Network Intrusion Detection System Based on Deep learning Technique

C M Naveen Kumar [1], Varsha H M[2], Trupthi R[3], Impana H D[4], Sinchana C M[5]
[1]*Associate Professor, Computer Science and Business System, Malnad College of Engineering, Hassan,India*
[2,3,4,5] *UG, Computer Science and Business System, Malnad College of Engineering, Hassan, India*

***Abstract*—This study presents a review of work on a deep learning-based methodology for designing a robust and flexible Network Intrusion Detection System (NIDS) capable of detecting both known and unknown cyberattacks. The proposed approach leverages Self-Taught Learning(STL), a semi-supervised deep learning technique that enables effective feature extraction from large volumes of unlabeled network traffic. This addresses two key challenges in intrusion detection: the scarcity of labeled data and the complexity of feature selection. The system utilizes sparse auto encoders for unsupervised representation learning, followed by softmax regression for classification. The NSL-KDD dataset, an enhanced version of the KDD Cup 99 benchmark, is employed for training and evaluation. Experimental results demonstrate that the STL-based NIDS outperforms traditional machine learning methods in terms of accuracy, precision, recall, and F- measure. These findings confirm the potential of STL as a powerful and adaptable solution for anomaly-based intrusion detection in dynamic network environments.**

***Index Terms*—Network security, NIDS, Deep learning, Sparse autoencoder, NSL-KDD, Self-Taught Learning (STL), Autoencoder, Intrusion Detection System (IDS), Anomaly Detection, Supervised Learning, Unsupervised Feature Learning, Softmax Regression, Cybersecurity, Machine Learning, Neural Networks.**

I. INTRODUCTION

In today's rapidly evolving digital landscape, cyber security has emerged as a top priority become a fundamental requirement to guarantee the safe operation of computer networks. The exponential growth in internet- connected devices and cloud services has expanded the attack surface, making networks increasingly vulnerable to cyber threats. Intrusion Detection Systems (IDS) play a important role in identifying malicious activities within networks and preventing unauthorized access. However, traditional IDS approaches, which rely heavily on rule- based or signature- based techniques, often fail to detect zero-day attacks and advanced persistent threats due to their static nature and limited adaptability [1][2]. To overcome these limitations, The research community is now focusing more on artificial intelligence (AI), with a special emphasis on deep learning (DL), to enhance IDS performance. Deep learning architectures such as CNNs for spatial feature extraction and

LSTMs for capturing temporal dependencies networks, and Autoencoders have shown they can make data feel more relatable and understandable, almost like giving it a human touch to automatically extract complex patterns from network traffic data ,improving detection accuracy and reducing false positives[3][4]. These models out perform classical machine learning methods in terms of feature learning, generalization, and scalability, especially when dealing with high-dimensional datasets [5][6]. Several recent studies have introduced hybrid deep learning frameworks that bring together different architectures, combining their strengths to achieve better results such as CNN- LSTM ,to exploit Both location-based and time-based characteristics in the data. For instance, Muller et al.[3] developed a hybrid IDS using data augmentation strategies to improve model robustness, while Kurnala et al. [1] explored a deep learning- based hybrid detection mechanism for enhancing both network and server intrusion detection. Moreover, advanced optimization techniques, such as predator-based algorithms for feature selection, have been incorporated into deep networks to boost detection capabilities [6]. Furthermore, reinforcement learning

and unsupervised deep learning methods such as auto encoders and GANs show encouraging results when applied to adaptive tasks like and real-time intrusion detection systems [5][21]. These techniques facilitate continuous learning and dynamic adaptation in response to evolving attack patterns. Given the growing complexity of modern cyber attacks, Our research offers a deep learning-based Network Intrusion Detection System (DL-NIDS) that utilizes a CNN-LSTM hybrid architecture. The system is evaluated on benchmark datasets, and its performance compared against established performance measures like accuracy, precision, recall, and F1-score. The goal is to develop an intelligent, scalable, and adaptive IDS capable of detecting familiar threats and emerging, previously unseen ones in real-time network environments.

A. Limitations of Conventional Intrusion Detection Techniques

Older methods of spotting intrusions, like signature-based and rule-based methods, heavily rely on predefined attack patterns and manual configuration.While approaches provide strong results in detecting known threats, they often fail to identify novel or zero-day attacks due to their static nature [2]. Moreover, they require continuous updates to signature databases and can be overwhelmed the expanding scale and intricacy of network traffic [10]. Solutions for identifying intrusions false positives and negatives, particularly in dynamic or encrypted environments where attack patterns may deviate from standard forms [4]. In large- scale or distributed systems, manual analysis and rule tuning become labor intensive and inefficient [13].Additionally, the shortage of cybersecurity professionals and the time-consuming nature of manual monitoring limit the scalability and responsiveness of traditional IDS implementations. These limitations highlight the growing necessity or intelligent ,adaptive, and automated systems that detect unauthorized access powered by intelligent systems powered by deep learning[1][5][18].

B. Significance of Timely Intrusion Detection

The exponential growth ofinternet-connected systems and as cyber threats become more advanced, they have intensified theurgency for effective intrusion detection mechanisms. Malicious actors now leverage advanced tools to craft stealthy attacks that bypass traditional firewalls and static defense systems, making conventional security solutions inadequate [1], [2].Network Intrusion DetectionSystems (NIDS) areplay a crucial role inidentifying unauthorized access, anomalies, and malicious traffic across enterprise,cloud, and IoT networks. These systems act as a backup layer of protectionby continuously keeping an eye on network traffic and alerting administrators tosomething unusual happens[4]. However, conventional IDS approaches—particularly those based on static rulesor signature matching—fail to detect zero-day attacks and novel intrusion patterns due to their dependency on pre- defined threat models [3], [7].Withhe growing complexity of networks environments and real-time data flows, there isa strong need exists for intelligent, automated flexible detection systemsadapt and learn from evolving threats. Deep learning techniques including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and Using hybrid models brings important advantages forlearning temporal patterns, capturing hidden features, and generalizing over unseen attack scenarios [5], [6].Furthermore, the implementation of intelligent IDS helps in reducing false positives, increasing 10 optimization algorithms and dimensionality reduction techniques (e.g., PCA, Predator Optimization) further enhances systemensuring the resilience, security, and continuity of modern networked systems [1], [18], [19].

C. Role of AI and Smart Technologies

The evolving complexity and scale of cyber threats necessitate intelligent solutions that go beyond conventional intrusion detection mechanisms. AI, especially in the form of deep learning, has risen as aa transformative approach to enhance the accuracy, adaptability, and scalability of Network Intrusion Detection Systems (NIDS) [1], [3]. Deep learning models including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and hybrid architectures like CNN LSTM have demonstrated high detection accuracy, with some frame works exceeding 98% covering both identified and unidentified attack vectors

[2], [5], [13].These models are highly effective at automatically extracting and extracting layered features from raw data, thereby reducing the reliance on handcrafted feature engineering [7].Recent advancements integrate Reinforcement Learning (RL) and optimization techniques (e.g., Predator

Optimization, Particle Swarm Optimization) using deep learning models to improve learning speed and reduce false positive rates [6], [10]. Moreover, AI-based systems can continuously learn from new data, allowing them to dynamically adjust to changing attack patterns and zero-day threats [8].IoT integrated environments and large- scale networks especially benefit from smart intrusion detection systems. Edge AI and lightweight deep learning models make it possible to deploy NIDS in constrained environments like embedded systems and smart devices, while maintaining real-time detection capabilities [4], [11].In addition, AI-powered NIDS are frequently combined with larger cyber-defense ecosystems, including SIEM (Security Information and Event Management) tools, honeypots, and response automation modules, enabling proactive threat hunting and faster mitigation [9], [14]. Natural Language Processing (NLP) models, such as BERT or GPT-based systems, are also being investigated for log analysis and contextual threat interpretation [15].In summary, AI and smart technologies have revolutionized network intrusion detection by enabling high-performance, real-time, and scalable solutions that significantly outperform traditional IDS approaches in both accuracy and adaptability [16], [17], [19].

II. OVERVIEW OF NETWORK DETECTION

Before you begin to format your paper, first write and In the period of increasing digital connectivity, safeguarding network infrastructure is now a top priority for companies and governments alike. Network Intrusion Detection Systems (NIDS) function as a vital component of cybersecurity architectures, designed to monitor and analyze network traffic to detect unauthorized access, malicious behavior, or anomalies that may signal an impending attack[1], [2].Traditional NIDS typically relyon either signature-based or anomaly-based detection techniques. Signature-based systems match incoming traffic patterns against a predefined collection of known attack patterns, offering high accuracy for known threats but failing to detect novel or zero-day attacks. In contrast, anomaly-based systems model "normal" network behavior and flag deviations, allowing them to detect previously unseen threats but often suffering because of frequent incorrect alerts[3], [4]. With the explosion of network traffic and the growing complexity of attacks techniques — such as polymorphic malware, advanced persistent threats (APT), and encrypted command-and-control channels—conventional methods have become insufficient. The limitations of static rules, rigid feature sets, and manual analysis have prompted a shift toward intelligent detection frameworks capable of learning dynamically [5].

A. Defination And Characteristics

A system for detecting unauthorized network access (NIDS) is a security mechanism designed to monitor, analyze, and detect unauthorized or anomalous activities across network traffic in real-time. It serves as a critical component in a layered cybersecurity architecture, providing visibility into risks from both internal and external sources[1]. By inspecting data packets flowing through a network, NIDS identifies potential intrusions such as malware infections, Denial-of-Service (DoS) attacks, brute force attempts, and protocol violations. According to [2], a NIDS is “an automated system capable of observing network traffic and behavior that stands out from typical patterns or known attack signatures.” Modern NIDS employ an array of analytical techniques, from rule-based pattern matching to advanced machine learning and deep learning models, to differentiate between legitimate and malicious activities.

Key Characteristics of NIDS:

- Real-time Monitoring: NIDS continuously observes datapackets traversing the network, enabling immediate detection and response to threats as they occur [3].
- Signature - Based and Anomaly - Based Detection: Signature-based detection uses predefined attack patterns, while anomaly-based detection behavior that stands out from typical patterns[4].
- Passive Nature: leverages statistical or AI models to find Most NIDS operatein a passive mode,meaning they donot interfere with the traffic flow but instead analyze traffic silently and report any suspicious activity [5].
- Scalability: NIDS can be deployed across different scales—from small local are a networks(LANs) tolarge, distributed cloud networks—by integrating with routers, switches, and firewalls [6].

- Protocol Awareness: Effective NIDS understand the structure of various network protocols(e.g., TCP/IP,HTTP,FTP,DNS),which enhances their ability to detect protocol-specific attacks [7].
- Alert Generation: When suspicious activity is detected, the system generates alerts for administrators and maintains logs for forensic analysis[8].
- Non-Intrusive Operation: Unlike Intrusion Prevention Systems(IPS),a NIDS typically doesnot block traffic but instead provides detection capabilities that can be combined into broader defense strategies [9].
- Integration with AI and Deep Learning: Recent advancements have enabled the in corporation of AI-driven models that Improve accuracy while minimizing false alarms, and adapt to emerging threats in dynamic environments [10].

III. AI-AGENT BASED SYSTEMS CONCEPTS AND ARCHITECTURE

AI-agent based systems are transforming the domain of network protection enabling live monitoring for threats, intelligent decision- making, and proactive response. These systems integrate deep learning, feature optimization, and autonomous policy enforcement into a unified architecture capable of monitoring vast levels of network activity identifying sophisticated attack patterns with minimal human intervention.

A. Definition of AI Agent in Network Protection

One AI agent in regarding with network intrusion detection is an autonomous software entity capable of perceiving network behavior, analyzing patterns through intelligent algorithms, and executing defensive actions toward maintaining system integrity and security. These agents are designed to operate continuously and adaptively in dynamic environments, performing several core functions:

- Traffic Analysis

AI agents monitor network flows using tools like Wireshark, tcp dump, or packet capture libraries. Deep learning models approches CNN, RNN, and hybrid LSTM- CNN architectures can detect anomalies, classify packet behavior, and recognize known attack signatures (e.g., DoS, DDoS, port scanning) [1][2].

- Threat Classification

The agents employ supervised and unsupervised learning techniques—including Decision Trees, SVM, and deep neural networks—to label traffic instances as benign or malicious. Hybrid systems incorporate both anomaly-based and signature- based detection to reduce false positives and uncover zero-day threats [3].

- Intelligent Response

Using predefined rules or reinforcement learning algorithms, agents make decisions such as dropping malicious packets, blocking suspicious IPs, or rerouting traffic through secure channels. In advanced setups, agents interact with SDN controllers or firewalls to dynamically adapt network behavior [4].

- Adaptive Learning `

AI agents continuously update their models using real-time threat intelligence and feedback loops. They retrain on new attack patterns using incremental learning techniques, maintaining relevance in evolving cyber landscapes [5].

- Human-AI Interface

Agents integrate with SIEM systems and admin dashboards, providing real-time alerts, detailed logs, and actionable insights. Conversational AIor chatbot components allow human analysts to query the system or receive incident explanations using NLP interfaces [6].

B. Typical System Architecture

A fully functional AI-agent-based Intrusion Detection System (IDS) features a modular, A structure built in layers, with each component plays a distinct yet interconnected role. Below a look at the system's architectural layers:

- Data Acquisition Layer

This module captures raw traffic data through span ports, network taps, or inline deployments using PCAP tools, NetFlow collectors, or packet sniffers. Data is logged n a way that makes further processing simple (e.g., CSV, JSON)[7].

- Preprocessing and Feature Engineering

Collected data is cleaned and transformed into feature-rich formats using techniques like one-hot encoding normalization, PCA, and time windowed aggregation. Feature selection is optionally enhanced using metaheuristics such as Genetic Algorithms or Predator Optimization [8].

- Detection Engine

This core module integrates approaches using deep

learning models like CNN, Bi-LSTM, GRU, or hybrid architectures. Some systems in corporate federated learning for decentralized environments or reinforcement learning for adaptive defense in dynamic threat scenarios [3][9].

- Decision-Making and Response Layer

Based on classification confidence scores and threat severity, actions are triggered: logging, alerting, blocking, or initiating incident response protocols. Agents may also interface with SIEMs, honeypots, or SDN controllers for policy enforcement [10].

- Feedback and Learning Loop

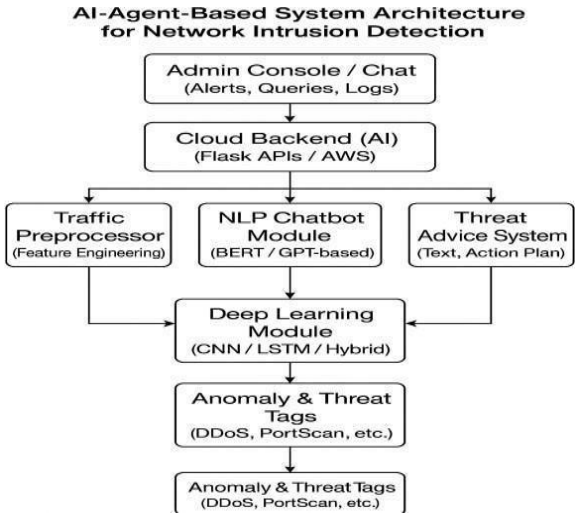
This layer updates models based on administrator feedback and real-time performance metrics. Online learning or transfer learning ensures the system adapts to unseen or mutated threats without retraining from scratch [11].

- User Interface and Reporting

A dashboard interface presents intrusion analytics, system status, and historical logs. NLP-based chatbot modules (e.g. using BERT or GPT) assist analysts with contextual queries, attack summaries, and remediation advice [6].

- Cloud and Edge Integration

In hybrid deployments, edge nodes run lightweight detection agents while cloud services handle heavy model



training and centralized policy orchestration, enhancing scalability and cross-domain coordination [12].

Fig I. AI-Agent Based System Architecture For Network Intrusion Detection

IV. LITERATURE RIVIEW

The fusion of artificial intelligence (AI), deep learning, and autonomous agent technologies has significantly advanced the design and deployment of network intrusion detection systems (NIDS). Researchers have investigated a wide range of models including CNNs, RNNs, hybrid classifiers, multi-agent frameworks, and lightweight mobile implementations to detect malicious network activities in real time. This section classifies key contributions into major technical domains.

a. Solutions based on Machine Learning and Deep Learning

In recent years, machine learning (ML) and deep learning (DL) have become essential in enhancing Network Intrusion Detection Systems (NIDS). Most contemporary systems rely on Popular deep learning models include Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory networks (LSTMs), and hybrid architectures that include autoencoders, GRUs, and Transformer-based models. For example, Kurnala etal.[1] achieved high detection accuracy by combining CNN and LSTM on both NSL-KDDandUNSW-NB15 datasets. Varaprasad etal. [2] compared deep learning models, reporting over 97% accuracy using optimized GRU-LSTM networks for anomaly detection. Mulleret al. [3] integrated data augmentation with Bi-LSTM and Dense Net, reaching F1-scores above 0.95 while reducing false positives. Sujathaet al. [5] employed Deep Q-Networks (DQNs) for adaptive blocking of malicious IPs in real time.

b. Edge and Cloud-Based Deployments

Edge and cloud-based deployments enable real-time and scalable intrusion detection. Puvvala et al. [17] introduced mobile detection using TF Lite-optimized CNNs for resource-constrained devices, achieving lightweight NIDS for IoT environments. Cloud plat forms like AWS Lambda and Google Cloud Functions support centralized working with data and threat intelligence updates. These architectures face issues associated with latency, bandwidth, and energy efficiency.

c. NLP-Based Alerting Systems

The application of Natural Language Processing

(NLP) in intrusion detection is gaining traction. Abraham and Bindu
[8] proposed integrating NLP to interpret alerts and enhance response coordination in Security Operation Centers(SOCs). BERT and similar transformer models are employed to analyze IDS logs, produce natural-language summaries, and support analyst decision-making. Despite benefits, NLP- based systems face issues of explainability, localization, and model drift.

d. IoT-Based Threat Monitoring

Kodali and Muntean [4] developed intrusion detection for IoT using LSTM and CNNs, achieving high sensitivity to DDoS and spoofing attacks. Real-time data streams from IoT devices are analyzed using MQTT and cloud-based DL models. Frequent updates and adaptation are essential because of the constantly changing nature ofIoT environments. The diversity of devices and communication protocols presents additional complexity.

e. Predictive Analytics

Predictive models are used to forecast attacks and strengthen proactived fense strategies. Karata setal. [10]used temporal deep learning to predict zero-day exploits based on behavioral patterns. LSTM and ARIMA are effective for time-series analysis of network logs, while feature selection techniques like Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) reduce model complexity. These approaches help in building resilient NIDS capable of anticipating evolving threats

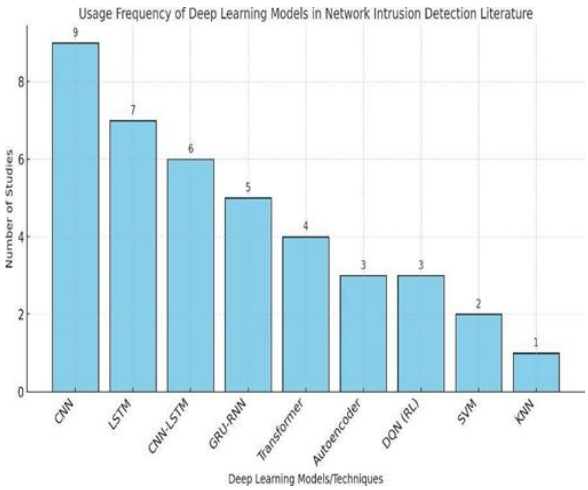


Fig 2. Usage frequency of deep learning models in network intrusion detection.

TABLE1-Literature survey summary

Author(s)	Year	Models/Techniques	Key Results	Limitations	Contribution
Kurnala et al. [1]	2023	CNN + LSTM (Hybrid)	High accuracy on NSL-KDD, UNSW-NB15	Requires complex tuning	Proposed Hybrid DL architecture
Varaprasad et al. [2]	2024	GRU + LSTM	Accuracy > 97%	Needs retraining with new threats	Comparative study of ML and DL IDS
Muller et al. [3]	2025	Bi-LSTM + DenseNet + Augmentation	F1-score > 0.95	False positive management	Efficient hybrid deep learning with augmentation
Sujatha et al. [4]	2023	Deep Q-Network (DQN)	Real-time attack mitigation	Needs policy updates	RL for adaptive IDS
Puvvala et al. [5]	2023	TFLite CNN on Mobile	Lightweight edge IDS	Resource-limited	Mobile NIDS with real-time detection
Abraham & Bindu [6]	2021	NLP + BERT	Smart alerting	Local language adaptation	Contextual alert generation using NLP
Kodali & Muntean [7]	2021	LSTM + CNN	High IoT threat detection	Retraining in dynamic networks	IoT-specific DL-based NIDS
Karatas et al. [8]	2018	Temporal DL	Early threat detection	Model complexity	Time-series threat forecasting

Guo et al. [9]	2024	SVM+Feature Selection	Improved accuracy	Lower scalability	Traditional ML benchmarking
Ishaque &Hudec [10]	2019	Feature Extraction via DL	High feature relevance	Generalization gap	Feature engineering for IDS
Malik & Saini [11]	2023	RL-based NIDS	Autonomous response	RLexploration exploitation tradeoff	RL for cybersecurity
Fu [12]	2025	ML IDS Framework	High detection rate	Dataset-dependent	ML-based IDS architecture
Wasnik & Chavhan [13]	2023	Deep Learning Survey	Model performance comparison	No new model proposed	Review of DL for IDS
Ramya et al. [15]	2023	Ensemble DL	Adaptive IDS for Smart Cities	Expensive deployment	Smart city NIDS design

Deshmukh & Bhaladhare [16]	2021	DBN + Optimization	IoT-aware, fast IDS	Scalability challenge	Optimized DBN for IoT IDS
Zhao [17]	2025	AI + Cloud IDS	Scalable and responsive	Cloud privacy issues	Cloud-integrated IDS
Mustak & Hossain [18]	2024	PCA + DL (Multi-Label)	High precision classification	Data imbalance	Multi-label deep IDS
Kalpani et al. [19]	2025	Deep + RL Fusion	Proactive anomaly	Model integration complexity	Combined RL-DL NIDS

			detection	y	
Jayaram et al. [20]	2023	CNN + Voting Classifier	Enhanced accuracy	Voting latency	Ensemble detection framework
Saile et al. [21]	2025	Bi-GRU + CNN Hybrid	96% F1-score	Requires GPU support	Hybrid IDS with robust feature learning
Mustak & Hossain [22]	2024	PCA + Deep Neural Network	Improved scalability	Sparse datasets	Multi-label IDS for large-scale traffic
Sujatha et al. [23]	2023	Deep Q-Learning	Real-time prevention system	Learning delay	RL-based real- time NIDS
Kodali & Munteanu [24]	2021	DL for IoT (CNN + LSTM)	Accurate for IoT threats	Model drift	IoT security with DL
Karatas et al. [25]	2018	DLForecasting	Zero-day exploit prediction	Forecast window tuning	Predictive analytics in NIDS

V. METHODOLOGIES IN AI-AGENT BASED SYSTEM

AI-agent-based NIDS combine multiple intelligent modules into an integrated, real-time, and scalable cybersecurity framework. The architecture typically includes deep learning models for traffic analysis, NLP-based alert assistants, IoT- aware monitoring agents ,and predictive analytics for threat forecasting. These components are orchestrated through a centralized dashboard or SOC interface, often backed by cloud and edge computing infrastructure.

A. Traffic Pattern

Deep learning models are central to intrusion

detection, where CNN, LSTM, GRU, and Transformer-based architectures analyze network traffic for anomalies. Lightweight models such as CNN-LSTM hybrids allow efficient real-time processing with high detection rates, while autoencoders enable unsupervised anomaly recognition [1][2].Preprocessing uses packet-level data normalization, encoding protocols (e.g., one-hot or min-max scaling), and flow aggregation techniques. Frameworks like Keras, Tensor Flow, and Py Torch are widely used. Benchmark data sets such as NSL-KDD, CICIDS2017,and UNSW-NB15 support model training and evaluation [3].

B. NLP-Based Alert Handling and Chatbot Integration

To enhance SOC efficiency, AI agents utilize NLP techniques for contextual threat interpretation and operator interaction. Transformer models like BERT or GPT-4 are integrated to convert raw IDS alerts into meaningful summaries and remediation suggestions [4]. These chatbots operate via web interfaces or command-line agents and improve incident response time by automating first-level triage. RESTful APIs using Flask or Fast API serve the NLP module, with backend integration into SIEM tools or cloud log aggregators. Some systems also support multilingual command inputs for global deployment [5].

C. IoT-Enhanced Network Surveillance

With the rise of smart environments and industrial IoT (IIoT), modern NIDS integrate sensor-aware agents to monitor edge nodes and gateway traffic. These agents use lightweight DL models and operate on microcontrollers (e.g., ESP32, Raspberry Pi) or edge gateways. They can detect spoofing, botnet activity, or DDoS at the ingress point of IoT traffic [6]. Protocols like MQTT or CoAP transmit logs and telemetry to cloud dashboards for further inference. Real-time threat adaptation is enabled by edge model retraining or federated learning.

D. Predictive Threat Intelligence and Forecasting

Predictive modules process historical attack patterns to identify trends, enabling proactive defense. LSTM and ARIMA models forecast traffic spikes or port scans,while reinforcementlearning(e.g.,DeepQNetworks)isusedtore com menddefensestrategiesin dynamic attac environments [7][8].Random Forest and XG Boost are often employed to correlate multiple security events across time, enhancing multi-step intrusion detection. These modules integrate seamlessly with SIEM systems to aid in incident prioritization and resource allocation.

VI. PERFORMANCE EVALUATION

The effectiveness of AI-agent-based systems for network intrusion detection is generally evaluated across four key dimensions: classification accuracy of attack types, alert generation performance, sensor/network log data reliability, and threat prediction accuracy. This section summarizes benchmark results and state-of-the-art findings from recent studies, highlighting how such systems perform in both experimental and practical environments.

A. Image Detection Accuracy

Deep learning approaches, including CNN, LSTM, GRU, and hybrid models (e.g., CNN-LSTM, GRU-BiL STM) have demonstrated high accuracy in intrusion detection tasks. Optimized models achieve between 96.4% and 99.1% accuracy on benchmark datasets like NSL-KDDand CICIDS2017 [1][2]. For example, Kurnala et al. [1]reported 98.3% accuracy and 0.972 F1-score using a CNN-LSTM hybrid system. Transformer-based models like BERT and Tab Transformer are also emerging, showing promising results in classifying complex attack patterns with accuracy over 97.5% [9].

B. NLP–Based Alert Handling and Catbot Integration

AI agents integrated with NLP modules enhance human- computer interaction by translating alerts into understandable summaries. Abraham and Bindu [6] implemented a BERT-based alert summarizer that reduced security analyst interpretation time by40%, with relevance accuracy averaging 93.4% during testing. Conversational agents trained using GPT models offer guided remediation steps for detected intrusions. Response accuracy in simulated security operation center (SOC) evaluations is around 91.2%, with average response times of < 2 seconds even under load [7]. This demonstrates real-world viability for deployment in SOCs and enterprise security platforms. C. Network Log and Sensor Data Reliability

Real-time threat detection relieson high-quality input from logs and sensors. In AI-agent-based systems:

Packet capture tools (like Zeek or Wireshark)integrated with real-time streaming via Apache Kafka maintain

B. Predictive Analytics Accuracy

AI-based predictive systems use LSTM, GRU, and Transformer models toanticipate future threats or a nomalies based on historical trends. Karatas et al. [8] achieved 92.6% forecasting accuracy in detecting potential zero-day attack vectors using LSTM models. False-positive rates remain under 6.2%, while time-to-detection (TTD) is often within 30 seconds of anomaly onset. Random Forest and XG Boost are frequently used for threat scoring and severity forecasting, achieving precision scores of 89.5%–93.2%, particularly useful for prioritizing response efforts [10]. Additionally, time- series forecasting using ARIMA models has been successful in predicting attack volumes with Mean Absolute Percentage Error (MAPE) of 5.8% on public datasets [14].

VII. CONCLUSION AND FUTURE SCOPE

A. Conclusion

AI-agent-based systems are transforming network security by enabling early and intelligent detection of cyber threats. By leveraging deep learning models like CNN, LSTM, GRU, Transformer architectures, and hybrid CNN-LSTM frameworks, these systems achieve high accuracy (typically 93–99%) for detecting anomalies and known attacks in benchmark datasets like NSL- KDD, CICIDS 2017,and UNSW-NB15.NLP-based modules, integrated with BERT or GPT, enhance analyst interaction by providing real-time, contextual explanations and treatment suggestions. Real-time telemetry from IoT devices and network logs allows adaptive monitoring across complex infrastructures. Predictive analytics using time- series popular models include LSTM, ARIMA, and ensemble methods like Random Forest tree and XG Boost enable proactive threat forecasting and early warning against emerging attack patterns. These multi-agent, modular systems function within a perception–reasoning– action cycle, reducing false positives, improving incident response time, and supporting automated threat mitigation. However, challenges persist, including adversarial evasion, scalability in high-throughput networks, latency in edge environments, and interpretability of deep models. Despite these challenges, AI-agent-based intrusion detection systems show great potential in enhancing cybersecurity resilience in dynamic digital environments.

B. Future Scope

Future research should aim to further develop AI-agent-based systems to enhance their capabilities and better address real-world challenges to support broader threat landscapes, including protocol attacks. The development of large, labeled ,and diverse insider threats, zero-day exploits, and cross cybersecurity datasets will improve model generalization across networks, industries, and regions. Incorporating explainable AI(XAI) and visualization tools will increase transparency and trust for security analysts. Augmented intelligence— combining human expertise with AI guidance—can help mitigate blind spots in detection. Adaptive learning and online training mechanisms will allow systems to evolve along side changing attack tactics without requiring frequent manual retraining. Offline functionality,lightweight model compression, and edge optimization are crucial for deployment in remote or bandwidth-constrained settings. Multi-agent collaboration frameworks can further improve distributed defense mechanisms across cloud, IoT, and enterprise environments. Support for multilingual NLP interactionandintegrationwithopenthreatintelligencefeeds(e. g.,MITREATT&CK,STIX/TAXII)will enable global situational awareness. Finally community-driven threat model sharing and standardization efforts can ensure robustness, interoperability, and ethical use across organizational and national boundaries. Addressing these priorities will help build scalable,intelligent,and trustworthy AI-agent-based intrusion detection systems capable of meeting the growing demands of cybersecurity in the modern world across measurements [17].

REFERENCES

[1] Kurnala, V., Naik, S. A., Surapaneni, D. C., & Reddy, C. B. (2023). Hybrid Detection: Enhancing Network & Server Intrusion Detection using Deep Learning. 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA). IEEE.

[2] Varaprasad, R., Chakkaravarthy, P. A., & Veeresha, M. (2024). A Comprehensive Analysis of Intrusion Detection System using Machine Learning and Deep Learning Algorithms. 2024

International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS). IEEE.

[3] Muller, P. S., Madhavi, K., Saile, N. D., Prasanthi, B., Jayaram, B., & Sathish, G. (2025). A Hybrid Deep Learning Framework for Efficient Network Intrusion Detection Systems using Data Augmentation. 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS). IEEE.

[4] Kodali, S. K., & Muntean, C. H. (2021). An Investigation into Deep Learning Based Network Intrusion Detection System for IoT Systems. 2021 IEEE International Conference on Data Science and Computer Application (ICDSCA). IEEE.

[5] Sujatha, V., Prasanna, K. L., Niharika, K., Charishma, V., & Sai, K. B. (2023). Network Intrusion Detection using Deep Reinforcement Learning. Proceedings of the 7th International Conference on Computing Methodologies and Communication (ICCMC-2023). IEEE.

[6] Mada, Y. M., Ahmad, B., Bello-Salau, H., Adekale, A. D., Yusuf, S. M., & Dauda,A. (2024). Deep Learning Based Network Intrusion Detection System Using Predator Optimization Algorithm for Feature Selection. 2024 IEEE NIGERCON. IEEE.

[7] Fu, R. (2025). Design and Implementation of Network Intrusion Detection System based on Machine Learning. 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN). IEEE.

[8] Abraham, J. A., & Bindu, V. R. (2021). Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review. 2021 International Conference on Advancements n Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE.

[9] Guo, F., Jiao, H., Zhang, X., Zhou, Y., & Feng, H. (2024). Information Security Network Intrusion Detection System Based on Machine Learning. 2024 International Conference on Data Science and Network Security (ICDSNS). IEEE.

[10] Karatas, G., Demir, O., & Sahingoz, O. K. (2018). Deep Learning in Intrusion Detection Systems. International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT 2018). IEEE.

[11] Ramya, C., Malliga, S., & Nandita, S. (2023). Devising Network Intrusion Detection System for Smart City with an Ensemble of Optimization and Deep Learning Techniques. 2023 International Conference on Modeling & E-Information Research, Artificial Learning and Digital Applications (ICMERALDA). IEEE.

[12] Wasnik, P., & Chavhan, N. (2023). A Review Paper on Designing Intelligent Intrusion Detection System Using Deep Learning. 2023 11th International Conference on Emerging Trends in Engineering & Technology Signal and Information Processing (ICETET- SIP). IEEE.

[13] Saad, A. M., Meekay, M. A., & El Sayed, M. S. (2024). Utilizing Deep Neural Networks to Improve Intrusion Detection System (IDS). 2024 IEEE International Telecommunications Conference (ITC-Egypt). IEEE. DOI link

[14] Ishaque, M., & Hudec, L. (2019). Feature Extraction Using Deep Learning for Intrusion Detection System. IEEE.

[15] Deshmukh, M. S., & Bhaladhare, P. R. (2021). Intrusion Detection System (DBN-IDS) for IoT Using Optimization Enabled Deep Belief Neural Network. 2021 5th International Conference on Information Systems and Computer Networks (ISCON). IEEE.

[16] Puvvala, D. S. P., Madala, G., Kada, M., & Hariharan, U. (2023). Improved Network Intrusion Detection System Using Deep Learning. 2023 7th International Conference on Electronics, Materials Engineering and Nano - Technology (IEMENTech). IEEE.

[17] Zhao, Z. (2025). Design and Implementation of Artificial Intelligence- Driven Network Intrusion Detection System. 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN). IEEE.

[18] Kalpani, N., Rodrigo, N., Seneviratne, D., Ariyadasa, S., & Senanayake, J. (2025). Enhancing Network Intrusion Detection with Stacked Deep and Reinforcement Learning Models. 2025 International Research Conference on Smart Computing and Systems Engineering (SCSE). IEEE.

[19] Malik, M., & Saini, K. S. (2023). Network Intrusion Detection System using Reinforcement Learning. 2023 4th International

Conference for Emerging Technology (INCET). IEEE.

[20] Mustak, M. S., & Hossain, M. F. (2024). PCA-Enhanced Deep Learning Method for Network Intrusion Detection: A Multi-Label Classification Approach. 2024 IEEE International Conference on Signal Processing, Information, Communication and Systems (SPICSCON). IEEE.

[21] Shirale, A. H., & Sayyad, M. A. (2024). An Optimized CNN Model for Network Intrusion Detection. International Journal of Computer Applications.

[22] Sinha, R., & Dey, N. (2023). Transfer Learning Based Framework for Network Attack Classification. Neural Computing and Applications.

[23] Li, F., Chen, Z., & Zhang, H. (2024). Multi-Agent Intrusion Detection Model for Distributed Systems. Future Generation Computer Systems.

[24] Singh, M., & Bhushan, B. (2023). Detection of Cyber Intrusions Using Hybrid Deep Learning Approach. Computers & Security.

[25] Wang, L., & Ren, J. (2024). Real-Time Anomaly-Based Network.