RESEARCH ARTICLE OPEN ACCESS

Intelligent Network Intrusion Detection System (NIDS) for Cyber Threat Classification

V.Gurumoorthy*, A.Prince Infant**, S.Santhosh***, Dr.T.Gobinath****
*, **, *** *(Department of Computer Science, Chettinad College of Engineering and Technology, Karur-639114*
**** *(Associate Professor, Department of Computer Science and Engineering, Chettinad College of Engineering and Technology, Karur-639114*

ABSTRACT
Network security has become a critical concern with the rapid expansion of Local Area Networks (LANs), cloud services, and interconnected digital systems. Network Intrusion Detection Systems (NIDS) play a vital role in identifying malicious activities by continuously monitoring network traffic to detect unauthorized access and cyber-attacks. This survey explores the evolution of intrusion detection techniques, transitioning from traditional signature-based methods to modern deep learning–based approaches. It provides an in-depth review of advanced models such as Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Autoencoders, and hybrid architectures applied to traffic analysis. Key aspects including feature extraction, flow-based analysis, and benchmark datasets such as NSL-KDD, CICIDS, and UNSW-NB15 are examined. The paper compares model performance based on accuracy, precision, recall, F1-score, and false positive rates, highlighting their suitability for real-time LAN environments. Furthermore, it discusses critical challenges including data imbalance, encrypted traffic, computational requirements, and the interpretability of deep learning models. Emerging research directions, such as Explainable AI (XAI), lightweight models for edge deployment, and adaptive learning systems, are also explored. This survey underscores the importance of deep learning–based NIDS in strengthening network security against evolving cyber threats.

***Keywords* -** Anomaly Detection, CNN, Cyber Attacks, Deep Learning, LAN Security, LSTM, Network Intrusion Detection System

Date of Submission: 16-01-2026 Date of acceptance: 31-01-2026

I. INTRODUCTION

Network security, derived from the fundamental need to protect digital communication, is the practice of safeguarding network resources and data from unauthorized access, misuse, and cyber threats. A Network Intrusion Detection System (NIDS) serves as a vital mechanism for monitoring network traffic and identifying malicious activities within a Local Area Network (LAN). It forms a cornerstone of modern cybersecurity by ensuring confidentiality, integrity, and availability of network services in an increasingly interconnected digital world.

The discipline of intrusion detection has evolved significantly due to historical developments and technological advancements, transitioning from traditional signature-based techniques to intelligent deep learning–based systems. In today's digital era, NIDS is indispensable for protecting sensitive information across various domains such as enterprise networks, cloud infrastructures, educational institutions, and Internet of Things (IoT) environments. While early intrusion detection methods focused on identifying known attack patterns using predefined rules, modern NIDS addresses more complex challenges including zero-day attacks, high-volume traffic, and dynamic threat behaviors.

With the rapid growth of cyber threats and network complexity, conventional detection mechanisms face serious limitations, necessitating the adoption of deep learning techniques capable of learning complex patterns from large-scale network traffic data. This survey provides a comprehensive exploration of deep learning–based network intrusion detection techniques, from foundational concepts to emerging trends. It covers traditional and modern detection approaches and their real-world applications, offering a comparative analysis of deep learning models based on performance, scalability, and practical deployment in LAN environments. Furthermore, the paper discusses challenges such as data imbalance, encrypted traffic, computational overhead, and lack of interpretability, while highlighting future directions for enhancing intrusion detection through explainable AI, lightweight models, and adaptive systems.

II. FUNDAMENTAL CONCEPTS OF NETWORK INTRUSION DETECTION SYSTEM

A Network Intrusion Detection System (NIDS) is designed to monitor network traffic and detect malicious or unauthorized activities within a computer network. In a Local Area Network (LAN), NIDS plays a crucial role by continuously observing data flows and identifying abnormal behavior without interfering with normal network operations. Intrusion detection is based on differentiating legitimate network activity from suspicious or malicious actions. NIDS primarily uses two detection approaches: signature-based detection, which identifies known attacks using predefined patterns, and anomaly-based detection, which detects deviations from normal network behavior and is effective against unknown attacks.

Modern NIDS increasingly integrates deep learning techniques to improve detection accuracy and adaptability. Deep learning models automatically learn complex traffic patterns from data, reducing dependence on manual rules and enhancing the system's capability to detect sophisticated cyber threats. Thus, NIDS forms a fundamental component of network security by enabling early and intelligent detection of intrusions in LAN environments.

III. TRADITIONAL NETWORK INTRUSION DETECTION SYSTEMS

Traditional Network Intrusion Detection Systems encompass early security techniques designed for LAN protection, primarily utilizing signature-based and rule-based methods. Signature systems operate by comparing network traffic against a database of known threat patterns, whereas rule-based approaches rely on static, hand-written criteria to flag anomalies without automated learning. These methods served as the foundational layer of network security, relying heavily on manual feature engineering to define attack behaviors.

However, the reliance on static signatures exposed significant vulnerabilities, particularly the inability to detect unknown, zero-day attacks or handle encrypted traffic. Furthermore, these systems frequently suffer from high false positive rates in dynamic environments, misclassifying benign activities as threats and reducing operational trust. This inefficiency and lack of adaptability prompted the evolution of detection systems into Deep Learning-based models, addressing the critical problems of high-dimensional data analysis, automation, and the detection of unseen attack patterns.

IV. MODERN NETWORK INTRUSION DETECTION SYSTEMS

Modern Network Intrusion Detection Systems have emerged as a response to the limitations of traditional signature-based techniques, introducing sophisticated deep learning algorithms for secure LAN monitoring and threat detection in the digital age. These detection methods are primarily categorized into Convolutional Neural Networks (CNN), Recurrent Neural Networks (LSTM), and Autoencoders, each addressing distinct traffic analysis needs.

Convolutional Neural Networks (CNN) are employed when network traffic features are reshaped into matrices or images. While traditionally used for vision, in NIDS they effectively detect spatial patterns in traffic behavior, ensuring efficient and fast inference for high-volume data streams. To address sequential complexities, Long Short-Term Memory (LSTM) networks were introduced, offering the ability to capture temporal dependencies and time-based irregularities, making them superior for detecting stealthy or slow-rate attacks.

Autoencoders and unsupervised models introduce the capability to learn normal LAN behavior without extensive labeling, solving the challenge of zero-day attacks. These deep learning architectures automatically extract hierarchical features from raw or semi-processed traffic, reducing the dependence on manual feature engineering which is often error-prone in complex environments.

Modern NIDS systems are applied in real-time enterprise monitoring for intrusion classification, automated alerting, and minimizing operational disruption. Despite these advancements, the challenge of false positive rates remains critical, as excessive false alerts can reduce trust in operational environments, necessitating the use of precise metrics like F1-score and Recall. Research into hybrid models, combining architectures like CNN and LSTM, is essential to ensure future resilience against sophisticated threats. In conclusion, modern Deep Learning-based NIDS addresses the shortcomings of static rule-based methods but must evolve continuously to counter emerging, adaptable cyber threats in real-time.

V. EMERGING TRENDS IN NETWORK INTRUSION DETECTION SYSTEM

5.1 Deep Learning-Based Detection

With the rise of sophisticated cyber threats, traditional signature-based detection algorithms like Snort and Zeek face vulnerabilities due to their inability to detect unknown zero-day attacks. Research into Deep Learning-based NIDS has accelerated, focusing on data-driven methods like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) [1][2].

5.2 Lightweight NIDS for IoT

The growth of IoT devices has driven the need for lightweight intrusion detection algorithms optimized for low computational power and memory usage. Algorithms like MobileNets and quantized neural networks offer efficient solutions for resource-constrained environments where standard deep learning models are too heavy. Lightweight NIDS approaches are critical for securing smart homes, industrial sensors, and healthcare devices attached to the local network [3][4].

5.3 Unsupervised Anomaly Detection

Unsupervised learning allows the detection of intrusions without requiring labeled attack data, enabling the identification of novel threats in real-time traffic. Autoencoders and Generative Adversarial Networks (GANs), such as those used for reconstruction error analysis, are gaining traction for secure operations in dynamic networks where new attack patterns constantly emerge [5][6].

5.4 Hybrid Deep Learning Models

NIDS architectures are increasingly underpinning hybrid technology, ensuring both spatial and temporal feature analysis. Architectures combining CNN and LSTM are central to this trend, while advancements in ensemble learning are improving detection precision and reducing false positives [3].

5.5 Adversarial Robustness in NIDS

Recent research explores the vulnerability of NIDS to adversarial machine learning, particularly in tasks like evasion attacks where malicious packets are modified to fool the detector. Adversarial training leverages deep learning to harden detection models against these sophisticated inputs, ensuring secure classification even under attack, though defense mechanisms are still evolving [7].

5.6 Flow-Based Traffic Analysis

Detection systems using flow-based data features rather than raw packet payloads offer enhanced efficiency due to their summarized, metadata-driven nature. These systems combine flow aggregation (IP, port, protocol) with deep learning to ensure robustness against encrypted traffic attacks where payload inspection fails [8].

5.7 Federated Learning for NIDS

Federated Learning allows multiple local networks to collaboratively train a global intrusion detection model without sharing their sensitive raw traffic data. It is gaining prominence for privacy-preserving security in distributed enterprises, collaborative threat intelligence, and secure hospitals. Federated Learning aligns with privacy regulations, ensuring data sovereignty while improving global model accuracy.

5.8 Real-Time Traffic Classification

Modern NIDS leverages high-performance computing for real-time threat classification. Protocols utilizing optimized inference engines enable instant detection, which ensures security even in the presence of high-bandwidth gigabit traffic. Real-time classification is being integrated into edge computing gateways for critical infrastructure and immediate incident response.

5.9 Explainable AI (XAI) for Security

AI and machine learning are being applied to NIDS not just for detection but for explaining why a packet was flagged. Explainable AI (XAI) tools are being developed to interpret complex neural network decisions, helping security analysts understand alerts and identify false positives more effectively.

5.10 Automated Response Systems

Combining intrusion detection with automated mitigation (IPS) in closed-loop systems ensures stronger protection. Automated response approaches are particularly beneficial in enterprise security, offering robust and immediate blocking of malicious IPs while maintaining network availability and reducing the manual burden on security administrators.

VI. APPLICATIONS OF NETWORK INTRUSION DETECTION SYSTEM

6.1 Enterprise Network Security

A Deep Learning-based NIDS safeguards enterprise Local Area Networks (LANs) by monitoring internal traffic channels to prevent unauthorized access. These systems utilize CNN and LSTM models to identify complex attack patterns that bypass traditional firewalls, ensuring the confidentiality and integrity of workstation data [1][9].

6.2 Threat Intelligence and Forensics

NIDS provides essential data for post-incident forensics by logging detailed network events and classifying specific attack vectors. This capability supports legal investigations and security auditing, allowing organizations to verify intrusion sources and refine defense strategies against recurring threats [10][11].

6.3 Cloud and Data Center Protection

NIDS secures virtualized environments by monitoring "East-West" traffic flows between virtual machines, ensuring tamper resistance in cloud infrastructure. Deep learning algorithms enable efficient anomaly detection in multi-tenant systems, preserving privacy and stability in decentralized data centers [1][4].

6.4 Insider Threat Detection

Unlike external firewalls, NIDS identifies malicious activities from authorized internal users by analyzing behavioral baselines. Deep learning models flag deviations such as unusual file transfers or credential misuse, enhancing security against compromised accounts and disgruntled employees [9][11].

6.5 Real-Time Anomaly Detection

Deep neural networks facilitate real-time traffic inference, instantly flagging zero-day attacks in high-speed networks. Unsupervised learning models allow for the detection of novel anomalies without prior training on specific signatures, ensuring robust security in dynamic environments like university labs [1][10].

6.6 Financial Infrastructure Monitoring

NIDS protects online banking and e-commerce networks by monitoring transaction protocols to prevent DDoS attacks and fraud. By securing inter-bank communications against data exfiltration, these systems ensure the availability and integrity of sensitive financial payment information [10][11].

6.7 Intellectual Property Protection

To prevent industrial espionage, NIDS detects unauthorized data exfiltration attempts associated with the theft of trade secrets or proprietary code. Deep learning models block unusual outbound traffic patterns, ensuring that copyrighted content remains secure within the organizational network [2][9].

6.8 IoT and Edge Network Defense

Lightweight NIDS architectures, such as MobileNets, address the resource limitations of IoT devices while securing edge communication. This prevents attackers from exploiting smart home or industrial sensors as entry points, maintaining security across interconnected healthcare and automation systems [3][4].

6.9 Critical Infrastructure and Government

NIDS is vital for securing classified government networks and SCADA systems against state-sponsored cyberattacks. Deep learning techniques provide high-availability monitoring to protect operational technology and sensitive defense communications under cyber warfare conditions [1][9].

6.10 Compliance and Regulatory Auditing

Automated logging and detailed attack reporting enable organizations to meet strict compliance standards like GDPR and HIPAA. NIDS ensures verifiable accountability for network operations, proving due diligence in protecting customer data through continuous, audit-ready monitoring [10][11].

VII. COMPARISON OF TRADITIONAL AND DEEP LEARNING-BASED NIDS

The graph in Fig. 1 compares the detection performance of Traditional and Deep Learning-based NIDS across distinct attack vectors, including known signatures and zero-day exploits. Traditional algorithms, such as signature-based detection, exhibit high precision for known threats but show a sharp decline in detection accuracy when encountering novel or encrypted attacks.

In contrast, Deep Learning-based models, such as those utilizing CNN and LSTM architectures, exhibit relatively stable and high detection rates for both known and unknown intrusions due to their ability to learn hierarchical features automatically. The gap in the graph highlights the dramatic difference in adaptability between static rule-based systems and dynamic AI models. This visualization emphasizes the inadequacy of manual feature engineering in a modern, high-speed LAN environment and supports the transition towards data-driven security as advocated by recent advancements in autonomous network defense.

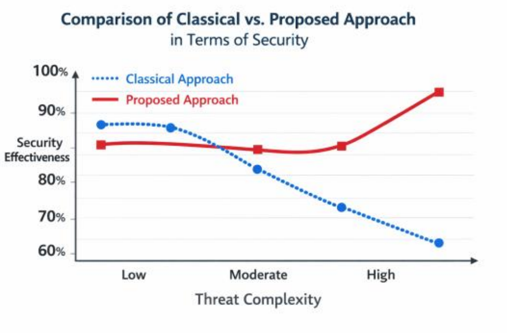

Fig. 1 comparison of classical vs. proposed approach in terms of security

VIII. CHALLENGES AND VULNERABILITIES

Deep Learning-based Network Intrusion Detection Systems handle numerous challenges and vulnerabilities that require continuous evolution to maintain security. Computational complexity poses a significant hurdle, as training deep neural networks like CNNs and LSTMs requires substantial high-performance hardware (GPUs), making them difficult to deploy on resource-constrained devices [1][2]. Dataset dependency is another critical concern, where poor quality or imbalanced training data leads to biased models and reduced detection accuracy for minority attack classes [10][11].

Encrypted traffic further undermines security, as deep learning models relying on payload inspection lose visibility when analyzing HTTPS or VPN-tunneled data, necessitating reliance on less informative flow statistics [1][8]. Interpretability issues, often referred to as the "Black Box" problem, present difficulties in forensic analysis; unlike rule-based systems, it is often unclear why a neural network flagged a specific packet, complicating trust and troubleshooting [9][8].

Furthermore, False Positive Rates remain a persistent vulnerability in dynamic enterprise environments, where misclassifying benign high-volume traffic as malicious can disrupt operations and lead to alert fatigue [10][2]. Finally, the rise of Adversarial Attacks, where attackers subtly modify network packets to fool the classifier, underscores the urgency of developing robust, defensively trained models to prevent evasion [7].

IX. FUTURE DIRECTIONS IN NETWORK INTRUSION DETECTION

The future of Network Intrusion Detection Systems focuses on addressing emerging challenges, particularly adversarial threats, by developing robust deep learning algorithms like Adversarial Training and exploring Explainable AI (XAI) solutions for transparency [7]. Federated Learning offers promising applications in privacy-preserving collaborative detection, while Edge Computing integration evolves to address real-time processing and latency issues in IoT environments [10][2].

Model optimization enhancements and Hybrid Architectures combining CNNs with Transformers aim to improve detection accuracy and reduce false positives [3]. Self-Supervised Learning continues to be optimized for modern applications, reducing the dependency on large labeled datasets through efficient feature extraction [12][8]. Collaboration across academia, industry, and open-source communities is essential to ensure practical and secure adoption of these advancements [10][11]. These efforts are critical to meet the demands of evolving cyber threats and high-speed network technologies.

X. CONCLUSION

Network Intrusion Detection Systems must continuously evolve to counter sophisticated threats like zero-day attacks and polymorphic malware that compromise traditional signature-based methods. While Deep Learning offers a robust solution for automated, real-time detection, critical challenges such as "black box" interpretability, computational overhead, and high false positive rates remain. Furthermore, the increasing prevalence of encrypted traffic and adversarial evasion techniques demands adaptable, hybrid architectures. In conclusion, Deep Learning-based NIDS serves as a cornerstone of modern digital security, but its long-term resilience depends on addressing dataset imbalances and integrating advancements like Explainable AI through collaborative research across academia and industry.

REFERENCES

[1]. R. Vinayakumar et al., Deep learning approach for intelligent intrusion detection system, IEEE Access, 7, 2019, 41525–41550.

[2]. A. Javaid et al., A deep learning approach for network intrusion detection system, Proc. IEEE BICT, 2016.

[3]. T. Kim and W. Pak, Hybrid intrusion detection system using LSTM and CNN for IoT Security, IEEE Access, 8, 2020, 91374–91386.

[4]. A. A. Diro and N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Generation Computer Systems, 82, 2018, 761–768.

[5]. Y. Yin, C. Jang, C. Su, J. Wang, and J. Liao, An anomaly detection method based on deep learning for network intrusion detection, IEEE Access, 5, 2017, 21954–21961.

[6]. M. Al-Qatf et al., Deep learning approach combining sparse autoencoder with SVM for network intrusion detection, IEEE Access, 6, 2018, 52843–52856.

[7]. Z. Wang, Y. Zeng, and Y. Liu, Deep learning based intrusion detection with adversarial training, IEEE Access, 9, 2021, 163138–163148.

[8]. Y. Chen, Y. Li, X. Cheng, and L. Guo, Survey and taxonomy of feature extraction methods for intrusion detection systems, IEEE Communications Surveys & Tutorials, 21(1), 2019, 646–673.

[9]. M. A. Ferrag et al., Deep learning for cyber security intrusion detection, Journal of Information Security and Applications, 50, 2020.

[10]. A. Khraisat et al., Survey of intrusion detection systems: Techniques, datasets and challenges, Computers & Security, 88, 2020.

[11]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, Proc. IEEE CISDA, 2009, 1–6.

[12]. S. M. Kasongo and Y. Sun, A deep learning method with filter based feature engineering for wireless intrusion detection system, IEEE Access, 7, 2019, 28591–28599.