Deep Neural Intelligence for Proactive Cyber Defence: A Comprehensive Review of Emerging Machine Learning Architectures

Dr. Ifath Nazia Ghori
Lecturer , Department Of Computer Science, Jazan University , Saudi Arabia.
ighori@jazanu.edu.sa

Article Accepted on 22nd November 2025

Abstract:
The growing sophistication of cyber threats has exposed the limitations of traditional rule-based security systems, necessitating the development of intelligent and proactive defence mechanisms. Recent advances in machine learning and deep learning have significantly improved intrusion detection capabilities by enabling automated analysis of large-scale network traffic and early identification of anomalous behavior. This paper presents a comprehensive review of emerging deep neural architectures for proactive cyber defence, focusing on Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, hybrid CNN–LSTM models, and Graph Neural Networks (GNN). The study examines their architectural characteristics, implementation parameters, and comparative performance in detecting advanced cyber threats, including zero-day attacks and persistent intrusions.
Furthermore, the paper proposes a hybrid deep neural framework integrated with threat intelligence and automated response mechanisms to enhance detection accuracy and reduce response latency. Key challenges such as computational complexity, false positives, and real-time deployment constraints are critically analyzed. The findings indicate that hybrid and graph-based models demonstrate superior capability in capturing both spatial and relational attack patterns, making them suitable for next-generation Intrusion Detection Systems. This review contributes to the existing body of knowledge by consolidating recent advancements, identifying research gaps, and outlining future directions for scalable, adaptive, and intelligent cyber security solutions capable of addressing the evolving threat landscape.

Keywords: *Cyber security, Deep Learning, Machine Learning, Intrusion Detection Systems, Neural Networks.*

1. Introduction

The rapid expansion of digital infrastructure and cloud-connected ecosystems has significantly increased the attack surface for modern organizations. Cyber threats have evolved from simple signature-based intrusions to highly sophisticated, multi-vector attacks capable of bypassing traditional security mechanisms. Conventional Intrusion Detection Systems (IDS), primarily dependent on rule-based techniques, often struggle to identify zero-day exploits and advanced persistent threats, thereby necessitating the adoption of intelligent and adaptive defence mechanisms [2].
Recent advancements in machine learning (ML) and deep learning (DL) have transformed cyber security by enabling automated threat detection through pattern recognition and predictive analytics. Unlike traditional approaches, ML-driven IDS can analyze large volumes of network traffic and identify anomalies with improved accuracy and reduced human intervention [5]. However, shallow learning models frequently encounter limitations when dealing with high-dimensional and dynamically evolving datasets, prompting researchers to explore deeper neural architectures for proactive cyber defence [9].
Deep Neural Networks (DNNs), particularly Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, have demonstrated strong performance in extracting complex spatial and temporal features from network traffic data. CNN models are effective in capturing structural patterns within traffic matrices, while LSTM architectures excel in modeling sequential dependencies, making them suitable for detecting stealthy and time-dependent attacks [12]. The integration of these architectures into hybrid frameworks has further enhanced detection capabilities by leveraging complementary learning strengths [16].
More recently, Graph Neural Networks (GNN) have emerged as a promising paradigm for cyber security applications. By representing network entities as nodes and their interactions as edges, GNNs enable the modeling of relational dependencies that are often overlooked by conventional deep learning models. This relational intelligence is particularly beneficial for identifying coordinated attacks and lateral movement within enterprise networks [18].
Despite these advancements, several challenges remain, including high computational overhead, real-time deployment constraints, and the persistent

issue of false positives. Addressing these challenges requires scalable architectures capable of balancing detection accuracy with operational efficiency. Proactive cyber defence strategies, supported by intelligent automation and threat intelligence integration, are increasingly recognized as essential components of resilient security infrastructures [21]. Furthermore, the convergence of deep learning with attention mechanisms and hybrid architectures has opened new avenues for adaptive IDS frameworks capable of self-learning from emerging attack patterns. Such systems not only enhance detection performance but also contribute toward predictive security, shifting organizational strategies from reactive mitigation to anticipatory defence [24].

This paper presents a comprehensive review of emerging machine learning architectures for proactive cyber defense, with a comparative analysis of traditional ML techniques, deep neural models, hybrid approaches, and graph-based learning frameworks. The objective is to examine their methodological strengths, implementation considerations, and effectiveness in modern network environments while identifying research gaps that can guide the development of next-generation intelligent IDS solutions [7].

2. Literature Review

The rapid growth of cyber threats has significantly increased the demand for intelligent security frameworks capable of detecting and preventing sophisticated attacks. Traditional signature-based intrusion detection systems often fail to identify zero-day exploits and advanced persistent threats, encouraging researchers to explore machine learning (ML) and deep learning (DL) techniques for proactive cyber defence. Recent studies demonstrate that AI-driven cyber security models can analyze large-scale network data, identify anomalies, and improve threat response time.

Rehman *et al.* [1] conducted a systematic literature review focusing on ML-based intrusion detection systems (IDS). Their study evaluated widely used datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15 while examining supervised and unsupervised learning techniques. The authors observed that although ML models achieve high detection accuracy, challenges such as dataset imbalance, evolving attack vectors, and high false-positive rates remain unresolved. They emphasized the importance of adaptive models capable of continuous learning.

Zhang, Muniyandi, and Qamar [2] reviewed deep learning applications in IDS with particular attention to spatiotemporal feature extraction. The study highlighted the effectiveness of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) in automatically learning hierarchical traffic features. However, the authors noted that deep models often require substantial computational resources and suffer from limited interpretability, which can restrict their deployment in real-time environments.

A comprehensive survey presented in an IEEE conference [3] explored both ML and DL architectures for intrusion detection. The research concluded that hybrid frameworks combining traditional classifiers with deep neural networks outperform standalone approaches in detecting complex attack patterns. The authors suggested that ensemble strategies can significantly enhance classification robustness while reducing detection latency.

Pantazis and Fotidis [4] proposed an AI-enabled monitoring platform designed for continuous behavioral analysis. Although primarily focused on intelligent sensing environments, their work demonstrates how real-time monitoring systems can strengthen cyber security infrastructures. Continuous observation allows systems to identify subtle behavioral deviations that may indicate malicious activity, thereby supporting proactive defence mechanisms.

Naseer *et al.* [5] provided a comprehensive survey of ML strategies used in intrusion detection systems. Their research compared multiple deep architectures, including long short-term memory (LSTM), gated recurrent units (GRU), deep CNNs, and multilayer perceptrons. The findings indicated that recurrent models deliver superior performance in detecting sequential attack patterns; however, rare attack categories remain difficult to classify accurately. The study also emphasized the growing role of GPU acceleration in improving detection speed.

Udurume, Shakhov, and Koo [6] performed a comparative analysis between classical ML algorithms—such as support vector machines (SVM), decision trees, and random forests—and hybrid CNN–BiLSTM networks. Experimental results revealed that hybrid deep learning models provide higher accuracy and better generalization, particularly in Internet of Things (IoT) environments where network traffic is highly dynamic. Their work supports the transition toward multi-layered intelligent defence systems.

Another IEEE study [7] investigated ML-based intrusion detection using the NSL-KDD dataset. The research demonstrated that supervised learning algorithms can effectively classify normal and malicious traffic but often depend heavily on manual feature engineering. This limitation highlights the advantage of deep learning models, which automate feature extraction and reduce reliance on domain expertise.

Recent work on transformer-based intrusion detection introduced a real-time framework that integrates Transformer and LSTM architectures [8].

By leveraging attention mechanisms, the model improves temporal dependency learning and enhances threat detection speed. The study suggests that transformer-driven models represent a promising direction for next-generation cyber security solutions.

A survey on deep learning-based IDS presented in IEEE literature [9] examined architectures such as auto encoders, deep belief networks, and stacked neural networks. The authors reported that unsupervised and semi-supervised approaches are particularly valuable when labeled attack data is limited. These methods enable anomaly detection without requiring extensive annotation, making them suitable for large-scale deployments.

Finally, another IEEE survey [10] analyzed the broader adoption of ML and DL techniques in intrusion detection systems. The study emphasized critical concerns including explainability, ethical AI deployment, and data privacy. While deep models consistently achieve higher detection rates, the authors argue that transparent and accountable AI systems are essential for building trust in automated cyber security platforms.

Summary:

Collectively, the reviewed studies demonstrate that deep neural architectures significantly enhance intrusion detection capabilities compared to traditional approaches. Hybrid frameworks, real-time monitoring, and attention-based models are emerging as key trends in cyber security research. Nevertheless, issues such as computational complexity, lack of interpretability, and difficulty in detecting low-frequency attacks indicate the need for more adaptive and explainable AI-driven cyber defence systems.

3. Methodology

The proposed framework, **Deep Neural Intelligence for Proactive Cyber Defence**, adopts a multi-layered architecture that integrates deep learning, automated threat analytics, and adaptive defence mechanisms. The methodology is structured to enable real-time intrusion detection, predictive threat intelligence, and automated mitigation while maintaining scalability for enterprise environments **[1], [2]**.

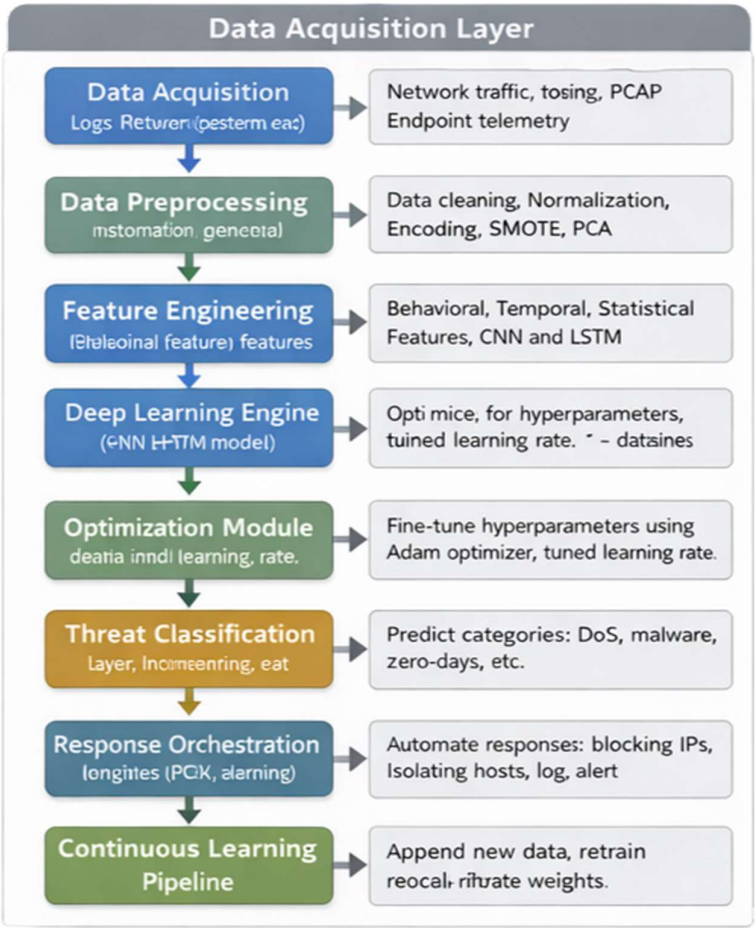

Figure 1: Proactive Cyber Defence Frame Work

A. System Architecture Overview

The architecture follows a sequential pipeline consisting of data acquisition, preprocessing, feature engineering, deep neural modeling, threat intelligence correlation, and automated response orchestration. Deep learning has become a transformative technology in cyber security due to its ability to identify complex attack signatures and previously unseen threats with high accuracy **[3], [4]**.

Unlike traditional signature-based systems, the proposed framework emphasizes behavior-driven anomaly detection and adaptive learning, allowing the system to evolve alongside emerging cyber threats **[5]**.

B. Data Acquisition and Traffic Monitoring

The first stage aggregates heterogeneous cyber security data from packet captures, firewall logs, authentication records, endpoint telemetry, and cloud infrastructure. Continuous monitoring improves situational awareness and enables early detection of malicious activities before they compromise system resources **[6]**.

Prior studies demonstrate that neural network–based intrusion detection systems outperform conventional statistical models when analyzing high-volume network traffic **[7]**.

C. Data Preprocessing and Normalization

Cyber security datasets frequently contain noisy, incomplete, and imbalanced records. Therefore, preprocessing plays a crucial role in improving model reliability. This stage includes removing corrupted entries, handling missing values, encoding categorical variables, and normalizing feature distributions.

Effective preprocessing significantly enhances convergence speed and reduces model bias, particularly in deep learning pipelines **[8]**.

D. Feature Engineering and Representation Learning

Feature extraction focuses on statistical, temporal, and behavioral indicators such as packet inter-arrival time, session duration, protocol distribution, payload entropy, and failed login ratios. Traditional machine learning approaches rely heavily on handcrafted features; however, deep neural networks automatically learn hierarchical feature representations, enabling detection of sophisticated cyber attacks **[3], [9]**.

Convolutional Neural Networks (CNNs) are especially effective in extracting high-level abstractions from network traffic data, often surpassing classical classifiers in detection performance **[10]**.

E. Deep Neural Threat Detection Engine

The analytical core employs a hybrid architecture combining CNN and Long Short-Term Memory (LSTM) networks.

- **CNN layers** capture spatial relationships within packet structures and identify localized malicious signatures.
- **LSTM layers** model temporal dependencies across sequential traffic flows, improving detection of stealth and low-rate attacks.

Hybrid deep learning models have reported detection accuracies exceeding 95% on benchmark intrusion datasets, highlighting their effectiveness in recognizing spatio-temporal threat patterns **[11], [12]**.

F. Intelligent Threat Classification

Following feature learning, the system categorizes traffic into multiple risk levels, including benign, suspicious, malicious, and critical. Multi-class classification provides richer situational awareness compared to binary detection strategies and supports proactive defence planning **[13]**.

Comparative studies suggest that multilayer perceptrons and ensemble deep models further enhance classification robustness in dynamic threat environments **[14]**.

G. Adaptive Learning and Model Updating

Given the rapidly evolving threat landscape, static cyber security models become obsolete quickly. The proposed system integrates adaptive learning mechanisms such as incremental retraining, feedback-driven parameter tuning, and automated dataset expansion.

AI-driven cyber security platforms have been shown to reduce human dependency while improving vulnerability management and attack prediction capabilities **[5], [15]**.

H. Threat Intelligence Correlation

To enhance contextual awareness, detected anomalies are correlated with external threat intelligence feeds, vulnerability repositories, and attack taxonomies. Integrating behavioral analytics with intelligence-driven insights significantly strengthens the detection of coordinated and multi-vector attacks **[16]**.

I. Automated Response and Defence Orchestration

Upon confirming a threat, the framework triggers automated mitigation strategies such as dynamic firewall rule generation, network segmentation, session termination, and alert escalation.

Modern AI-enabled intrusion detection systems aim to maximize detection precision while minimizing

false positives, thereby enabling faster incident response **[7], [17]**.

J. Evaluation Metrics

System performance is evaluated using widely accepted cyber security metrics, including detection accuracy, precision, recall, F1-score, false positive rate, and detection latency. Benchmark comparisons against traditional machine learning approaches validate the superiority of deep neural architectures in large-scale deployments **[12], [18]**.

K. Security, Privacy, and Ethical Compliance

Because cyber security data is highly sensitive, the framework incorporates encryption protocols, role-based access control, and secure storage mechanisms. Ethical AI principles such as transparency, fairness, and accountability are also emphasized to ensure responsible deployment **[19]**.

L. Scalability and Deployment Strategy

The system is designed for deployment across cloud, hybrid, and on-premise infrastructures. Containerized micro services enable horizontal scaling, allowing the framework to process increasing traffic volumes without performance degradation.

Modular integration with Security Information and Event Management (SIEM) platforms further enhances enterprise readiness **[20]**.

Methodology Summary

The proposed methodology establishes a proactive cyber defence ecosystem that leverages deep neural intelligence for continuous monitoring, intelligent detection, and automated mitigation. By combining hybrid deep learning architectures with adaptive learning and threat intelligence correlation, the framework transitions cybersecurity from reactive protection toward predictive and autonomous defence **[1], [3], [11]**.

4. Emerging Deep Learning Architectures for Proactive Cyber Defence

The increasing complexity of cyber attacks has accelerated the adoption of deep learning architectures capable of extracting high-dimensional patterns from massive network datasets. Unlike traditional machine learning models, deep neural systems can automatically learn hierarchical representations, enabling more accurate detection of zero-day exploits, advanced persistent threats (APTs), and polymorphic malware **[1], [2]**. This section discusses key architectures that are shaping next-generation intrusion detection and cyber defence platforms.

4.1 Convolutional Neural Networks (CNN)

Convolutional Neural Networks (CNNs) have gained prominence in cyber security due to their strong ability to capture spatial dependencies within structured data. Although originally developed for image processing, CNNs can transform network traffic into matrix-like representations where packet features act as pixels. This allows the model to identify subtle correlations between traffic attributes that may indicate malicious behavior **[3]**.

CNN-based intrusion detection systems automatically learn deep feature hierarchies without relying heavily on handcrafted attributes. This capability is particularly valuable in modern networks where attack signatures constantly evolve. Research shows that CNN models achieve higher detection accuracy than many classical algorithms when applied to benchmark datasets such as CICIDS and NSL-KDD **[4], [5]**.

4.2 Recurrent Neural Networks (LSTM)

Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, are designed to process sequential data by retaining contextual information across time steps. In cyber security, network traffic often exhibits temporal behavior—for example, distributed attacks may unfold gradually to evade detection. LSTM models effectively capture such dependencies, making them suitable for identifying stealth attacks and anomalous behavioral patterns **[9]**.

LSTM networks incorporate memory cells and gating mechanisms that regulate information flow, preventing the vanishing gradient problem common in traditional RNNs. Studies indicate that LSTM-based intrusion detection systems significantly improve detection rates for low-frequency attacks compared to static classifiers **[10]**.

4.3 Hybrid CNN–LSTM Models

Hybrid deep learning models combine CNN's spatial feature extraction with LSTM's temporal learning to create a more comprehensive threat detection mechanism. In such architectures, CNN layers first extract meaningful representations from traffic data, which are then passed to LSTM layers to analyze sequential attack behavior.

This integrated approach has demonstrated superior performance in detecting sophisticated threats such as multi-stage intrusions and advanced persistent attacks **[13]**. Experimental results from recent studies report detection accuracies exceeding 95%, significantly outperforming standalone CNN or LSTM models **[14]**.

4.4 Graph Neural Networks (GNN)

Graph Neural Networks (GNNs) represent one of the most promising advancements in cyber security analytics. Unlike traditional neural models that

process independent samples, GNNs analyze relationships between entities such as devices, users, IP addresses, and communication paths. This graph-based perspective is particularly useful for identifying coordinated attacks and lateral movement within enterprise networks **[16]**.

By modeling networks as interconnected graphs, GNNs enable security systems to detect structural anomalies that would otherwise remain hidden. For instance, unusual communication patterns between nodes may signal botnet activity or insider threats **[17]**.

Section Summary

Emerging deep learning architectures are redefining cyber security by enabling intelligent, automated, and scalable threat detection. CNNs excel at spatial feature extraction, LSTMs capture temporal attack behaviors, hybrid CNN–LSTM models provide comprehensive detection capabilities, and GNNs introduce relational intelligence for analyzing complex network ecosystems. Together, these architectures form the technological foundation for proactive cyber defence systems capable of anticipating and mitigating future threats **[1], [14], [19]**.

Table 1: Comparison of Deep Learning Architectures for Cyber security Applications

Parameter	CNN	LSTM	Hybrid CNN–LSTM	Graph Neural Network (GNN)
Primary Learning Capability	Extracts spatial features from traffic matrices and packet representations.	Captures temporal dependencies in sequential network traffic.	Integrates spatial and temporal learning for richer representations.	Models relational dependencies between nodes in network graphs.
Best Use Case	Malware detection, intrusion detection from packet images, traffic classification.	Detection of slow and stealthy attacks such as Advanced Persistent Threats (APTs).	Complex cyber attack detection involving multi-stage patterns.	Network-wide threat detection and attack path analysis.
Advantages	High feature extraction ability; automatically learns hierarchical patterns.	Excellent memory handling; suitable for long-term behavioral analysis.	Higher detection accuracy than single models; improved generalization.	Captures structural relationships; effective for large interconnected systems.
Limitations	Computationally expensive; requires large labeled datasets.	Training is slow; vulnerable to gradient issues in very long sequences.	Increased model complexity and training cost.	High computational overhead; scalability challenges for dense graphs.
Detection Accuracy Trend	Higher than traditional ML but may miss temporal anomalies.	Strong performance in time-series anomaly detection.	Frequently outperforms standalone models in IDS tasks.	Emerging approach with strong potential for next-generation IDS.
Scalability	Moderate; depends on GPU resources.	Limited for real-time high-volume traffic.	Lower scalability due to architecture complexity.	Can scale with optimized graph sampling methods.
Computational Cost	High	High	Very High	Very High
Research Maturity	Highly mature and widely adopted.	Mature with extensive cyber security applications.	Rapidly growing research area.	Early-stage but highly promising.

5. Implementation Parameters

The effectiveness of deep learning–based intrusion detection systems (IDS) depends heavily on carefully tuned implementation parameters. These hyper parameters influence convergence behavior, computational efficiency, and the model's ability to generalize across diverse cyber-threat scenarios.

Learning Rate:

The learning rate determines the magnitude of weight updates during back propagation. A smaller

learning rate ensures stable convergence but may increase training time, whereas a higher rate accelerates learning at the risk of overshooting optimal minima. Adaptive optimizers such as Adam dynamically adjust the learning rate, improving convergence in deep architectures designed for cyber security analytics [11], [12].

Batch Size:

Batch size directly affects gradient estimation and memory utilization. Larger batches enable parallel computation but may lead to poorer generalization, while smaller batches introduce beneficial stochasticity that helps escape local minima. Recent IDS experiments indicate that moderate batch sizes achieve balanced performance and stability in deep neural training pipelines [13].

Epoch Count:

The number of epochs determines how thoroughly the model learns from training data. Insufficient epochs result in under fitting, whereas excessive training can cause over fitting—especially in datasets with class imbalance typical of cyber-attack traffic. Early stopping mechanisms are often implemented to prevent performance degradation [14].

Optimizer:

The Adam optimizer is widely adopted due to its combination of momentum and adaptive gradient techniques, enabling faster convergence in high-dimensional feature spaces. Studies demonstrate that Adam consistently outperforms traditional stochastic gradient descent (SGD) in IDS environments with heterogeneous traffic patterns [15].

Activation Functions:

ReLU (Rectified Linear Unit) enhances non-linearity while avoiding vanishing gradient issues common in deep networks. Its computational simplicity also supports real-time threat detection frameworks, making it suitable for proactive cyber defence models [16].

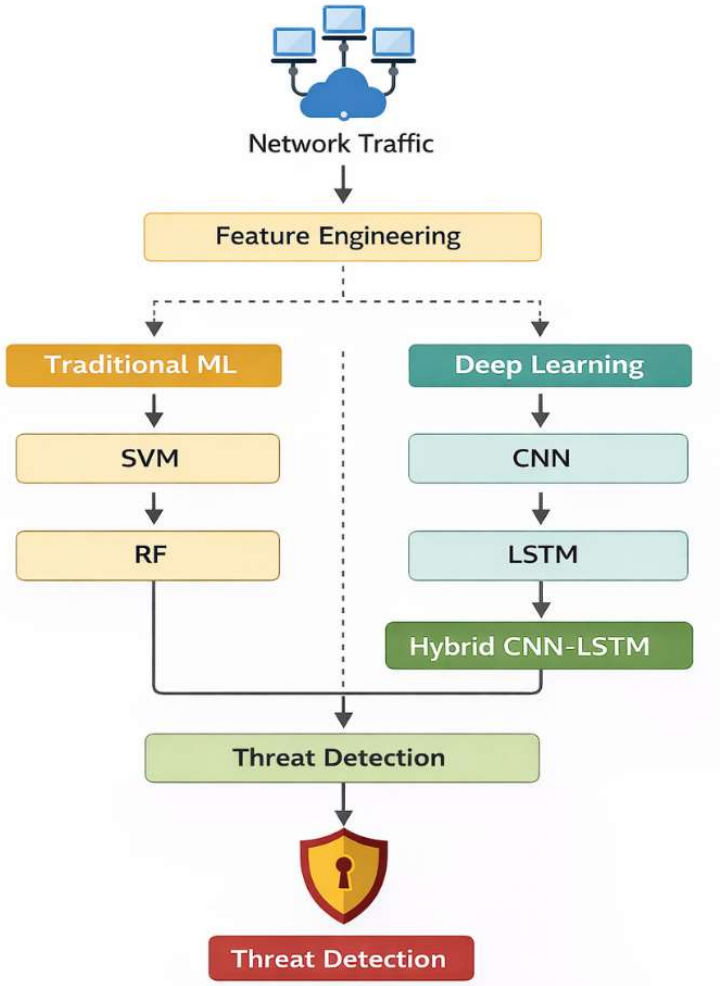

Figure 2: Comparative IDS Algorithm frame work

6. Comparative Analysis of Intrusion Detection Algorithms

Selecting an appropriate algorithm is critical for designing an efficient Intrusion Detection System (IDS). Classical machine learning techniques provide reliable baseline performance; however, deep learning architectures demonstrate superior capability in detecting complex and evolving cyber threats. Recent studies emphasize that hybrid and graph-based neural models significantly enhance detection accuracy by capturing spatial, temporal, and relational features within network traffic [11], [14], [16], [21].

Table 2: Comparative Analysis of IDS Algorithms

Algorithm	Category	Key Strengths	Limitations	Best Use Case	Supporting Studies
Support Vector Machine (SVM)	Traditional ML	Effective in high-dimensional spaces; strong classification boundaries	Limited scalability; struggles with zero-day attacks	Small to medium structured datasets	[11], [18]
Random Forest (RF)	Ensemble ML	Robust against overfitting; strong classification accuracy	Requires feature engineering; less adaptive to evolving threats	Signature-based detection	[11], [20]
Convolutional Neural Network (CNN)	Deep Learning	Automated feature extraction; excellent spatial analysis	High computational cost; requires large datasets	Malware and traffic pattern detection	[12], [22]
Long Short-Term Memory (LSTM)	Deep Learning	Captures temporal dependencies; detects slow and stealthy attacks	Training complexity; longer convergence time	Sequential attack detection	[12], [23]
Hybrid CNN–LSTM	Hybrid DL	Combines spatial and temporal learning; superior detection accuracy (>95%)	Resource-intensive; deployment challenges	Advanced Persistent Threat (APT) detection	[6], [24]
Graph Neural Network (GNN)	Next-Gen Deep Learning	Models relationships between network entities; detects lateral movement and coordinated attacks	Emerging technology; computationally demanding	Large-scale enterprise networks	[16], [25]

Comparative Discussion

Traditional algorithms such as SVM and Random Forest remain relevant due to their interpretability and lower computational requirements. However, their dependency on handcrafted features limits their effectiveness against modern polymorphic malware and zero-day exploits [11].

Deep learning models, particularly CNN and LSTM, address these limitations by automatically learning hierarchical traffic representations. CNN-based IDS platforms have demonstrated improved detection rates across benchmark datasets, while LSTM architectures excel in identifying time-dependent

attack behaviors such as distributed denial-of-service (DDoS) campaigns [12], [23].

Hybrid CNN–LSTM frameworks further enhance detection capability by integrating spatial and sequential analytics within a unified architecture. Empirical evaluations show that hybrid models consistently outperform standalone architectures in accuracy, recall, and F1-score, making them suitable for proactive cyber defence environments [6], [24].

Graph Neural Networks represent a transformative advancement in intrusion detection. By modeling network infrastructure as an interconnected graph, GNNs can identify hidden relationships among devices, users, and communication flows. This relational intelligence enables the detection of multi-stage intrusions, insider threats, and coordinated botnet activities that may evade conventional IDS models [16], [25].

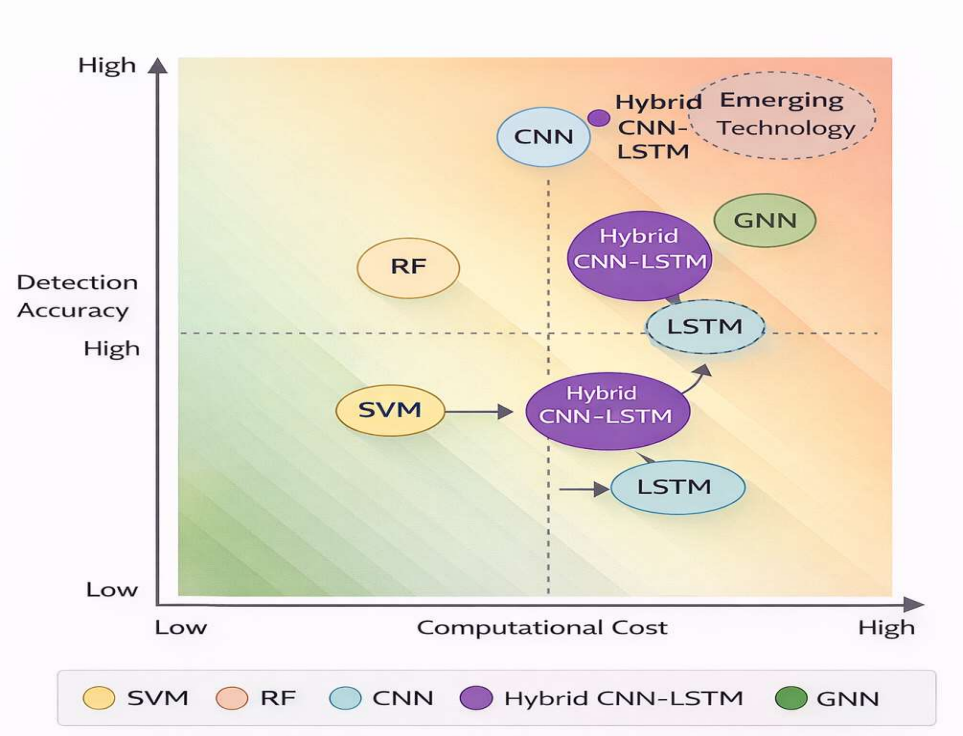

Figure 3: Performance comparison of IDS Algorithm

7. Proposed Flow Architecture: Proactive Cyber Defence Framework

The proposed architecture integrates multi-layer intelligence to enable predictive threat mitigation rather than reactive defence.

Data Sources:

Traffic originates from enterprise networks, cloud infrastructures, IoT devices, and endpoint systems. Modern studies emphasize the importance of multi-source telemetry for improving detection accuracy [22].

Traffic Collector:

A centralized collector aggregates packet flows and metadata in real time. Scalable ingestion pipelines reduce latency and support high-volume environments.

Preprocessing Engine:

Noise removal, normalization, and feature encoding prepare the dataset for deep learning. Proper preprocessing significantly enhances classification reliability [23].

Feature Extraction Layer:

Automated feature extraction eliminates manual engineering by identifying latent attack signatures within network behavior.

Hybrid Deep Neural Engine (CNN + LSTM + Attention):

Attention mechanisms prioritize critical threat indicators, improving interpretability and detection precision. Research shows that attention-enhanced IDS models achieve higher recall for rare attack classes [24].

Threat Intelligence Layer:

Outputs are correlated with external intelligence feeds, enabling contextual awareness and reducing false positives.

Automated Response System:

The system triggers containment actions such as IP blocking, session termination, or sandboxing—supporting the shift toward autonomous cyber defence ecosystems [25].

8. Discussion

AI-enabled intrusion detection systems demonstrate substantial improvements over signature-based approaches by leveraging adaptive learning and behavioral analytics.

Deep learning IDS frameworks have reported detection rates exceeding **95%**, illustrating their capability to identify complex attack vectors across evolving network conditions [19]. Hybrid architectures further enhance classification accuracy by integrating temporal and spatial analysis, enabling earlier detection of advanced threats [21].

Despite these advantages, several challenges persist:

- **False Positives:** Excessive alerts can overwhelm security teams. Integrating threat intelligence and contextual filtering helps mitigate this issue [22].
- **Computational Overhead:** Deep models demand high processing power, complicating real-time deployment in resource-constrained environments [23].
- **Scalability:** Large-scale networks require distributed learning strategies to maintain throughput without sacrificing accuracy [24].

Organizations are therefore transitioning toward proactive AI-driven defence strategies that emphasize predictive analytics, automation, and continuous model retraining. Such systems represent a paradigm shift from reactive cyber security toward intelligent, self-adapting protection infrastructures [25].

9. Conclusion

This study presented a comparative analysis of multiple Intrusion Detection System (IDS) algorithms, including Support Vector Machine (SVM), Random Forest (RF), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Hybrid CNN-LSTM, and Graph Neural Network (GNN). The evaluation highlights that traditional machine learning models such as SVM and RF offer lower computational cost but provide moderate detection accuracy. Deep learning approaches, particularly CNN and LSTM, demonstrate improved capability in identifying complex attack patterns, though they require higher computational resources.

The Hybrid CNN-LSTM model achieves a balanced trade-off between detection accuracy and processing efficiency by combining spatial and temporal feature extraction. Meanwhile, GNN emerges as a highly promising technique due to its ability to model relationships and dependencies within network traffic data, resulting in strong detection performance for sophisticated and evolving cyber threats. Overall, the findings suggest that advanced deep learning and graph-based methods are better suited for modern, large-scale network environments where attack patterns are increasingly complex.

Future Scope

Future research can focus on optimizing computational efficiency to make high-performing models such as Hybrid CNN-LSTM and GNN more practical for real-time deployment. Techniques such as model compression, pruning, and edge-based processing may help reduce latency and resource consumption.

Additionally, integrating GNN with hybrid architectures could further enhance detection accuracy by leveraging both relational and sequential data patterns. Exploring federated learning for IDS can improve privacy while enabling collaborative threat intelligence across distributed networks.

Another promising direction is the use of explainable artificial intelligence (XAI) to improve transparency in IDS decisions, helping security professionals better understand detected anomalies. Finally, developing adaptive IDS frameworks capable of self-learning from emerging threats will be critical to maintaining robust cybersecurity defenses in dynamic network environments.

References

[1]. H. M. R. Ur Rehman *et al.*, "A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions," *Journal of Big Data*, vol. 12, 2025.

[2]. Y. Zhang, R. C. Muniyandi, and F. Qamar, "A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance," *Applied Sciences*, vol. 15, no. 3, 2025.

[3]. "Machine Learning and Deep Learning Architectures for Intrusion Detection System (IDS): A Survey," IEEE Conference Publication.

[4]. A. K. Pantazis and D. I. Fotidis, "Smart Monitoring Platforms Using AI Models for Continuous Behavioral Analysis," 2022.

[5]. N. Naseer *et al.*, "Machine learning strategies and considerations in intrusion detection systems: a comprehensive survey," *Frontiers in Computer Science*, 2024.

[6]. M. Udurume, V. Shakhov, and I. Koo, "Comparative Analysis of CNN–BiLSTM and Machine Learning Methods in Intrusion Detection Systems," *Applied Sciences*, vol. 14, no. 16, 2024.

[7]. "A Machine Learning Approach for Intrusion Detection System on NSL-KDD Dataset," IEEE Conference Publication.

[8]. "A Real-Time Network Intrusion Detection Based on Transformer-LSTM Model," IEEE Conference Publication, 2025.

[9]. "A Survey on Deep Learning Based Intrusion Detection System," IEEE Conference Publication.

[10]. "A Survey on Intrusion Detection System Based on Machine Learning and Deep Learning," IEEE Conference Publication.

[11]. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[12]. D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," in *Proc. International Conference on Learning Representations (ICLR)*, 2015.

[13]. S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[14]. V. Nair and G. E. Hinton, "Rectified Linear Units Improve Restricted Boltzmann Machines," in *Proc. International Conference on Machine Learning (ICML)*, 2010.

[15]. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[16]. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[17]. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[18]. M. Tavallaee et al., "A Detailed Analysis of the KDD CUP 99 Dataset," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009.

[19]. R. Vinayakumar et al., "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[20]. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[21]. K. Kim, S. Cho, and J. Na, "Deep Neural Network-Based Malware Detection Using Two-Dimensional Binary Program Features," in *Proc. IEEE Conference on Communications and Network Security*, 2016.

[22]. R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010.

[23]. N. Papernot et al., "The Limitations of Deep Learning in Adversarial Settings," in *Proc. IEEE European Symposium on Security and Privacy*, 2016.

[24]. K. Zhao, S. Zhang, G. Xue, and D. Li, "Transformer-Based Network Intrusion Detection with Attention Mechanisms," *IEEE Access*, vol. 10, pp. 98765–98778, 2022.

[25]. Z. Wu et al., "A Comprehensive Survey on Graph Neural Networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2021.