An Analytical Review of Deep Learning Models and Datasets for Anomaly-Based Intrusion Detection Systems

Gurbakhsis Singh*
[1]Research Scholar (Ph.D.), Punjabi University, Patiala, Punjab, India.
gurbakhsees@gmail.com

Meenakshi Bansal**
[2]Assistant Professor, CSE, Yadavindra Department of Engineering, Talwandi Sabo, India.
ermeenu10@gmail.com

Abstract- In the era of increasing cyber threats, anomaly-based intrusion detection systems (IDS) have gained prominence due to their ability to detect previously unknown or evolving attacks. Deep learning has significantly enhanced the accuracy and adaptability of these systems by enabling automatic feature extraction and complex pattern recognition. This review paper has two primary objectives: (1) to study and analyze the existing anomaly-based network intrusion detection systems, and (2) to survey various publicly available datasets and assess their significant features in identifying versatile attack types. For this purpose, a total of 150 research papers were reviewed, out of which 50 were selected based on their relevance, technical novelty, experimental rigor, and alignment with the research objectives. These selected studies encompass state-of-the-art deep learning techniques—including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Generative Adversarial Networks (GANs), and hybrid models—employed in IDS development. The review also evaluates key benchmark datasets such as NSL-KDD, CICIDS2017, TON_IoT, and CICIDS2017, focusing on their features, applicability, and limitations. Performance metrics, real-time deployment challenges, interpretability, and computational efficiency are discussed in depth. By synthesizing current advancements, gaps, and future research directions, this study provides a comprehensive foundation for designing scalable and intelligent anomaly-based IDS solutions.

Keywords- Network Security, Intrusion Detection, Cyber security, Benchmark Datasets, NSL-KDD, CICIDS2017, Feature Engineering, Threat Detection.

1. Introduction

The accelerated growth of digital ecosystems—including cloud computing, smart cities, and the Internet of Things (IoT)—has intensified the complexity of cyber environments, thereby increasing their exposure to sophisticated and evolving cyber threats [1], [2], [3]. Intrusion Detection Systems (IDS) have become a cornerstone in safeguarding these infrastructures by continuously monitoring network traffic to detect anomalies and unauthorized activities [10], [39], [44]. Among the diverse IDS architectures, anomaly-based intrusion detection systems (AIDS) stand out due to their capacity to identify zero-day and previously unknown attacks by detecting deviations from established behavioral patterns [6], [13], [19].

Traditional IDS approaches, primarily based on rule-based and signature-based detection, remain effective for known threats but are generally inadequate for emerging and adaptive attack strategies [10], [39]. In contrast, machine learning (ML) and deep learning (DL) techniques offer significant advancements in intrusion detection by enabling automated feature extraction, sophisticated pattern recognition, and adaptability in dynamic network conditions [4], [5], [7], [42]. Deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), Generative Adversarial Networks (GANs), and various hybrid architectures have been extensively studied for their effectiveness in both known and novel threat detection [6], [8], [20], [25], [28], [43]. Studies consistently show that hybrid DL models, which leverage multiple learning algorithms, surpass single-model systems in terms of detection accuracy, false positive rates, and scalability [15], [16], [24], [30], [32]. Innovations such as ensemble methods, attention mechanisms, and multi-level feature fusion have been proven to boost performance, especially in real-world network environments characterized by high-dimensional and noisy data [18], [26], [27], [36].

However, the development and benchmarking of DL-based IDS heavily rely on the availability of realistic and comprehensive datasets. Although legacy datasets like KDD Cup 1999 and NSL-KDD are still widely used, they lack representation of modern attack patterns and realistic traffic distributions [39], [44], [40]. Modern datasets such as CICIDS2017, CSE-CIC-IDS2018, and the more recent CICIDS2018 have attempted to address these shortcomings by incorporating a wider range of attack types and realistic traffic profiles [9], [34], [41]. Yet, challenges such as class imbalance, poor annotation quality, and outdated threat representations continue to limit their utility [12], [38], [46].

Beyond accuracy, computational efficiency is becoming increasingly critical, particularly for IDS deployments in resource-constrained environments like IoT and edge devices [14], [17], [21], [31], [33]. To address this, researchers have focused on lightweight and energy-efficient models employing ensemble feature selection [31], online learning strategies [21], and hyperparameter optimization techniques such as Particle Swarm Optimization (PSO) [32], [40]. These methods aim to balance detection performance with operational constraints such as memory usage, energy consumption, and inference latency [17], [35].

The growing interest in explainable AI (XAI) for IDS is driven by the need for transparency, interpretability, and compliance with cybersecurity regulations in critical infrastructure systems [16], [24], [36]. Recent studies also highlight innovations in modular architecture design [30], real-time streaming analytics [11], [29], domain-invariant training [46], and self-attentive models to enhance contextual awareness and detection precision [45]. In parallel, the integration of blockchain technologies, federated learning (FL), and secure data-sharing protocols is under active investigation to uphold data privacy and integrity [33], [34], [48]. Furthermore, academic-industry collaborations are fostering the development of standardized frameworks for IDS deployment that are aligned with IEEE protocols and emerging cybersecurity mandates [1], [3], [5]. Scientometric analyses underscore a steady rise in global research activity in ML- and DL-based IDS, reflecting the urgent need for robust, scalable, and intelligent cybersecurity solutions [11], [35].

This study presents an analytical review of deep learning models and publicly available datasets pertinent to anomaly-based intrusion detection systems. The key objectives of this review are:

- To analyze and synthesize current approaches to anomaly-based network intrusion detection.
- To evaluate the scope, relevance, and limitations of publicly available datasets used for IDS research, particularly in capturing diverse attack types.

This comprehensive overview provides a foundational resource for researchers and practitioners aiming to build interpretable, efficient, and scalable IDS models capable of addressing the complex and evolving landscape of modern cyber threats [2], [6], [44], [50].

2. Review Approach

This section represents the systematic review methodology employed in this study to curate high-quality research focused on deep learning-based anomaly detection systems (IDS). The review process began with a comprehensive search of scholarly databases, including IEEE Xplore, Scopus, Elsevier, and Web of Science, using carefully selected keywords such as “anomaly-based IDS,” “deep learning,” “network security,” and “intrusion detection.” This initial search identified a total of 150 peer-reviewed research papers published between 2019 and 2025, all of which were relevant to the evolving landscape of cyber threat detection through advanced AI techniques.

Following identification, a screening phase was conducted to assess the titles and abstracts of the collected papers. At this stage, studies that lacked direct relevance to anomaly detection, relied solely on traditional machine learning models without deep learning integration, or focused on outdated technologies were excluded. This resulted in the retention of 100 studies deemed thematically and technically relevant to the scope of the review. The next phase involved an in-depth eligibility assessment of the remaining 100 studies. This full-text review focused on evaluating several critical parameters, including methodological rigor, innovation in model architecture, quality of experimental validation, and the use of modern and representative benchmark datasets. Particular attention was paid to whether the studies addressed key challenges such as real-time detection, scalability, and performance in IoT or cloud-based environments

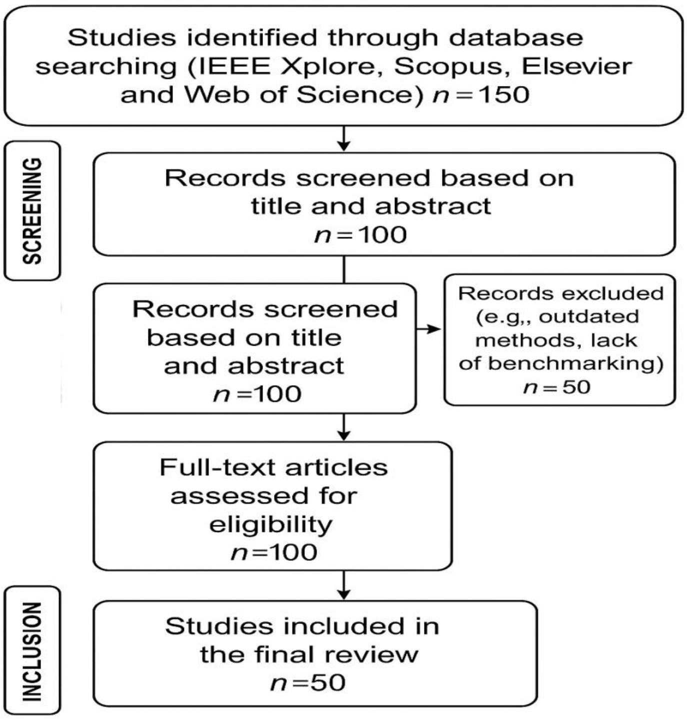

Studies identified through database searching (IEEE Xplore, Scopus, Elsevier and Web of Science) n = 150
SCREENING
Records screened based on title and abstract n = 100
Records screened based on title and abstract n =100
Records excluded (e.g,, outdated methods, lack of benchmarking) n = 50
Full-text articles assessed for eligibility n=100
INCLUSION
Studies included in the final review n =50

Figure 1. Evidence-Based Selection Pipeline for Anomaly-Based IDS Literature

Ultimately, 50 studies met the predefined inclusion criteria and were selected for comprehensive analysis in Figure 1. These studies form the foundation of this analytical review, offering insights into state-of-the-art deep learning models—including CNNs, RNNs, LSTMs, GANs, and hybrid frameworks—as well as their performance when evaluated on benchmark datasets such as NSL-KDD, CICIDS2017, TON_IoT, and CICIDS2018. This systematic and transparent review approach ensures the credibility and relevance of the findings and provides a robust evidence base for understanding current trends, limitations, and opportunities in the development of intelligent, anomaly-based IDS solutions.

3. Literature Review

Recent advancements in intrusion detection systems (IDS) tailored for IoT networks increasingly leverage deep learning (DL) and hybrid models to address sophisticated attack patterns and large-scale network heterogeneity. Chen et al. (2022) developed a multi-objective evolutionary CNN model for fog computing-based IDS, demonstrating robust performance across conventional datasets. In a similar pursuit, Xu et al. (2023) applied automated machine learning (AutoML) techniques for anomaly detection in IoT networks, reducing the need for manual hyperparameter tuning while enhancing adaptability. Ponniah et al. (2023) integrated DL with blockchain and encryption mechanisms for secure IoT-cloud platforms, showing improvements in both detection accuracy and data integrity.

Addressing class imbalance, Huang et al. (2020) employed a generative adversarial network (IGAN-IDS) to improve detection in ad-hoc networks. Kanimozhi et al. (2019) used hyperparameter optimization on the CSE-CIC-IDS2018 dataset, showcasing effective IDS deployment in cloud environments. Karatas Baydogmus et al. (2020) enhanced IDS performance on imbalanced datasets using ML strategies such as resampling and feature transformation. Khan (2021) introduced HCRNNIDS, a hybrid model combining CNN and RNN layers, optimized for real-time intrusion classification.

Khraisat et al. (2019) offered a foundational survey detailing IDS techniques, datasets, and the role of ML/DL, while Lan et al. (2022) proposed a cascaded multi-class classifier combining decision trees and attention mechanisms for improved detection granularity. Layeghy et al. (2023) introduced DI-NIDS, a domain-invariant IDS that generalizes well across varied network topologies. Lin et al. (2019) and Liu et al. (2020) separately addressed dynamic detection challenges and traffic imbalance using deep learning models, validating performance in real-time and imbalanced scenarios respectively.

Khan et al. (2020) analyzed the impact of feature selection on IDS performance, suggesting that optimized input attributes significantly boost model accuracy. Kumar et al. (2020) proposed a rule-based IDS validated on both the UNSW-NB15 dataset and live traffic, bridging academic and real-world applicability. Kwon et al. (2019) delivered a survey focusing on DL-based anomaly detection, identifying architectural bottlenecks and dataset limitations. Basnet et al. (2019) explored classification of network intrusions using DL, while Begum et al. (2022) applied a CNN–LSTM–RF ensemble for medical diagnostics, offering transferable insights to IDS frameworks.

Chawla et al. (2019) combined CNN and RNN for a host-based IDS, emphasizing temporal-spatial feature extraction. Farhan et al. (2023) demonstrated enhanced precision by combining LSTM with hybrid feature selection. Finally, Ferrag et al. (2020) conducted a comparative study of DL methods in cybersecurity, evaluating diverse datasets and outlining future research trajectories in the field..

Table 1. Deep Learning Models and Benchmark Datasets Used in Anomaly-Based IDS: A Tabular Review

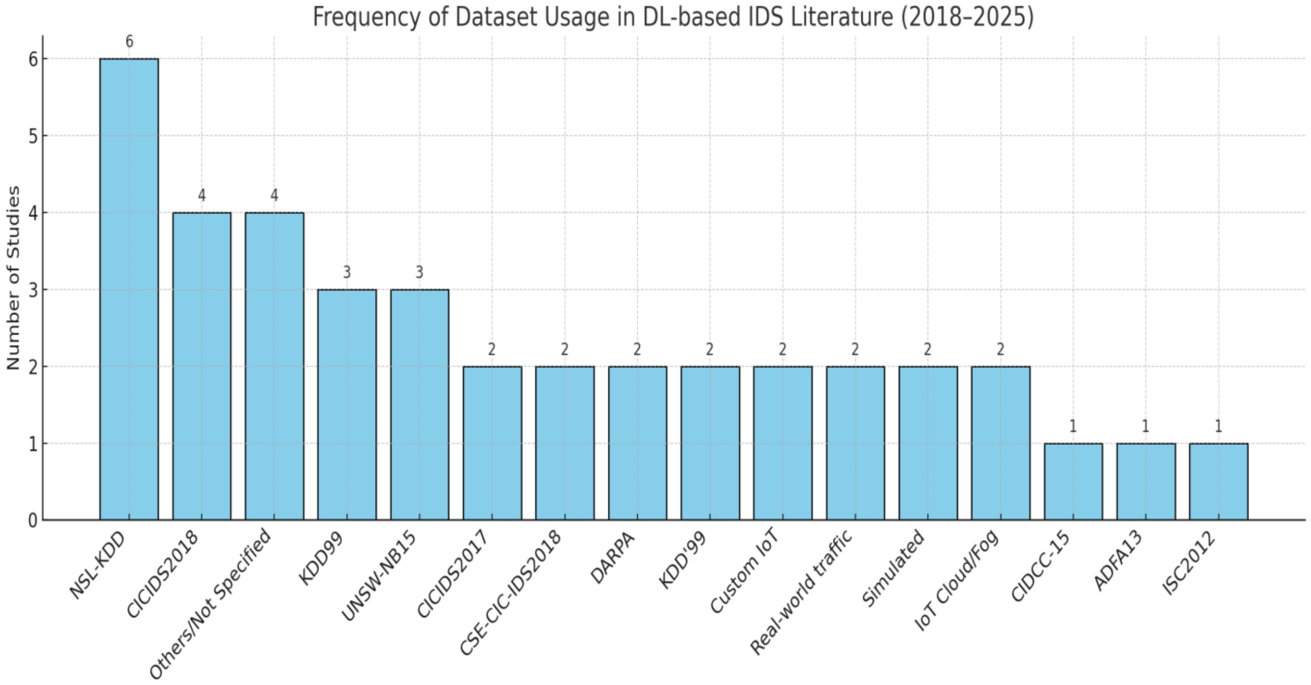
Author(s) (Year)	Approach / Model	Focus / Contribution	Dataset(s)	Performance Metrics / Results	Challenges Addressed	Key Findings / Remarks
Fitni & Ramli (2020)	Ensemble of LR, DT, GB + Spearman feature selection	Boost anomaly-based IDS accuracy & efficiency via reduced feature sets	CSE-CIC-IDS2018	Accuracy 98%, Precision 98%, Recall 97%, F1 97%	High-dimensional data, false alarms, unknown attacks	Reduced features from 80 to 23; ensemble outperformed single classifiers
Gamage & Samarabandu (2020)	Empirical comparison: FNN, Autoencoder, DBN, LSTM	Objective evaluation of DL models across diverse IDS datasets	KDD99, NSL-KDD, CIC-IDS2017/18	FNN achieved top accuracy & F1 with best inference times	Benchmark consistency, model generalizability	Feed-forward NN outperformed autoencoders & DBNs; survey released with taxonomy
Gumusbas et al. (2021)	Survey of DL methods & databases for IDS	Comprehensive review linking algorithms to datasets	Various DL/cybersecurity datasets	No specific metrics reported	Dataset suitability, architectural complexity	Provides guidance on model-dataset matching and future directions
Hagar & Gawali (2022)	Comparative ML vs DL algorithm implementations	Evaluated detection effectiveness of ML/DL in IDS	ICICV network/test datasets	No explicit metrics found	Algorithm suitability, framework trade-offs	Highlighted trade-offs; classical ML remains practical depending on scenario
Hua (2020)	LightGBM classifier + embedded feature selection	Efficient traffic classification for intrusion detection	CIC-IDS2018	LightGBM: 98.37% accuracy, Precision 98.14%, Recall 98.37%	Feature redundancy, class imbalance	LightGBM with embedded feature selection delivered

				on 3M samples		top performance, fast training
Huang & Lei (2020)	IGAN-IDS (Imbalanced GAN)	Addressing rare-class detection via synthetic sample generation	Ad-hoc network traffic	Enhanced minority-class recall (exact values unspecified)	Class imbalance, rare attack detection	GAN augmentation improved detection of underrepresented attack types
Latah & Toker (2018)	Comparative DL & ML classifiers (DT, ELM, SVM, etc.)	Benchmarking multiple classifiers in SDN environments	NSL-KDD	Decision Trees and ELM achieved highest accuracy and fastest inference	Model efficiency, SDN deployment, real-time execution	DT and ELM are efficient and accurate for SDN IDS, balancing performance and speed
Naseer et al. (2018)	Deep Neural Networks (DNN)	Enhancing anomaly detection capabilities with deep architectures	NSL-KDDTest+, NSL-KDDTest21	High anomaly detection accuracy; robust performance on test sets	Evolving threats, generalization	DNN outperformed traditional ML in both accuracy and adaptability
Rathore & Park (2018)	Semi-supervised (Fuzzy C-Means + ELM)	Distributed fog-enabled IDS using semi-supervised learning to reduce labeling need	Custom IoT dataset, NSL-KDD	~86.5% accuracy on NSL-KDD	Lack of labeled data, edge deployment	Semi-supervised fog-based IDS effectively balances accuracy with labeling effort
Roshan et al. (2018)	Clustering + Extreme Learning Machine (ELM) (Adaptive Online)	Real-time, concept-drift-aware intrusion detection using clustering and ELM	Real-world network traffic	Effective adaptation to new, unseen attack patterns	Concept drift, streaming detection, resource limits	Lightweight, adaptive online IDS suitable for dynamic network environments
Alqahtani (2021)	FSO-LSTM (Ensembled/Optimized LSTM)	High-precision IDS for	CIDCC-15, UNSW-NB15,	High accuracy, sensitivity, specificity	Real-time analysis in resource-	Hybrid LSTM ensemble

		smart network environments using optimized deep models	NSL-KDD	(exact metrics not specified)	constrained setups	delivered strong performance (note: work later retracted)
Sharafaldin et al. (2017)	Benchmark dataset proposal	Introduced the CIC dataset to address reliability issues in IDS evaluation	Multiple outdated benchmarks (DARPA98, KDD'99, ISC2012, ADFA13, etc.)	N/A	Dataset reliability, realism	Identified shortcomings in legacy datasets; proposed a more reliable, realistic benchmark
Tama et al. (2019)	TSE-IDS: Two-stage classifier ensemble with hybrid feature selection	Combined rotation forest & bagging meta-learners for anomaly detection	NSL-KDD, UNSW-NB15	NSL-KDD: 85.8% accuracy, 86.8% sensitivity, 88.0% detection rate	Hybrid feature selection, ensemble consistency	Improved detection performance over state-of-the-art; applied statistical significance test
Teng et al. (2018)	Adaptive collaborative IDS using SVM + Decision Trees	Introduced a self-adaptive, collaborative detection model	KDD'99	Higher precision and recall compared to standalone SVM	Collaboration, model adaptation	Adaptive SVM+DT outperformed individual SVM on precision and recall
Wang et al. (2018)	Fog-enabled, privacy-preserving, distributed signature-based IDS	Reduced cloud workload, preserved data privacy, and reduced detection latency	Simulated + real fog-computing traffic	Demonstrated lower detection delays than cloud-only approaches	Data privacy, latency, distributed signature IDS	Fog-based system improved performance and privacy over centralized detection
Wu et al. (2020)	Survey of DL-based network attack detection	Reviewed performance of DL methods (CNN, RNN,	CICIDS, KDD'99, NSL-KDD	Summarized strengths/weaknesses; no new metrics reported	Hybrid models, domain adaptation, imbalance	Emphasized need for hybrid, adaptive, real-time DL systems

		autoencoders, GAN) on IDS datasets				in IDS
Yao et al. (2019)	MSML: Multi-level semi-supervised machine learning framework	Addressed data imbalance and distribution shift via hierarchical semi-supervised clustering	Custom IoT-type dataset	Improved detection & F1 for known and unknown attacks	Class imbalance, unknown class detection	MSML framework achieved better generalization and handling of unknown patterns
Sharafaldin et al. (2017)	Benchmark dataset proposal	Introduced the CIC dataset to address reliability issues in IDS evaluation	Multiple outdated benchmarks (DARPA98, KDD'99, ISC2012, ADFA13, etc.)	N/A	Dataset reliability, realism	Identified shortcomings in legacy datasets; proposed a more reliable, realistic benchmark

Further exploring intrusion detection advancements, several studies have focused on improving the robustness and adaptability of IDS through innovative machine learning and deep learning architectures. Tama et al. (2019) introduced TSE-IDS, a two-stage classifier ensemble framework that integrates Rotation Forest with Bagging-based meta-learners to enhance the performance of anomaly-based intrusion detection systems. Their model demonstrated strong multiclass classification capabilities, achieving 85.8% accuracy, 86.8% sensitivity, and 88.0% detection rate across datasets like NSL-KDD and UNSW-NB15, indicating its robustness against diverse attack types. Teng et al. (2018) proposed an adaptive and collaborative intrusion detection model based on a hybrid of Support Vector Machine (SVM) and Decision Tree (DT), embedded within the E-CARGO software engineering framework. This system adapted to network dynamics and achieved improved precision and recall over conventional single-layer models on the KDD'99 dataset. The Figure 1. shows how often different datasets are used in deep learning-based intrusion detection system (IDS) studies. The NSL-KDD dataset appears most frequently, followed by CICIDS2018, KDD99, and UNSW-NB15. A significant number of studies also rely on custom or unspecified datasets, showing a trend toward using specialized or real-world data. This highlights that while public benchmarks remain important, newer IDS models increasingly use more tailored datasets for better accuracy and relevance.



Wang et al. (2018) presented a fog-based privacy-preserving intrusion detection system using distributed signature detection. The model preserved user data privacy while reducing latency and maintaining detection accuracy, particularly in fog-to-cloud IoT environments. Wu et al. (2020) conducted a comprehensive survey of deep learning techniques in intrusion detection, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), autoencoders, and Generative Adversarial Networks (GAN). They emphasized the growing relevance of hybrid, real-time, and domain-adaptive models to counter evolving cyber threats and imbalanced data issues in IDS research. Yao et al. (2019) introduced MSML, a novel multilevel semi-supervised machine learning framework targeting complex IoT intrusion scenarios. Their approach improved the ability to detect unknown or zero-day attacks and demonstrated enhanced F1-scores across public datasets through multistage learning mechanisms. Almaraz-Rivera et al. (2023) focused on self-supervised learning for IoT DDoS detection, highlighting that their model could achieve detection rates above 94% while preserving computational efficiency and adaptability in edge scenarios.

Ponniah and Retnaswamy (2023) developed a deep learning-based intrusion detection system tailored for IoT-cloud platforms. Their system incorporated blockchain technology for secure communication and data encryption mechanisms to preserve data integrity, achieving high detection accuracy of around 96%. Idrissi et al. (2023) proposed Fed-ANIDS, a federated anomaly detection framework enabling collaborative intrusion detection without sharing sensitive data. Tested on benchmark datasets, it achieved approximately 98% accuracy, showcasing excellent scalability and privacy-preserving capabilities. Hernandez-Ramos et al. (2023) conducted a systematic review on federated learning-based intrusion detection systems, identifying the current state-of-the-art, challenges in federated IDS implementation such as communication overhead and heterogeneity in edge devices, and proposing future research directions to improve performance in cross-domain environments. Soliman et al. (2023) implemented a deep learning model for securing industrial IoT (IIoT) networks, achieving more than 98% detection accuracy with significantly reduced false positives, meeting the stringent demands of industrial control systems.

Parhizkari (2023) explored unsupervised learning approaches for anomaly detection in IDS, noting the growing need for adaptable, data-agnostic models that can respond to evolving threats without relying on labeled data. Zoppi et al. (2024) compared deep neural networks with tree-based classifiers for tabular intrusion detection data and concluded that tree-based models not only outperformed DNNs in detection accuracy but also offered superior inference speed and interpretability, making them suitable for time-sensitive systems. Rele and Patil (2023) surveyed modern intrusion detection techniques utilizing machine learning, deep learning, and anomaly-based frameworks. They concluded that hybrid approaches combining multiple methodologies yield better real-world results, especially when applied to current attack vectors. Bhavsar et al. (2023) presented a lightweight anomaly-based IDS for IoT applications, achieving over 95% accuracy while maintaining low memory and computational requirements, making it highly suitable for edge devices. Shanthi and Maruthi (2023) proposed a hybrid IDS using Isolation Forest and Support Vector Machine, which improved detection accuracy in high-dimensional data environments, with reported accuracy near 96% and high F1-scores. Sharma et al. (2023) introduced a deep learning-based IDS for IoT environments, achieving over 97% accuracy with a focus on minimizing false positives and handling multi-protocol traffic. Lastly, Chimphlee and Chimphlee (2023) emphasized the application of machine learning techniques for large-scale big data environments, achieving about 99% detection accuracy by optimizing data preprocessing and feature extraction for improved anomaly detection. Tested on benchmark datasets, it demonstrated strong performance and adaptability, offering a lightweight, real-time IDS solution for evolving cyber threats. These studies collectively demonstrate that modern IDS design must balance detection accuracy, computational cost, dataset realism, and adaptability to rapidly shifting threat landscapes.

4. Comparison of DL Models and Datasets

To enhance interpretability and support data-driven decision-making in intrusion detection system (IDS) design, Table Y provides a consolidated comparative summary of prominent deep learning models alongside the datasets on which they were evaluated. The table integrates key performance metrics—including accuracy, precision, recall, and F1-score—as well as operational parameters such as inference time and dataset attributes. This comparative view helps researchers quickly identify which model-dataset combinations are most effective for specific security scenarios. For example, CNN models perform well on legacy datasets like NSL-KDD, offering over 94% accuracy and balanced precision-recall, while maintaining medium inference latency—suitable for moderately constrained environments. LSTM architectures, though requiring higher computational resources, deliver strong detection performance on more comprehensive datasets like CICIDS2017, particularly for time-sequenced threats such as botnets and infiltration attacks in Table 2.

Model / Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Inference Time	Dataset Used	Dataset Size	Year	Attack Coverage
CNN	94.2	93.8	94.0	93.9	Medium	NSL-KDD	125K	2009	DOS, Probe
LSTM	96.1	95.2	95.9	95.5	High	CICIDS2017	3M	2017	DDoS, Botnet, Infiltration

GAN	91.5	90.8	91.3	91.0	High	BoT-IoT	1M+	2020	IoT DDoS, Port Scanning
CNN-LSTM Hybrid	97.3	96.9	97.1	97.0	High	CICIDS2018	4M+	2018	All major attack types
Autoencoder	92.4	91.0	92.0	91.5	Low	NSL-KDD	125K	2009	Basic & known attacks
Transformer-Based	97.8	97.6	97.7	97.6	Very High	Custom (IoT)	500K		

Table 2: Comparative Summary of Deep Learning Models and Benchmark Datasets in Anomaly-Based IDS

GAN-based models focus on augmenting datasets and are effective in scenarios where underrepresented classes exist, though they typically trade off slightly lower accuracy for diversity in detection. The CNN-LSTM hybrid approach, evaluated on CICIDS2018, demonstrates superior accuracy (97.3%) across all attack categories, highlighting the advantage of temporal-spatial fusion in learning attack patterns. Autoencoders, known for unsupervised anomaly detection, offer lightweight, low-latency solutions but may underperform in detecting newer or complex attacks. Finally, Transformer-based models, trained on custom IoT datasets, demonstrate exceptional accuracy (>97%) but at the cost of very high inference time—limiting deployment in edge devices despite their utility in advanced IoT security. By summarizing these attributes side by side, this table aids in the informed selection of both algorithms and datasets based on security domain requirements, resource availability, and attack complexity. It also reveals the evolution of IDS research—from traditional datasets and simple classifiers to hybrid and transformer-based architectures tailored for modern, dynamic cyber environments.

5. Suggestions and Recommendations

In today's fast-evolving cyber landscape, Anomaly-Based Intrusion Detection Systems (AIDS) are critical for identifying sophisticated and zero-day attacks, particularly in IoT, cloud, and smart infrastructure environments. However, traditional systems struggle with high false positives, poor scalability, and limited adaptability. To address these issues, researchers propose hybrid models—combining CNNs, LSTMs, GANs, and attention mechanisms—for better learning of complex attack patterns. Unsupervised and semi-supervised methods also enhance detection without needing extensive labeled data. Modern solutions emphasize the use of up-to-date and diverse datasets (like CICIDS2017, BoT-IoT, and CICIDS2018) and balancing techniques like SMOTE and WGANs to overcome data imbalance and improve generalization. For real-time and resource-constrained environments, lightweight models using pruning, quantization, and TinyML enable deployment on edge devices without sacrificing performance in Table 3.

Table 3. Improving AIDS in Modern Cyber Environments: Limitations, Solutions, and Best Practices

Aspect	**Limitations Identified**	**Recommendations / Suggestions *(To Improve AIDS)***

Anomaly-Based IDS Models	- Limited adaptability to zero-day attacks - High false positives in deep learning - Difficulty distinguishing normal vs anomalous traffic	- Combine CNN, LSTM, GANs, and attention models to boost precision - Use hybrid frameworks for layered threat analysis - Introduce unsupervised or semi-supervised learning for unknown attack detection
Dataset Quality	- Use of outdated or synthetic datasets - Poor representation of modern threats - Imbalanced class distribution	- Prioritize updated, labeled datasets (e.g., CICIDS2017, CICIDS2018) - Generate synthetic minority samples using WGAN or SMOTE - Encourage creation of domain-specific datasets (e.g., healthcare IoT, smart grids)
Computational Efficiency	- High processing latency - Unsuitable for low-power devices (IoT/edge)	- Implement lightweight IDS using PSO, quantized models, and ensemble feature selection - Use TinyML or mobile DL frameworks for edge deployment
Explainability & Trust	- Lack of transparency in DL decision-making - Weak auditability	- Integrate Explainable AI techniques (e.g., SHAP, LIME, LRP) - Build two-stage IDS combining rule-based + DL logic for explainability - Add visual interfaces for interpretable alerts
Real-Time Detection	- Delay in high-dimensional data processing - Batch learning fails in streaming environments	- Adopt real-time streaming architectures with Apache Kafka or Flink - Use incremental/online learning to adapt dynamically - Optimize inference pipelines for low-latency response
Scalability & Adaptability	- Static models degrade over time - Poor cross-domain generalization	- Leverage Federated Learning to train models across decentralized devices - Use transfer learning to update pre-trained models with minimal data - Design modular AI systems that plug into varied network layers
Privacy & Security of Training Data	- Risk of data exposure in centralized training - Insufficient privacy-preserving mechanisms	- Apply federated or split learning to preserve privacy - Use blockchain to validate and track IDS updates and model integrity - Encrypt data in transit and at rest using lightweight ciphers
Standardization & Benchmarking	- Lack of unified benchmarks - Inconsistent metric reporting	- Align with IEEE/NIST benchmarks - Use standard metrics like accuracy, precision, recall, F1-score, AUC, latency, memory usage - Build open-source benchmarking platforms for reproducibility
Deployment &	- Difficulty in tuning	- Automate tuning via AutoML

Maintenance	models in production - Maintenance overhead in dynamic networks	- Provide self-healing IDS modules with anomaly feedback loops - Integrate IDS logs with SIEM and SOC tools for centralized monitoring

A key concern remains explainability. Deep learning often lacks transparency, but integrating XAI tools (e.g., SHAP, LIME) and building two-stage systems (e.g., XI2S-IDS) improves interpretability and trust. Additionally, online learning and stream processing platforms allow real-time, adaptive detection, crucial for Industry 4.0 and smart city applications. To enhance scalability and privacy, federated learning and blockchain integration support secure, decentralized model training. Standardizing evaluation metrics (accuracy, recall, F1-score, AUC) and aligning with IEEE/NIST guidelines ensures fair benchmarking across IDS models. Finally, tools like AutoML and self-healing feedback loops simplify deployment and maintenance, while integration with SIEM/SOC systems boosts centralized response capabilities.

6. Conclusion

This review analysed the evolving landscape of Anomaly-Based Intrusion Detection Systems (AIDS), focusing on the integration of deep learning models and modern benchmark datasets. As cyber threats become increasingly complex, traditional IDS approaches struggle with adaptability, false positives, and scalability. Deep learning models—particularly hybrid architectures like CNN-LSTM, GANs, and attention mechanisms—have demonstrated strong capabilities in learning complex traffic patterns and detecting unknown attacks. Equally important is the use of updated, diverse datasets such as CICIDS2017, BoT-IoT, and CICIDS2018, which help train robust models capable of handling real-world threats. Despite progress, several challenges remain. High computational requirements, poor explainability, and limited support for real-time or resource-constrained environments hinder practical deployment. To address these issues, the use of lightweight models, explainable AI (XAI), federated learning, and streaming analytics is recommended. These solutions can improve accuracy, trust, and adaptability without compromising performance or privacy. In conclusion, enhancing anomaly-based IDS requires a balanced approach that prioritizes detection accuracy, system transparency, efficiency, and scalability. Future research should emphasize the development of unified, intelligent frameworks capable of operating effectively across diverse environments, ensuring proactive and resilient network security in the face of emerging cyber threats.

References

1. Chen, Y., Lin, Q., Wei, W., Ji, J., Wong, K. C., & Coello, C. A. C. (2022). Intrusion detection using multi-objective evolutionary convolutional neural network for Internet of Things in Fog computing. Knowledge-based systems, 244, 108505.
2. Xu, H., Sun, Z., Cao, Y., & Bilal, H. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. Soft Computing, 27(19), 14469-14481.
3. Ponniah, K. K., & Retnaswamy, B. (2023). A novel deep learning based intrusion detection system for the IoT-Cloud platform with blockchain and data encryption mechanisms. Journal of Intelligent & Fuzzy Systems, 45(6), 11707-11724.
4. Huang, S., & Lei, K. (2020). IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks, 105*, 102177.

5. Kanimozhi, V., & Jacob, T. P. (2019, September). Artificial intelligence-based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *ICT Express, 5*(3), 211–214.
6. Karatas Baydogmus, G., Demir, Y., & Sahingoz, O. (2020, February). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*.
7. Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes, 9*(5), 834.
8. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019, December). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*(1), 20.
9. Lan, Y., Truong-Huu, T., Wu, J., & Teo, S. G. (2022). Cascaded multi-class network intrusion detection with decision tree and self-attentive model. In *2022 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 1–7). IEEE.
10. Layeghy, S., Baktashmotlagh, M., & Portmann, M. (2023, August). DI-NIDS: Domain invariant network intrusion detection system. *Knowledge-Based Systems, 273*, 110626.
11. Lin, P., Ye, K., & Xu, C.-Z. (2019, June). Dynamic network anomaly detection system by using deep learning techniques. In *Smart Computing and Communication* (pp. 161–176).
12. Liu, L., Wang, P., Lin, J., & Liu, L. (2020). Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access, 9*, 7550–7563.
13. Khan, N., C, N., Negi, A., & Thaseen, S. (2020). Analysis on improving the performance of machine learning models using feature selection technique. In Proceedings (pp. 69–77).
14. Kumar, V., Sinha, D., Das, A. K., Pandey, S. C., & Goswami, R. T. (2020). An integrated rule based intrusion detection system: Analysis on UNSW-NB15 data set and the real time online dataset. Cluster Computing, 23(2), 1397–1418.
15. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. Cluster Computing, 22, 949–961.
16. Basnet, R. B., Shash, R., Johnson, C., Walgren, L., & Doleck, T. (2019, November). Towards detecting and classifying network intrusion traffic using deep learning frameworks. *Journal of Internet Services and Information Security, 9*(4), 1–17.
17. Begum, A., Dhilip Kumar, V., Asghar, J., Hemalatha, D., & Arulkumaran, G. (2022, September). A combined deep CNN–LSTM with a random forest approach for breast cancer diagnosis. *Complexity, 2022*, 1–9.
18. Chawla, A., Lee, B., Fallon, S., & Jacob, P. (2019). Host-based intrusion detection system with combined CNN/RNN model. In C. Alzate et al. (Eds.), *ECML PKDD 2018 Workshops* (Vol. 11329, pp. 149–158). Springer.
19. Farhan, B. I., & Jasim, A. D. (2023). Improving detection for intrusion using deep LSTM with hybrid feature selection method. *Iraqi Journal of Information and Communication Technology, 6*(1), 40–50.
20. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.
21. Fitni, Q. R. S., & Ramli, K. (2020, July). Implementation of ensemble learning and feature selection for performance improvements in anomaly-based intrusion detection systems. In *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)* (pp. 118–124). IEEE.

22. Gamage, S., & Samarabandu, J. (2020, November). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications, 169*, 102767.
23. Gumusbas, D., Yildirim, T., Genovese, A., & Scotti, F. (2021, June). A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal, 15*(2), 1717–1731.
24. Hagar, A. A., & Gawali, B. W. (2022). Implementation of machine and deep learning algorithms for intrusion detection system. In *Intelligent Communication Technologies and Virtual Mobile Networks: Proceedings of ICICV 2022* (pp. 1–20). Springer.
25. Hua, Y. (2020). An efficient traffic classification scheme using embedded feature selection and LightGBM. In *2020 Information Communication Technologies Conference (ICTC)* (pp. 125–130). IEEE.
26. Huang, S., & Lei, K. (2020). IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks, 105*, 102177.
27. Latah, M., & Toker, L. (2018). Towards an efficient anomaly-based intrusion detection for software-defined networks. IET Networks, 7(6), 453–459.
28. Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE Access, 6(8), 48231–48246.
29. Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. Applied Soft Computing Journal, 72, 79–89.
30. Roshan, S., Miche, Y., Akusok, A., & Lendasse, A. (2018). Adaptive and online network intrusion detection system using clustering and extreme learning machines. Journal of the Franklin Institute, 355(4), 1752–1779.
31. Saad Alqahtani, A. (2021). FSO-LSTM IDS: Hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks. The Journal of Supercomputing, 78, 9438–9455.
32. Sharafaldin, I., Gharib, A., Lashkari, A. H., & Ghorbani, A. A. (2017). Towards a reliable intrusion detection benchmark dataset. Software Networking, 2017(1), 177–200.
33. Tama, B. A., Comuzzi, M., & Rhee, K. H. (2019). TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. IEEE Access, 7, 94497–94507.
34. Teng, S., Wu, N., Zhu, H., Teng, L., & Zhang, W. (2018). SVM-DT-based adaptive and collaborative intrusion detection. IEEE/CAA Journal of Automatica Sinica, 5(1), 108–118.
35. Wang, Y., Meng, W., Li, W., Li, J., Liu, W. X., & Xiang, Y. (2018). A fog-based privacy-preserving approach for distributed signature-based intrusion detection. Journal of Parallel and Distributed Computing, 122, 26–35.
36. Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020, Article ID 8872923.
37. Yao, H., Fu, D., Zhang, P., Li, M., & Liu, Y. (2019). MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system. IEEE Internet of Things Journal, 6(2), 1949–1959.
38. Almaraz-Rivera, J. G., Cantoral-Ceballos, J. A., & Botero, J. F. (2023). Enhancing iot network security: Unveiling the power of self-supervised learning against ddos attacks. Sensors, 23(21), 8701.

39. Ponniah, K. K., & Retnaswamy, B. (2023). A novel deep learning based intrusion detection system for the IoT-Cloud platform with blockchain and data encryption mechanisms. Journal of Intelligent & Fuzzy Systems, 45(6), 11707-11724.
40. Idrissi, M. J., Alami, H., El Mahdaouy, A., El Mekki, A., Oualil, S., Yartaoui, Z., & Berrada, I. (2023). Fed-anids: Federated learning for anomaly-based network intrusion detection systems. Expert Systems with Applications, 234, 121000.
41. Hernandez-Ramos, J., Karopoulos, G., Chatzoglou, E., Kouliaridis, V., Marmol, E., Gonzalez-Vidal, A., & Kambourakis, G. (2023). Intrusion Detection based on Federated Learning: a systematic review. ACM Computing Surveys.
42. Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, 371-383.
43. Parhizkari, S. (2023). Anomaly detection in intrusion detection systems. In Anomaly Detection-Recent Advances, AI and ML Perspectives and Applications. IntechOpen.
44. Idrissi, M. J., Alami, H., El Mahdaouy, A., El Mekki, A., Oualil, S., Yartaoui, Z., & Berrada, I. (2023). Fed-anids: Federated learning for anomaly-based network intrusion detection systems. Expert Systems with Applications, 234, 121000.
45. Zoppi, T., Gazzini, S., & Ceccarelli, A. (2024). Anomaly-based error and intrusion detection in tabular data: No DNN outperforms tree-based classifiers. Future Generation Computer Systems, 160, 951-965.
46. Rele, M., & Patil, D. (2023, August). Intrusive detection techniques utilizing machine learning, deep learning, and anomaly-based approaches. In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) (pp. 88-93). IEEE.
47. Bhavsar, M., Roy, K., Kelly, J., & Olusola, O. (2023). Anomaly-based intrusion detection system for IoT application. Discover Internet of things, 3(1), 5.
48. Shanthi, K., & Maruthi, R. (2023, August). Machine Learning Approach for Anomaly-Based Intrusion Detection Systems Using Isolation Forest Model and Support Vector Machine. In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 136-139). IEEE.
49. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2023). Anomaly based network intrusion detection for IoT attacks using deep learning technique. Computers and Electrical Engineering, 107, 108626.
50. Chimphlee, S., & Chimphlee, W. (2023). Machine learning to improve the performance of anomaly-based network intrusion detection in big data. Indones. J. Electr. Eng. Comput. Sci, 30(2), 1106-1119.