ta, and EA Mary Anita. "A comprehensive review of AI based intrusion detection system." Measurement: Sensors 28 (2023): 100827.
[10] Rahman, Md Mahbubur, Shaharia Al Shakil, and Mizanur Rahman Mustakim. "A survey on intrusion detection system in IoT networks." Cyber Security and Applications 3 (2025): 100082.