Journal of Computing and Data Technology

https://journal.krrishpub.com/index.php/jcdt/index

REVIEW ARTICLE

A Comprehensive Systematic Review of AI-based Network Intrusion Detection Systems: Techniques, Datasets, Challenges, and Future Research Directions

Mehdi Gheisari [a,b,c], Zhou Pingmei [b], Basheer Riskhan [d,*], Malusi Sibiya [e], Muhammad Faizan Khan [f,g], Seyed Kazem Gheblezadeh [h]

[a] *Institute of Artificial Intelligence, Shaoxing University, 508 West Huancheng Road, Yuecheng District, Zhejiang, 312000, China.*
[b] *Department of R& D, Shenzhen BKD Co LTD, No. 1, Huibei Road, Kengzi Subdistrict, Pingshan District, Shenzhen, China.*
[c] *Department of Computer Engineering, Shi.C., Islamic Azad University, Shiraz, Iran.*
[d] *Dean and Associate Professor of School of Computer and Informatics, Albukhary International University (AIU), Jalan Tun Abdul Razak, 05200, Alor Setar, Kedah Darul Aman, Malaysia.*
[e] *Centre for Augmented Intelligence and Data Science, University of South Africa, Florida Campus, Roodepoort 1709, South Africa.*
[f] *Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan.*
[g] *School of Computer Science & Cyber Engineering, Guangzhou University, Guangzhou 510006, China.*
[h] *Department of Computer Engineering, Islamic Azad University Maybod: Meybod, Yazd Province, Iran.*

Abstract

The rapid expansion of cloud computing platforms, Internet of Things (IoT) ecosystems, edge devices, software-defined networks, and distributed enterprise infrastructures has significantly increased the complexity and scale of modern cybersecurity environments. Traditional signature-based intrusion detection systems are increasingly ineffective against sophisticated cyber threats such as zero-day attacks, advanced persistent threats, ransomware propagation, botnet activities, and encrypted malicious traffic because they rely heavily on predefined attack signatures and static rule-based detection mechanisms. Consequently, AI driven intrusion detection systems have emerged as promising solutions for intelligent threat detection, adaptive cybersecurity analytics, and real-time network defense. This paper presents a comprehensive systematic literature review of AI based network intrusion detection systems with particular emphasis on machine learning, deep learning, federated learning, and intelligent anomaly detection frameworks. Furthermore, the study evaluates benchmark cybersecurity datasets including NSL-KDD, CICIDS2017, UNSW-NB15, DARPA, and TON-IoT datasets to investigate their effectiveness, scalability, realism, and applicability for modern intrusion detection research. Comparative analysis indicates that deep learning and hybrid AI techniques significantly improve intrusion detection accuracy, adaptive threat detection, and real-time cybersecurity analytics compared with traditional approaches. The paper further discusses major challenges including adversarial attacks, encrypted traffic analysis, dataset imbalance, explainability, computational overhead, and concept drift. Emerging research directions such as federated intrusion detection, Transformer-based cybersecurity, graph neural networks, self-supervised learning, and explainable AI are also critically analyzed.

Keywords: Network security, Intrusion detection, Artificial intelligence, Deep learning, Cybersecurity, Anomaly detection, Federated learning.

Article information:
ISSN: 3107-9466 (Online)
Published by: **Krrish Scientific Publications Pvt. Ltd.**
DOI: https://doi.org/10.71426/jcdt.v2.i1.pp140-150
Received: *02 May 2026* | Revised: *30 May 2026* | Accepted: *01 June 2026* | Published: *02 June 2026*

1. Introduction

Modern digital infrastructures heavily depend on secure communication networks for data exchange, cloud computing, financial systems, industrial automation, healthcare

*Corresponding author
Email addresses: mehdi.gheisari61@gmail.com, MEHDI.gheisari@yandex.com (Mehdi Gheisari), 393272357@qq.com (Zhou Pingmei), b.riskhan@aiu.edu.my (Basheer Riskhan), sibiym@unisa.ac.za (Malusi Sibiya), khanmuhammadfaizan@uoh.edu.pk, faizan@gzhu.edu.cn (Muhammad Faizan Khan), saman2644@gmail.com (Seyed Kazem Gheblezadeh).

platforms, and critical national infrastructure. However, the increasing sophistication of cyberattacks has introduced significant security challenges for enterprise and distributed networks [1]–[3]. Traditional signature-based security systems often fail to detect emerging attacks because they depend on predefined attack patterns and static rule sets [4], [5]. Consequently, AI and machine learning approaches have gained substantial attention in network security research.

According to recent cybersecurity industry reports, global cybercrime costs are projected to exceed trillions of dollars annually due to increasing ransomware campaigns, AI-assisted phishing attacks, cloud vulnerabilities, and large-scale data breaches. These rapidly evolving attack patterns necessitate adaptive and intelligent cybersecurity mechanisms capable of real-time threat detection.

Machine learning based intrusion detection systems are capable of identifying abnormal network behaviors through statistical learning and behavioral analysis [6], [7]. Deep learning architectures including convolutional neural networks, recurrent neural networks, and autoencoders have demonstrated strong performance in anomaly detection and traffic classification tasks [8]–[10]. Furthermore, real-time cybersecurity systems increasingly rely on adaptive intelligence to identify zero-day threats and polymorphic malware [11], [12].

Recent research trends further indicate that intelligent intrusion detection systems are increasingly evolving toward adaptive deep learning, distributed cybersecurity analytics, and real-time behavioral threat intelligence frameworks [37], [38], [43]. Traditional rule-based intrusion detection systems such as Snort remain effective for predefined attack signatures but demonstrate limited capability against polymorphic malware and zero-day attacks [44]. Furthermore, benchmark intrusion detection datasets such as KDD Cup 99 and NSL-KDD continue to face criticism regarding outdated traffic patterns, synthetic attack behavior, and limited representation of modern enterprise network environments [49].

This review manuscript systematically investigates recent advancements in AI driven intrusion detection systems, intelligent cybersecurity architectures, anomaly detection methodologies, and deep learning based network security frameworks proposed in contemporary cybersecurity research. Unlike existing review studies, this paper provides a unified comparative analysis of machine learning, deep learning, federated learning, Transformer-based intrusion detection, graph neural cybersecurity frameworks, explainable AI techniques, and edge intelligence driven cybersecurity systems. The review additionally integrates comparative dataset analysis, deployment challenges, adversarial robustness, scalability evaluation, and future research directions within a single systematic framework. Fig. 1 shows taxonomy of AI-based intrusion detection systems discussed in this manuscript.

1.1. Research objectives

The primary objectives of this systematic review are summarized as follows:

1. To critically analyze traditional machine learning and advanced deep learning based intrusion detection methodologies utilized in modern cybersecurity systems.
2. To compare benchmark cybersecurity datasets including NSL-KDD, CICIDS2017, UNSW-NB15, DARPA, and TON-IoT datasets based on scalability, realism, feature diversity, and attack representation capability.
3. To investigate emerging intelligent cybersecurity frameworks including federated learning, graph neural networks, Transformer-based intrusion detection systems, explainable AI, and edge AI security architectures.
4. To evaluate intrusion detection systems using technical performance metrics including detection accuracy, precision, recall, F1-score, computational complexity, scalability, and real-time deployment capability.
5. To identify major research gaps associated with encrypted traffic analysis, adversarial machine learning attacks, false positive reduction, concept drift, privacy preservation, and distributed cybersecurity infrastructures.
6. To discuss future research directions for scalable, explainable, adaptive, and privacy-preserving AI driven cybersecurity systems for next-generation enterprise environments.

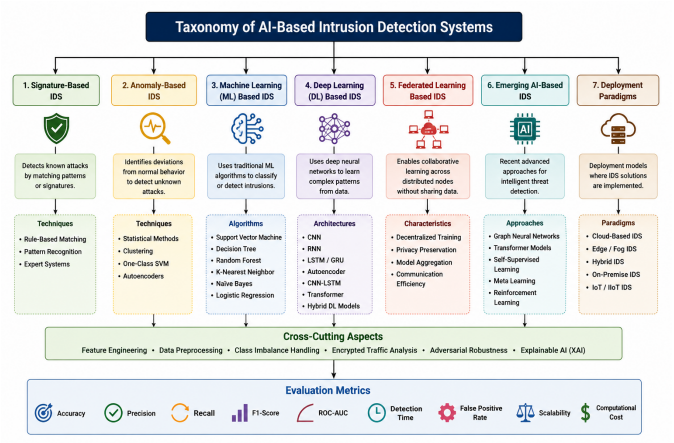

Figure 1: Taxonomy of AI-based intrusion detection systems.

2. Literature Review

Network intrusion detection has been widely studied in cybersecurity research for several decades due to the rapid increase in cyberattacks, distributed network infrastructures, and intelligent malicious activities targeting enterprise environments. Early intrusion detection research primarily focused on misuse detection and abnormal behavior analysis within computer systems and communication networks. Denning [1] introduced one of the earliest intrusion detection models based on abnormal system behavior analysis and audit trail monitoring. Subsequent studies explored expert systems, statistical analysis methods, and rule-based misuse detection techniques for identifying malicious network activities [2], [3]. Traditional signature-based systems such as Snort demonstrated strong capability for detecting predefined attack patterns but remained ineffective against zero-day attacks, adaptive malware, encrypted threats, and polymorphic attack behaviors [4], [44].

As enterprise networks evolved toward cloud-native infrastructures, Internet of Things ecosystems, distributed edge computing environments, and software-defined networking architectures, the complexity and scale of cybersecurity threats significantly increased. Consequently, intelligent AI driven cybersecurity frameworks emerged as promising solutions for adaptive anomaly detection, automated threat intelligence generation, and real-time network security analytics [6], [7]. Machine learning and deep learning techniques have demonstrated substantial capability for learning network traffic behavior, detecting abnormal communication patterns, and identifying sophisticated cyberattacks across heterogeneous enterprise environments.

Recent cybersecurity research additionally emphasizes the importance of scalable, explainable, and privacy-preserving intrusion detection systems capable of operating under real-time deployment constraints. Advanced intrusion detection frameworks increasingly integrate deep learning architectures, federated learning, graph neural networks, self-supervised learning, explainable AI, and edge intelligence driven cybersecurity analytics [36]–[38]. These intelligent frameworks aim to improve detection accuracy, encrypted traffic analysis, adversarial robustness, and adaptive threat intelligence generation within next-generation cybersecurity infrastructures.

2.1. Existing survey and review studies

Several survey and review studies have comprehensively investigated network intrusion detection systems from different cybersecurity perspectives including anomaly detection, machine learning, deep learning, distributed intrusion detection, and intelligent behavioral analytics. Existing review studies primarily focus on either traditional machine learning approaches, benchmark cybersecurity datasets, or deep learning based anomaly detection mechanisms. However, many studies provide limited discussion regarding emerging cybersecurity technologies such as federated learning, Transformer-based cybersecurity analytics, graph neural network intrusion detection systems, explainable AI, and adversarial robustness.

Garcia-Teodoro et al. [5] provided one of the earliest comprehensive reviews of anomaly-based intrusion detection techniques and highlighted challenges associated with false positives, scalability limitations, and adaptive attack behavior. Sommer and Paxson [6] critically analyzed the applicability of machine learning techniques for intrusion detection systems and emphasized challenges associated with feature engineering, dataset quality, and deployment realism. Buczak and Guven [7] presented a detailed survey of data mining and machine learning methods for cybersecurity intrusion detection and discussed supervised and unsupervised cybersecurity analytics approaches.

Recent survey studies have increasingly focused on deep learning cybersecurity architectures and intelligent network anomaly detection systems. Ferrag et al. [36] comparatively evaluated deep learning based intrusion detection systems across multiple benchmark cybersecurity datasets and analyzed the effectiveness of CNN, RNN, autoencoder, and hybrid deep learning frameworks for anomaly detection and malicious traffic analysis. Kumar et al. [37] investigated evolving research trends in network intrusion detection systems and identified emerging cybersecurity directions including explainable AI, federated intrusion detection, and intelligent anomaly analytics. Kilincer et al. [38] comparatively analyzed machine learning algorithms for cybersecurity intrusion detection using heterogeneous benchmark datasets and reported that ensemble learning frameworks and deep neural architectures achieve strong detection performance under large-scale traffic environments.

Lakshminarayana et al. [43] further reviewed modern intrusion detection techniques including statistical analysis methods, machine learning approaches, and deep learning cybersecurity systems. Ring et al. [34] provided an extensive survey of benchmark intrusion detection datasets and highlighted the limitations associated with outdated traffic patterns, synthetic attack behaviors, and lack of realistic enterprise network representations in existing cybersecurity datasets.

Despite these significant contributions, several limitations remain within current review studies. Most existing surveys provide limited comparative analysis regarding computational complexity, real-time deployment capability, adversarial robustness, encrypted traffic analysis, and privacy preservation in distributed enterprise environments. Furthermore, recent advancements involving federated learning, graph neural networks, self-supervised cybersecurity analytics, edge intelligence, and explainable AI have not yet been comprehensively integrated within a unified systematic review framework. Therefore, a technically detailed and systematically organized review integrating conventional intrusion detection systems, deep learning cybersecurity frameworks, federated intrusion detection architectures, benchmark dataset evaluation, explainable AI, adversarial machine learning, and future intelligent cybersecurity directions remains necessary for next-generation enterprise network security research.

2.2. ML-based intrusion detection systems

Machine learning based intrusion detection systems have significantly improved intelligent traffic analysis capability and automated anomaly detection performance within enterprise cybersecurity environments [53]-[54]. Traditional machine learning frameworks rely on supervised and unsupervised learning techniques to classify normal and malicious network traffic behaviors using statistical features extracted from communication patterns, packet flows, and system logs.

Support vector machines, decision trees, random forests, k-nearest neighbor algorithms, naïve Bayes classifiers, and ensemble learning frameworks have been widely utilized for network intrusion detection tasks [13] – [15]. Mukkamala et al. [13] demonstrated the effectiveness of support vector machines and neural networks for intrusion detection using network traffic features derived from benchmark cybersecurity datasets. Lee and Stolfo [14] introduced data mining approaches for intrusion detection systems and emphasized the role of intelligent feature extraction and traffic classification in cybersecurity analytics. Breiman [15] proposed random forest classifiers that later became highly effective for intrusion detection due to their strong classification capability and resistance to overfitting.

Comparative evaluations indicate that machine learning intrusion detection systems achieve strong classification

accuracy for structured cybersecurity datasets while maintaining moderate computational complexity [38]. Ensemble learning approaches and random forest classifiers particularly demonstrate high performance for traffic classification tasks involving heterogeneous network attack categories. Furthermore, statistical learning techniques improve adaptive anomaly detection capability by identifying deviations from normal communication behavior patterns.

Survey studies additionally demonstrate that machine learning based intrusion detection systems remain highly effective for supervised cybersecurity analytics and traffic classification tasks [43]. However, conventional machine learning techniques still face several limitations when analyzing high-dimensional traffic data, encrypted communications, and continuously evolving attack patterns within large-scale distributed network environments. Traditional feature engineering approaches additionally require domain expertise and often struggle to generalize under dynamic cybersecurity conditions.

Consequently, recent intrusion detection research increasingly investigates deep learning architectures capable of automated hierarchical feature learning, intelligent behavioral analysis, and adaptive anomaly detection under heterogeneous network infrastructures.

2.3. DL-based intrusion detection systems

Deep learning based intrusion detection systems have emerged as highly effective cybersecurity solutions for intelligent anomaly detection, encrypted traffic analysis, adaptive behavioral analytics, and automated feature extraction. Unlike conventional machine learning approaches, deep neural architectures can automatically learn hierarchical traffic representations from large-scale cybersecurity datasets without requiring extensive manual feature engineering [57], [58].

Convolutional neural networks have demonstrated strong capability for spatial traffic representation learning and malware communication analysis [29], [30]. Wang et al. [29] proposed CNN based malware traffic classification frameworks capable of learning network communication patterns through representation learning techniques. Javaid et al. [30] further demonstrated that deep learning architectures significantly improve intrusion detection accuracy and adaptive threat intelligence generation compared with conventional machine learning models.

Recurrent neural networks and long short-term memory architectures are highly effective for temporal anomaly detection and sequential network traffic analysis [16], [17]. Yin et al.[9] proposed an RNN based intrusion detection framework capable of learning sequential traffic dependencies for intelligent anomaly detection. Hochreiter and Schmidhuber [16] have introduced long short-term memory architectures that later became widely utilized for sequential cybersecurity analytics due to their ability to model long-range temporal dependencies. Hundman et al. [17] further demonstrated the effectiveness of LSTM based anomaly detection systems for identifying abnormal behaviors within complex telemetry environments.

Autoencoder based intrusion detection systems additionally provide strong capability for unsupervised anomaly detection and high-dimensional traffic representation learning [10], [18]. Shone et al. [10] proposed a deep autoencoder architecture for intelligent network intrusion detection and demonstrated improved anomaly detection performance under benchmark cybersecurity datasets. Sakurada and Yairi [18] further investigated nonlinear dimensionality reduction using autoencoder architectures for anomaly detection in high-dimensional sensory datasets.

Recent deep learning cybersecurity research increasingly focuses on hybrid architectures integrating convolutional neural networks, recurrent neural networks, and intelligent behavioral analytics frameworks [53]–[56]. Khan et al. [35] proposed a scalable CNN-LSTM hybrid intrusion detection framework capable of improving sequential attack analysis and encrypted traffic detection performance. Vinayakumar et al. [33] additionally demonstrated that hybrid deep learning architectures significantly improve adaptive intrusion detection capability across heterogeneous network attack environments.

Online and self-supervised deep learning frameworks have also emerged as promising solutions for adaptive cybersecurity analytics within dynamically evolving network environments. Nakıp and Gelenbe [41] proposed self-supervised deep learning architectures for intrusion detection systems capable of continuously learning adaptive network behaviors without extensive labeled training datasets. Wahab [42] further investigated online deep learning approaches for intrusion detection under concept drift environments and demonstrated improved real-time anomaly detection capability within evolving IoT infrastructures.

Sparse deep denoising autoencoder frameworks additionally improve dimensionality reduction and anomaly detection capability under high-dimensional cybersecurity datasets [48]. Furthermore, recent hybrid Seq2Seq and ConvLSTM subnet architectures have demonstrated strong capability for intelligent sequential attack analysis and temporal anomaly detection [40].

Despite these significant advancements, deep learning based intrusion detection systems still face important challenges associated with computational complexity, adversarial robustness, explainability, scalability limitations, and resource-intensive deployment requirements for large-scale enterprise environments.

2.4. FL-based intrusion detection systems

Federated learning and distributed AI techniques have emerged as promising solutions for privacy-preserving cybersecurity analytics and collaborative intrusion detection across distributed enterprise infrastructures [19], [20]. Traditional centralized intrusion detection systems often require direct aggregation of sensitive traffic data, thereby introducing privacy concerns, regulatory limitations, and communication bottlenecks within cloud-native cybersecurity environments.

Yang et al. [19] introduced federated machine learning concepts for distributed intelligent analytics and demonstrated that decentralized learning approaches can improve collaborative model training without directly sharing sensitive raw data. McMahan et al. [20] further proposed communication-efficient distributed deep learning architectures capable of training neural networks across decentralized environments with reduced communication overhead.

Federated intrusion detection systems enable distributed anomaly detection capability across cloud infrastructures,

IoT ecosystems, edge computing environments, and heterogeneous enterprise networks. Diro and Chilamkurti [32] proposed distributed deep learning frameworks for intrusion detection within Internet of Things environments and demonstrated improved scalability and collaborative cybersecurity intelligence generation.

Recent research additionally investigates decentralized deep learning frameworks for multi-access edge computing and communication-efficient edge intelligence. Sun et al. [47] analyzed trustworthiness and communication efficiency challenges within decentralized deep learning architectures and highlighted the importance of scalable edge intelligence for distributed AI cybersecurity systems. Privacy preservation and inference security additionally remain major research concerns within federated intrusion detection environments. Salem et al. [45] investigated inference privacy challenges in machine learning systems and emphasized the risks associated with sensitive information leakage during collaborative learning processes.

Recent online intrusion detection frameworks such as Kitsune further demonstrated the effectiveness of lightweight autoencoder ensembles for real-time anomaly detection within edge environments [23]. Mirsky et al. [23] proposed a lightweight ensemble autoencoder architecture capable of adaptive online anomaly detection under distributed enterprise traffic environments.

Benchmark datasets including NSL-KDD, CICIDS2017, UNSW-NB15, and DARPA continue to be widely utilized for evaluating federated intrusion detection systems under heterogeneous attack scenarios [24]–[26], [34]. However, distributed intrusion detection systems still face several important limitations including communication overhead, synchronization complexity, privacy leakage risks, adversarial manipulation, and deployment scalability challenges across large-scale enterprise environments.

Although federated cybersecurity frameworks demonstrate strong capability for collaborative intelligent threat analytics and distributed anomaly detection, further research remains necessary for improving explainability, adversarial robustness, adaptive real-time deployment, and trustworthy distributed cybersecurity intelligence generation.

3. Emerging AI based intrusion detection frameworks

3.1. Recent advances in large language models and generative AI for cybersecurity

Recent advancements in large language models and generative AI have introduced new opportunities for intelligent cybersecurity analytics, automated threat intelligence generation, malware behavior interpretation, phishing detection, and security log analysis. Transformer-based architectures and foundation models are increasingly utilized for contextual anomaly detection, automated vulnerability assessment, and adaptive threat reasoning in enterprise environments.

Generative AI techniques are also being investigated for synthetic cybersecurity dataset generation, adversarial attack simulation, and intelligent penetration testing frameworks. However, challenges associated with hallucination, explainability, computational cost, and adversarial prompt manipulation remain significant research concerns in AI-driven cybersecurity systems.

3.1.1. Transformer-based intrusion detection systems

Transformer architectures have recently emerged as highly effective approaches for sequential network traffic analysis and adaptive anomaly detection. Self-attention mechanisms enable Transformer-based cybersecurity frameworks to capture long-range traffic dependencies and contextual communication behavior more effectively compared with conventional recurrent neural networks.

3.1.2. GNN-based intrusion detection systems

Graph neural network based intrusion detection systems model network traffic as graph structures consisting of interconnected communication nodes and traffic relationships. These graph-driven cybersecurity frameworks effectively capture attack propagation behavior and distributed malicious activities within enterprise environments.

3.1.3. Explainable AI for cybersecurity

Explainable AI techniques improve transparency and interpretability in intelligent intrusion detection systems. Explainable cybersecurity frameworks utilize SHAP and LIME techniques to provide interpretable threat detection capability and feature importance analysis.

3.1.4. Edge AI and lightweight intrusion detection systems

Edge AI based intrusion detection systems focus on deploying lightweight intelligent cybersecurity frameworks within Internet of Things and edge computing environments to enable low-latency real-time threat detection.

3.2. Comparative analysis of existing studies

Recent advancements in AI driven intrusion detection systems have significantly improved the capability of modern network security frameworks to identify sophisticated cyber threats, anomalous traffic behaviors, and zero-day attacks. Existing cybersecurity studies demonstrate that machine learning and deep learning based intrusion detection techniques provide superior adaptability, automated feature extraction capability, and intelligent behavioral analysis compared with conventional signature-based security mechanisms [6], [7].

Traditional machine learning approaches including support vector machines, decision trees, k-nearest neighbors, and random forest classifiers have been extensively applied for network traffic classification and anomaly detection tasks [13]–[15]. These approaches demonstrate strong classification performance for structured network traffic datasets and moderate computational complexity. However, their effectiveness decreases when analyzing high-dimensional encrypted traffic and rapidly evolving attack patterns in large-scale distributed network environments.

Deep learning based intrusion detection systems have substantially improved cybersecurity analytics through hierarchical feature learning and temporal traffic analysis. Recurrent neural networks, long short-term memory architectures, convolutional neural networks, and autoencoder

based anomaly detection frameworks have demonstrated strong capability in detecting sophisticated network intrusions, encrypted malicious traffic, and adaptive adversarial attacks [8]–[10], [16], [18]. Furthermore, hybrid deep learning architectures integrating CNN and LSTM models have significantly enhanced sequential attack detection, behavioral traffic analysis, and real-time anomaly identification [29]–[33].

Distributed and federated intrusion detection frameworks have also emerged as promising cybersecurity solutions for cloud-native infrastructures, Internet of Things ecosystems, and distributed enterprise environments. Federated learning based intrusion detection systems enable collaborative threat intelligence generation and privacy-preserving anomaly detection without directly sharing sensitive network traffic data [19], [20], [32]. These intelligent distributed cybersecurity architectures improve scalability, decentralized learning capability, and adaptive threat mitigation in heterogeneous network infrastructures.

The comparative analysis presented in Table 1 demonstrates that deep learning and hybrid AI based intrusion detection systems substantially improve anomaly detection capability, encrypted traffic analysis, adaptive threat intelligence, and real-time cybersecurity analytics compared with traditional rule-based and shallow machine learning approaches. Statistical anomaly detection techniques have also demonstrated significant effectiveness in identifying abnormal traffic behaviors and unknown attack patterns within dynamic network environments [27]. However, computational scalability, adversarial robustness, explainability, false positive reduction, and distributed deployment complexity remain major research challenges for next-generation intelligent network security systems.

4. Summary of reviewed research studies

Recent AI based intrusion detection research demonstrates significant advancements in intelligent cybersecurity analytics, anomaly detection capability, and adaptive threat identification. Existing studies primarily focus on machine learning, deep learning, hybrid intrusion detection architectures, and distributed cybersecurity frameworks for identifying sophisticated cyberattacks and abnormal network traffic patterns.

Deep learning based approaches including recurrent neural networks, convolutional neural networks, autoencoders, and hybrid CNN-LSTM architectures have demonstrated strong capability in encrypted traffic analysis, sequential anomaly detection, and adaptive cybersecurity intelligence. Furthermore, federated learning and distributed intrusion detection systems have emerged as promising solutions for privacy-preserving cybersecurity analytics within cloud and Internet of Things environments.

Table 2 summarizes the major AI based intrusion detection studies reviewed in this paper, including their datasets, methodologies, performance metrics, and major research limitations.

4.1. Research gaps and contributions

Despite substantial advancements in AI based intrusion detection systems, several important research challenges remain unresolved in modern cybersecurity infrastructures. Existing intelligent intrusion detection frameworks often struggle to effectively analyze encrypted network traffic and maintain robust performance against adversarial machine learning attacks. Furthermore, many deep learning based cybersecurity systems require extensive computational resources and large-scale training datasets, thereby limiting deployment capability within resource-constrained edge environments.

Current intrusion detection research also faces challenges associated with false positive reduction, dataset imbalance, concept drift, scalability limitations, explainability deficiencies, and privacy preservation in distributed enterprise infrastructures. Additionally, limited availability of realistic and heterogeneous cybersecurity datasets restricts the generalization capability of existing intrusion detection models across dynamic network environments.

Another significant limitation of existing intrusion detection research is the absence of standardized evaluation methodologies across heterogeneous cybersecurity datasets. Many studies report high detection accuracy under controlled experimental conditions but fail to demonstrate robustness under real-time deployment scenarios involving encrypted traffic, class imbalance, adversarial manipulation, and concept drift. Consequently, direct performance comparison among intelligent intrusion detection frameworks remains challenging.

The major contributions of this review are summarized as follows:

- Comprehensive comparison of machine learning, deep learning, federated learning, Transformer-based, and graph neural network based intrusion detection frameworks.
- Technical evaluation of benchmark intrusion detection datasets and their practical limitations.
- Comparative investigation of explainable AI, adversarial robustness, and encrypted traffic analysis techniques.
- Critical analysis of scalability, computational complexity, deployment overhead, and real-time applicability of intelligent intrusion detection systems.
- Identification of future research directions including edge AI cybersecurity, self-supervised intrusion detection, and distributed intelligent threat analytics.

4.2. Performance evaluation metrics

AI based intrusion detection systems are commonly evaluated using multiple cybersecurity performance metrics including accuracy, precision, recall, F1-score, false positive rate, detection rate, and computational latency.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

$$F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{4}$$

Table 1: Comparative analysis of existing intrusion detection techniques.

Technique	**Dataset**	**Strengths**	**Limitations**
SVM	NSL-KDD	Effective for structured traffic classification, anomaly detection, high-dimensional feature analysis, and moderate-sized cybersecurity datasets	Limited scalability for large-scale real-time traffic analysis, reduced performance under encrypted traffic, and computational inefficiency for massive datasets
Random Forest	CICIDS2017	High classification accuracy, reduced overfitting, strong ensemble learning capability, and effective feature importance estimation	Lower effectiveness for sequential traffic analysis, increased memory consumption, and limited temporal dependency modeling capability
RNN/LSTM	UNSW-NB15	Strong temporal traffic learning capability, sequential anomaly detection, adaptive behavioral analysis, and effective long-range dependency modeling	High computational complexity, extensive training requirements, gradient instability, and increased deployment latency for real-time systems
Autoencoder-based IDS	NSL-KDD	Effective unsupervised anomaly detection, automated feature extraction, nonlinear dimensionality reduction, and capability for unknown attack identification	Sensitive to dataset imbalance, noisy traffic behavior, reconstruction bias, and instability under adversarial attack environments
CNN-LSTM hybrid IDS	CICIDS2017	Improved encrypted traffic analysis, spatial-temporal feature extraction, adaptive attack detection, and enhanced intelligent behavioral analytics	Increased deployment complexity, computational overhead, extensive GPU requirements, and scalability challenges for edge infrastructures
Federated intrusion detection	Distributed IoT Traffic	Privacy-preserving collaborative cybersecurity analytics, decentralized learning capability, scalable distributed intelligence, and reduced centralized data dependency	Communication overhead, synchronization challenges, inference privacy leakage, heterogeneous client behavior, and adversarial federated manipulation risks
Transformer-based IDS	CSE-CIC-IDS2018	Long-range dependency learning, contextual traffic representation, adaptive attention mechanisms, and strong sequential anomaly analysis capability	Extremely high computational complexity, large-scale training requirements, memory overhead, and reduced explainability in real-time deployments
GNN IDS	Bot-IoT	Effective attack propagation analysis, communication relationship modeling, distributed anomaly identification, and intelligent graph-based threat analytics	Complex graph construction requirements, scalability limitations, and high processing overhead for dynamic enterprise networks
Self-supervised IDS	TON-IoT	Reduced dependency on labeled datasets, adaptive online learning capability, and improved anomaly generalization under evolving attack environments	Training instability, pseudo-label noise sensitivity, and limited benchmark standardization for evaluation consistency

In (1)-(4), the TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives respectively.

5. Benchmark Intrusion detection datasets

Benchmark intrusion detection datasets play an important role in evaluating the effectiveness, scalability, and generalization capability of AI based cybersecurity frameworks.

5.1. NSL-KDD Dataset

The NSL-KDD dataset was developed as an improved version of the KDD Cup 1999 dataset to eliminate duplicate records and improve dataset balance. The dataset contains multiple attack categories including denial-of-service attacks, probing attacks, remote-to-local attacks, and user-to-root attacks [24].

5.2. CICIDS2017 Dataset

The CICIDS2017 dataset provides realistic network traffic and modern cyberattack scenarios including brute-force attacks, botnet traffic, denial-of-service attacks, and web-based attacks. The dataset is extensively utilized for evaluating deep learning based intrusion detection systems [25].

5.3. UNSW-NB15 Dataset

The UNSW-NB15 dataset includes modern hybrid network traffic generated using realistic attack simulation environments. The dataset contains diverse traffic features and contemporary cyberattack categories [26].

5.4. TON-IoT Dataset

The TON-IoT dataset was specifically designed for Internet of Things cybersecurity research. It includes telemetry data, operating system logs, IoT traffic, and distributed attack behaviors generated within smart environments.

Table 2: Summary of reviewed AI-based intrusion detection studies.

Reference	**Technique**	**Dataset**	**Model Type**	**Performance Metric**	**Major Limitation**
Yin et al. [9]	RNN	NSL-KDD	Deep Learning	High Accuracy	High Training Complexity
Shone et al. [10]	Autoencoder	NSL-KDD	Unsupervised Deep Learning	Improved Detection Rate	Dataset Imbalance
Diro et al. [32]	Distributed Deep Learning	IoT Traffic	Federated Learning	Privacy Preservation	Communication Cost
Khan et al. [35]	CNN-LSTM	CICIDS2017	Hybrid Deep Learning	Strong Sequential Analysis	Computational Overhead
Ferrag et al. [36]	Deep Learning IDS	Multiple Datasets	Comparative Review	Strong Classification	Explainability Issues

Table 3: Comparison of benchmark intrusion detection datasets

Dataset	**Year**	**Traffic Type**	**Advantages**	**Limitations**
NSL-KDD	2009	Simulated	Reduced redundancy, balanced training records, improved benchmark consistency, and simplified preprocessing for traditional intrusion detection evaluation	Outdated attack patterns, unrealistic modern traffic behavior, limited encrypted traffic representation, and inadequate scalability for contemporary enterprise environments
CICIDS2017	2017	Realistic	Modern attack scenarios with realistic traffic behavior, diverse attack categories, encrypted communication representation, and comprehensive flow-based features	Complex preprocessing requirements, large feature dimensionality, computational overhead, and significant class imbalance issues
UNSW-NB15	2015	Hybrid	Diverse attack categories, contemporary traffic generation, realistic hybrid traffic simulation, and rich feature representation for anomaly analysis	Dataset imbalance, noisy traffic instances, limited large-scale deployment representation, and preprocessing complexity
TON-IoT	2020	IoT Traffic	Supports IoT, edge, telemetry, and distributed attack analysis with realistic smart-environment traffic generation and heterogeneous device behavior	High-dimensional features, preprocessing complexity, computational overhead, and limited standardization for cross-platform benchmarking
DARPA 1998	1998	Simulated	One of the earliest standardized benchmark datasets for intrusion detection evaluation and attack classification research	Synthetic traffic generation, outdated attack representation, unrealistic communication patterns, and limited applicability for modern cybersecurity environments
Bot-IoT	2019	IoT Traffic	Large-scale IoT attack representation, botnet traffic analysis capability, and support for distributed denial-of-service attack evaluation	Severe dataset imbalance, redundancy issues, and limited encrypted communication representation
CSE-CIC-IDS2018	2018	Realistic	Large-scale realistic enterprise traffic generation, modern attack diversity, and extensive network flow features for deep learning analysis	High computational requirements, preprocessing complexity, and large storage overhead for real-time deployment

6. Conclusion

This paper presented a systematic technical literature review of AI based intrusion detection systems and intelligent network security frameworks. The review analyzed machine learning based intrusion detection models, deep learning cybersecurity architectures, anomaly detection techniques, federated learning frameworks, and benchmark intrusion detection datasets widely used in cybersecurity research. The analysis demonstrated that deep learning based intrusion detection systems significantly improve anomaly detection capability, adaptive threat intelligence, and real-time cybersecurity analytics compared with traditional signature-based approaches. Furthermore, hybrid intelligent cybersecurity frameworks integrating anomaly detection, behavioral analytics, and distributed learning mechanisms have emerged as promising approaches for large-scale enterprise network environments. The review also identified critical research challenges associated with encrypted traffic analysis, adversarial robustness, explainable AI, false positive reduction, and computational scalability in distributed cybersecurity infrastructures. Future

research is expected to focus on explainable intrusion detection systems, graph neural cybersecurity architectures, federated intrusion detection frameworks, and edge-based intelligent security analytics.

Declarations and ethical statements

Conflict of interest: The authors declare that there is no conflict of interest.
Funding statement: The authors declare that no specific funding was received for this research.
Artificial Intelligence usage statement: During the preparation of this manuscript, the authors utilized AvalAI (https://avalai.ir/) solely for language refinement and grammatical corrections. The authors carefully reviewed and revised the generated content and take full responsibility for the accuracy, integrity, and originality of the final manuscript.
Availability of data and materials: All data and information used in this work were obtained from publicly available published literature and cited sources.

CRediT authorship contribution statement

Mehdi Gheisari: Conceptualization, Investigation, Writing – review & editing. **Zhou Pingmei**: Data collection, Data curation & Visualization. **Basheer Riskhan**: Conceptualization & Formal analysis. **Malusi Sibiya**: Conceptualization & Formal analysis. **Muhammad Faizan Khan**: Conceptualization, Editing & Formal analysis.

Publisher's note

Krrish Scientific Publications Pvt. Ltd. and the ***Journal of Computing and Data Technology*** remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Denning DE. An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*. 1987 Feb 28(2):222-32. Available from: https://doi.org/10.1109/TSE.1987.232894

[2] Lunt TF. A survey of intrusion detection techniques. *Computers & Security*. 1993 Jun 1;12(4):405-18. Available from: https://doi.org/10.1016/0167-4048(93)90029-5

[3] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*. 2013 Jan 1;36(1):42-57. Available from: https://doi.org/10.1016/j.jnca.2012.05.003

[4] Roesch M. Snort: Lightweight intrusion detection for networks. *In LISA '99: Proceedings of the 13th USENIX conference on System administration* 1999 Nov 7 (Vol. 99, No. 1, pp. 229-238).

[5] Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*. 2009 Feb 1;28(1-2):18-28. Available from: https://doi.org/10.1016/j.cose.2008.08.003

[6] Sommer R, Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *In 2010 IEEE symposium on security and privacy* 2010 May 16 (pp. 305-316). IEEE. Available from: https://doi.org/10.1109/SP.2010.25

[7] Buczak AL, Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2015 Oct 26;18(2):1153-76. Available from: https://doi.org/10.1109/COMST.2015.2494502

[8] Kim G, Lee S, Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*. 2014 Mar 1;41(4):1690-700. Available from: https://doi.org/10.1016/j.eswa.2013.08.066

[9] Yin C, Zhu Y, Fei J, He X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*. 2017 Oct 12;5:21954-61. Available from: https://doi.org/10.1109/ACCESS.2017.2762418

[10] Shone N, Ngoc TN, Phai VD, Shi Q. A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*. 2018 Jan 22;2(1):41-50. Available from: https://doi.org/10.1109/TETCI.2017.2772792

[11] Vinayakumar R, Soman KP, Poornachandran P. Applying deep learning approaches for network traffic prediction. *In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* 2017 Sep 13 (pp. 2353-2358). IEEE. Available from: https://doi.org/10.1109/ICACCI.2017.8126198

[12] Apruzzese G, Colajanni M, Ferretti L, Guido A, Marchetti M. On the effectiveness of machine and deep learning for cyber security. *In 2018 10th international conference on cyber Conflict (CyCon)* 2018 May 29 (pp. 371-390). IEEE. Available from: https://doi.org/10.23919/CYCON.2018.8405026

[13] Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. *In Proceedings of IEEE international joint conference on neural networks* 2002 May 12 (Vol. 2, pp. 1702-1707). Available from: https://doi.org/10.1109/IJCNN.2002.1007774

[14] Lee W, Stolfo S. Data mining approaches for intrusion detection. *SSYM'98: Proceedings of the 7th conference on USENIX Security Symposium - Volume 7, San Antonio, Texas* January 26-29, 1998. Available from: https://dl.acm.org/doi/10.5555/1267549.1267555

[15] Breiman L. Random Forests. *Machine learning*. 2001 Oct;45(1):5-32. Available from: https://link.springer.com/article/10.1023/A:1010933404324

[16] Hochreiter S, Schmidhuber J. Long Short-Term memory. *Neural Computation*. 1997 Nov 1;9(8):1735–80. Available from: https://doi.org/10.1162/neco.1997.9.8.1735

[17] Hundman K, Constantinou V, Laporte C, Colwell I, Soderstrom T.Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding. *In Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*2018 Jul 19 (pp. 387-395). Available from: https://doi.org/10.1145/3219819.3219845

[18] Sakurada M, Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction. *In Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis* 2014 Dec 2 (pp. 4-11). Available from: https://dl.acm.org/doi/abs/10.1145/2689746.2689747

[19] Yang Q, Liu Y, Chen T, Tong Y. Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*. 2019 Jan 28;10(2):1-9. Available from: https://doi.org/10.1145/3298981

[20] McMahan B, Moore E, Ramage D, Hampson S, y Arcas BA. Communication-Efficient Learning of Deep Networks from Decentralized Data. *In Artificial intelligence and statistics* 2017 Apr 10 (pp. 1273-1282). Pmlr. Available from: https://doi.org/10.48550/arXiv.1602.05629

[21] Goodfellow IJ, Shlens J, Szegedy C. Explaining and Harnessing Adversarial Examples. *arXiv preprint arXiv:1412.6572*. 2014 Dec 20. Available from: https://doi.org/10.48550/arXiv.1412.6572

[22] Papernot N, McDaniel P, Sinha A, Wellman MP. SoK: Security and Privacy in Machine Learning. *In 2018 IEEE European*

symposium on security and privacy (EuroS&P) 2018 Apr 24 (pp. 399-414). IEEE. Available from: https://doi.org/10.1109/EuroSP.2018.00035

[23] Mirsky Y, Doitshman T, Elovici Y, Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. *arXiv preprint arXiv:1802.09089*. 2018 Feb 25. Available from: https://doi.org/10.48550/arXiv.1802.09089

[24] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. *In 2009 IEEE symposium on computational intelligence for security and defense applications* 2009 Jul 8 (pp. 1-6). IEEE . Available from: https://doi.org/10.1109/CISDA.2009.5356528

[25] Sharafaldin I, Lashkari AH, Ghorbani AA. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy - ICISSP*.2018 Jan 22;1(2018):108-116. Available from: https://doi.org/10.5220/0006639801080116

[26] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *In 2015 military communications and information systems conference (MilCIS)* 2015 Nov 10 (pp. 1-6). Ieee. Available from: https://doi.org/10.1109/MilCIS.2015.7348942

[27] Patcha A, Park JM. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*. 2007 Aug 22;51(12):3448-70. Available from: https://doi.org/10.1016/j.comnet.2007.02.001

[28] Lippmann RP, Fried DJ, Graf I, Haines JW, Kendall KR, McClung D, Weber D, Webster SE, Wyschogrod D, Cunningham RK, Zissman MA. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation. *In Proceedings DARPA Information survivability conference and exposition*. DISCEX'00 2000 Jan 25 (Vol. 2, pp. 12-26). IEEE. Available from: https://doi.org/10.1109/DISCEX.2000.821506

[29] Wang W, Zhu M, Zeng X, Ye X, Sheng Y. Malware traffic classification using convolutional neural network for representation learning. *In 2017 International conference on information networking (ICOIN)* 2017 Jan 11 (pp. 712-717). IEEE. Available from: https://doi.org/10.1109/ICOIN.2017.7899588

[30] Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system. *EAI Endorsed Transactions on Security and Safety*. 2016 Dec 1;3(9):21. Available from: https://doi.org/10.4108/eai.3-12-2015.2262516

[31] Alrawashdeh K, Purdy C. Toward an Online Anomaly Intrusion Detection System Based on Deep Learning. *In 2016 15th IEEE international conference on machine learning and applications (ICMLA)* 2016 Dec 18 (pp. 195-200). IEEE. Available from: https://doi.org/10.1109/ICMLA.2016.0040

[32] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*. 2018 May 1;82:761-8. Available from: https://doi.org/10.1016/j.future.2017.08.043

[33] Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*. 2019 Apr 3;7:41525-50. Available from: https://doi.org/10.1109/ACCESS.2019.2895334

[34] Ring M, Wunderlich S, Scheuring D, Landes D, Hotho A. A survey of network-based intrusion detection data sets. *Computers & security*. 2019 Sep 1;86:147-67. Available from: https://doi.org/10.1016/j.cose.2019.06.005

[35] Khan MA, Karim MR, Kim Y. A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*. 2019 Apr 22;11(4):583. Available from: https://doi.org/10.3390/sym11040583

[36] Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*. 2020 Feb 1;50:102419. Available from: https://doi.org/10.1016/j.jisa.2019.102419

[37] Kumar S, Gupta S, Arora S. Research Trends in Network-Based Intrusion Detection Systems: A Review. *IEEE Access*. 2021 Nov 22;9:157761-79. Available from: https://doi.org/10.1109/ACCESS.2021.3129775

[38] Kilincer IF, Ertam F, Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks*. 2021 Apr 7;188:107840. Available from: https://doi.org/10.1016/j.comnet.2021.107840

[39] Jullian O, Otero B, Rodriguez E, Gutierrez N, Antona H, Canal R. Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. *Journal of Network and Systems Management*. 2023 Apr;31(2):33. Available from: https://link.springer.com/article/10.1007/s10922-023-09722-7

[40] Hariharan S, Jerusha YA, Suganeshwari G, Ibrahim SS, Tupakula U, Varadharajan V. A Hybrid Deep Learning Model for Network Intrusion Detection System Using Seq2Seq and ConvLSTM-Subnets. *IEEE Access*. 2025 Feb 13. Available from: https://doi.org/10.1109/ACCESS.2025.3541399

[41] Nakıp M, Gelenbe E. Online Self-Supervised Deep Learning for Intrusion Detection Systems. *IEEE Transactions on Information Forensics and Security*. 2024 May 16;19:5668-83. Available from: https://doi.org/10.1109/TIFS.2024.3402148

[42] Wahab OA. Intrusion Detection in the IoT Under Data and Concept Drifts: Online Deep Learning Approach. *IEEE Internet of Things Journal*. 2022 Apr 12;9(20):19706-16. Available from: https://doi.org/10.1109/JIOT.2022.3167005

[43] Lakshminarayana DH, Philips J, Tabrizi N. A Survey of Intrusion Detection Techniques. *In 2019 18th IEEE international conference on machine learning and applications (ICMLA)* 2019 Dec 16 (pp. 1122-1129). IEEE. Available from: https://doi.org/10.1109/ICMLA.2019.00187

[44] Khamphakdee N, Benjamas N, Saiyod S. Improving Intrusion Detection System based on Snort rules for network probe attack detection. *In 2014 2nd International Conference on Information and Communication Technology (ICoICT)* 2014 May 28 (pp. 69-74). IEEE. Available from: https://doi.org/10.1109/ICoICT.2014.6914042

[45] Salem A, Cherubin G, Evans D, Köpf B, Paverd A, Suri A, Tople S, Zanella-Béguelin S. SoK: Let the Privacy Games Begin! A Unified Treatment of Data Inference Privacy in Machine Learning. *In 2023 IEEE Symposium on Security and Privacy (SP)* 2023 May 21 (pp. 327-345). IEEE. Available from: https://doi.org/10.1109/SP46215.2023.10179281

[46] Bendiab G, Shiaeles S, Alruban A, Kolokotronis N. IoT Malware Network Traffic Classification using Visual Representation and Deep Learning. *In 2020 6th IEEE Conference on Network Softwarization (NetSoft)* 2020 Jun 29 (pp. 444-449). IEEE. Available from: https://doi.org/10.1109/NetSoft48620.2020.9165381

[47] Sun Y, Ochiai H, Esaki H. Decentralized Deep Learning for Multi-Access Edge Computing: A Survey on Communication Efficiency and Trustworthiness. *IEEE Transactions on Artificial Intelligence*. 2021 Dec 10;3(6):963-72. Available from: https://doi.org/10.1109/TAI.2021.3133819

[48] Manjunatha BA, Shastry KA, Naresh E, Pareek PK, Reddy KT. A network intrusion detection framework on sparse deep denoising auto-encoder for dimensionality reduction. *Soft Computing*. 2024 Mar;28(5):4503-17. Available from: https://link.springer.com/article/10.1007/s00500-023-09408-x

[49] Siddique K, Akhtar Z, Khan FA, Kim Y. KDD Cup 99 Data Sets: A Perspective on the Role of Data Sets in Network Intrusion Detection Research. *Computer*. 2019 Mar 21;52(2):41-51. Available from: https://doi.org/10.1109/MC.2018.2888764

[50] Fidel G, Bitton R, Shabtai A. When Explainability Meets Adversarial Learning: Detecting Adversarial Examples using SHAP Signatures. *In 2020 International Joint Conference on Neural Networks (IJCNN)* 2020 Jul 19 (pp. 1-8). IEEE. Available from: https://doi.org/10.1109/IJCNN48605.2020.9207637

[51] Pothireddy SR. Cloud-Native AI-Driven Enterprise Automation for Scalable Digital Process Transformation in Multi-Industry Ecosystems. *Journal of Applied Sciences and Modelling*. 2025 Dec 31:60-74. Available from: https://doi.org/10.71426/jas

m.v1.i1.pp60-74

[52] Oyinna B, Udo PD, Nurhidayat I, Muslimyar AR. Integrating data processing and advanced analytics for scalable knowledge discovery in complex data environments. *Journal of Computing and Data Technology*. 2025;1(2):115-20. Available from: https://doi.org/10.71426/jcdt.v1.i2.pp115-120

[53] Penaganti R. Security-Trust-Determinism Co-Design Using Hybrid Intrusion Detection With Temporal Modeling for Real-Time Publish-Subscribe Middleware. *IEEE Communications Standards Magazine*. 2026 Apr 1. Available from: https://doi.org/10.1109/MCOMSTD.2026.3676622

[54] Penaganti R. Graph neural network-based framework for real-time financial fraud detection in digital payment ecosystems. *Journal of Computing and Data Technology*. 2025;1(2):91-7. Available from: https://doi.org/10.71426/jcdt.v1.i2.pp91-97

[55] Safaei Yaraziz M, Jalili A, Gheisari M, Liu Y. Recent trends towards privacy-preservation in Internet of Things, its challenges and future directions. *IET circuits, devices & systems*. 2023 Mar;17(2):53-61. Available from: https://doi.org/10.1049/cds2.12138

[56] Gheisari M, Ebrahimzadeh F, Rahimi M, Moazzamigodarzi M, Liu Y, Dutta Pramanik PK, Heravi MA, Mehbodniya A, Ghaderzadeh M, Feylizadeh MR, Kosari S. Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey. *CAAI Transactions on Intelligence Technology*. 2023 Sep;8(3):581-606. Available from: https://doi.org/10.1049/cit2.12180

[57] Lee CC, Lin TH, Tsai CS. A new authenticated group key agreement in a mobile environment. *Annals of Telecommunications*. 2009 Dec;64(11):735. Available from: https://doi.org/10.1007/s12243-009-0096-z

[58] Li CT, Lee CC, Weng CY. An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dynamics*. 2013 Dec;74(4):1133-43. Available from: https://doi.org/10.1007/s11071-013-1029-y