Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Systematic Review of Multi-Model Machine Learning Approaches for Network Anomaly Detection and Security

Mitesh Bargadiya[1*], Deepak K. Yadav[2], Lalita Tonke[3]

[1,2,3]SAGE University, Indore (M.P.), India

[1]miteshbargadiya@gmail.com,[2]deepak_ku_yadav@outlook.com, [3]lalita.tonke1@gmail.com

*Corresponding Author & Email: Mitesh Bargadiya

miteshbargadiya@gmail.com

ARTICLE INFO

Received: 29 Nov 2024

Revised: 16 Dec 2024

Accepted: 23 Dec 2024

Published: 30 Dec 2024

ABSTRACT

The rapid expansion of interconnected digital infrastructures such as Cyber-Physical Systems (CPS), Supervisory Control and Data Acquisition (SCADA) networks, Internet of Things (IoT) environments, smart grids, cloud platforms, and smart cities has significantly increased exposure to cyber threats. Traditional anomaly detection and intrusion detection systems, largely based on signature matching and rule-based monitoring, struggle to detect sophisticated attacks such as zero-day intrusions, distributed denial-of-service (DDoS) campaigns, stealth anomalies, and adversarial manipulation. Consequently, researchers have adopted machine learning (ML) and deep learning (DL) techniques to enhance anomaly detection accuracy, robustness, and adaptability across diverse network environments. This systematic review examines recent multi-model approaches including supervised, unsupervised, ensemble, hybrid, and deep learning-based frameworks used for network anomaly detection and cyber security improvement. The review highlights widely used models such as Support Vector Machines, Random Forest, Gradient Boosting, Convolutional Neural Networks, Long Short-Term Memory networks, and Autoencoders, alongside emerging multi-model integrations such as GAN-based synthetic data generation, Transformer-based sequential modeling, Vision Transformers, and fusion pipelines combining Isolation Forest, GANs, and Transformers. Findings reveal that hybrid and multi-model architectures frequently outperform standalone methods, especially in domains such as CPS water distribution, DDoS detection, cloud anomaly classification, and IoT intrusion detection, with multiple studies reporting near-perfect performance under controlled datasets. However, major limitations remain, including dependence on benchmark datasets, lack of real-world industrial validation,

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

limited explainability, computational complexity, dataset imbalance, and insufficient evaluation against encrypted and zero-day attacks. This review consolidates existing methodologies, compares strengths and weaknesses across domains, identifies critical research gaps, and provides future research directions focused on deployment-ready, scalable, explainable, privacy-aware, and edge-efficient anomaly detection frameworks for next-generation network security.

Keywords: Systematic Review; Network Anomaly Detection; Intrusion Detection System (IDS); Multi-Model Machine Learning; Hybrid Deep Learning; Cybersecurity; DDoS, SCADA Security; Cyber-Physical Systems; IoT Security; Generative Adversarial Networks (GAN); Transformers; Vision Transformers; Autoencoders; Industry 4.0; Critical Infrastructure Protection.

Introduction

Industrial and digital infrastructures have become deeply dependent on interconnected networks, making cybersecurity a fundamental requirement for modern computing environments. From traditional enterprise communication systems to advanced Industry 4.0 architectures, networks now support critical operations such as power distribution, transportation, healthcare services, smart homes, and large-scale cloud applications [1]. These networks are no longer isolated; instead, they rely on internet connectivity, remote management, and interoperable protocols that improve efficiency but also increase exposure to cyber threats. As attackers continuously exploit vulnerabilities in connected systems, network security has evolved from being a supportive feature to becoming a core necessity for ensuring safety, reliability, and operational continuity [2].

One of the most significant challenges in cybersecurity is the detection of anomalous activities that may indicate intrusions, malware behavior, denial-of-service attacks, or unauthorized access. Conventional security mechanisms such as firewalls, rule-based intrusion detection systems (IDS), and signature-based detection tools have played an important role in identifying known threats [3]. However, these traditional methods struggle against emerging cyberattacks, particularly those that are stealthy, adaptive, or previously unseen (zero-day attacks). In environments such as Supervisory Control and Data Acquisition (SCADA) systems and Cyber-Physical Systems (CPS), the consequences of an attack are more severe because security incidents can disrupt physical infrastructure such as water plants, smart grids, and industrial automation processes. Similarly, Internet of Things (IoT) environments introduce massive device heterogeneity and continuous data generation, making manual or rule-based monitoring inadequate [4].

To address these limitations, researchers have increasingly adopted machine learning (ML) and deep learning (DL) techniques for anomaly detection. ML models such as Support Vector Machines (SVM), Random Forest, and Gradient Boosting are widely used because they can learn discriminative patterns from traffic data and improve detection accuracy compared to static rules [5]. Deep learning models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Autoencoders further enhance anomaly detection by learning complex representations from high-dimensional network traffic and time-series signals. However, individual models often face challenges such as data imbalance, scarcity of labeled anomalies, high false-alarm rates, and weak generalization across datasets [6].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Consequently, recent studies show a growing shift toward multi-model and hybrid learning frameworks, where deep learning-based feature extraction is combined with machine learning classifiers for improved robustness. Additionally, advanced approaches such as Generative Adversarial Networks (GANs) are being explored to generate synthetic anomaly samples and overcome rare-event scarcity, while Transformer and Vision Transformer (ViT) architectures are gaining attention due to their capability of capturing long-range dependencies and achieving high detection performance [7]. In this context, a systematic review of multi-model machine learning approaches is essential to summarize existing methodologies, analyze reported results, identify research gaps, and outline future directions for building reliable, scalable, and intelligent network security systems [8].

2. Literature Review

SCADA systems, crucial for industrial automation, are vulnerable to cyberattacks due to their connectivity and remote access capabilities. This study uses a testbed environment to simulate a water plant with a SCADA system, designing five DDoS attack scenarios to evaluate the system's resilience. Various machine learning models, including hybrid deep learning models, were applied to detect these attacks, with the hybrid and decision tree models achieving the highest accuracies of 95% and 99%, respectively [1].

Anomaly detection is essential for identifying potential network security threats. Traditional methods are inadequate against sophisticated cyber threats, prompting the adoption of machine learning (ML) techniques. This paper reviews various ML approaches, such as supervised, unsupervised, ensemble, and hybrid methods, exploring their effectiveness in enhancing anomaly detection accuracy and robustness [2].

Cyberattacks on critical infrastructure networks pose significant challenges for conventional machine learning methods. This paper introduces a deep learning-based approach using DNN, LSTM, and Deep Sparse Autoencoder models to improve anomaly detection accuracy. The method is validated on IoT datasets, demonstrating superior performance over traditional techniques [3].

Anomaly detection faces data scarcity challenges, particularly for rare abnormal behaviors. This study reviews the use of Generative Adversarial Networks (GANs) for network anomaly detection, focusing on their capability for representation learning. It provides insights into the practical application and effectiveness of GANs in improving anomaly detection systems [4].

This study proposes a one-dimensional CNN model for network anomaly detection, categorizing network traffic data by protocol types (TCP, UDP, and others). Using feature selection and oversampling techniques, the model achieved notable F-scores for different categories, demonstrating its effectiveness on the UNSW-NB15 dataset [5].

This paper presents a hybrid deep learning model combining a GRU-based Stacked Autoencoder with various anomaly detection algorithms to enhance cybersecurity in smart grids. Evaluated using the IEC 60870-5-104 dataset, the proposed approach outperformed standalone methods, proving effective in accurately detecting and preventing cyberattacks [6].

This study introduces a neural network-based security monitoring system for Beijing, utilizing multimodal data such as video, audio, and thermal data for comprehensive surveillance. The system achieved high accuracy in detecting overcrowding, unauthorized access, and unattended objects, with rapid response times due to edge computing. Advanced AI techniques like transfer learning and GANs improved adaptability, demonstrating the system’s potential to enhance urban security infrastructure [7].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This study proposes a fusion model combining Isolation Forest, GAN, and Transformer for network anomaly detection and log analysis. Each component contributes uniquely: Isolation Forest identifies anomalies, GAN generates synthetic data for training, and Transformer models time-series data. The model shows improved accuracy and reduced false alarms, highlighting its effectiveness in detecting network issues and promoting deep learning applications in network security [8].

As smart home networks become more complex, they face increased risks from adversarial attacks. This paper proposes a machine learning-based anomaly detection method, using network traffic data to distinguish between normal and abnormal behaviors. Tested against various adversarial attacks, the method achieved high accuracy and reliability, proving effective in safeguarding smart home networks [9].

This study presents a machine learning-based anomaly detection system for electric vehicle (EV) charging infrastructure. By analyzing charging data and records, the system accurately identifies abnormalities such as power surges and extended charging durations. The model's high accuracy and proactive maintenance strategies enhance the dependability and security of EV charging networks, providing a robust tool for real-world applications [10].

Addressing the challenge of detecting anomalies in complex cloud environments, this study proposes a deep Convolutional Neural Network (CNN) model, enhanced by a random forest feature selection method. Tested on the CSE-CIC-IDS2018 dataset, the model achieved 97.07% accuracy with high precision, recall, and F1 scores, demonstrating its effectiveness for real-time anomaly detection in Industry 4.0 systems [11].

This paper presents a new approach for detecting unusual activities in network traffic by combining Contractive Autoencoders (CAEs) and K-means clustering. The model uses CAEs for efficient data processing and K-means to detect deviations from normal patterns, achieving an F1 Score of 0.92 on the NSL-KDD dataset. This method is 8.2% more effective than a basic Autoencoder and 5.7% better than K-means alone, demonstrating significant improvements in network anomaly detection [12].

This study proposes an anomaly-based network outlier detection system (NODS) using optimized SVM and Gaussian Naive Bayes algorithms. Employing the NSL-KDD and CICIDS2017 datasets, the system demonstrates high classification accuracy and low false alarm rates. The results indicate the effectiveness of the SVM-based NODS compared to other existing methods for enhancing network security [13].

The paper introduces MST-DVGAN, an unsupervised dual variational GAN model, to detect anomalies in multivariate time series data for CPS security. The model enhances the distinction between normal and abnormal data and is tested on datasets like SWAT, WADI, and NSL_KDD. Results show consistent performance improvement over existing methods [14].

This study proposes a two-level anomaly detection strategy for Cyber-Physical Systems (CPS), using a hybrid CNN-LSTM for binary classification and a Gradient Boosting Machine for precise anomaly detection. Evaluated on a Water Distribution Testbed dataset, the model achieved F1-scores of 100% and 97.3% for network and physical data, respectively, demonstrating its high efficiency [15].

This paper focuses on using machine learning-based anomaly detection and adaptive defense mechanisms to enhance IoT security. It evaluates various ML models, including Random Forest and Gradient Boosting, and identifies Gradient Boosting as the most effective model with a precision of 89.34%, highlighting the potential of ML in safeguarding IoT devices against cyber threats [16].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The study addresses IoT security challenges by developing an intrusion detection system (IDS) using optimized ML and DL techniques, such as SVM, ensemble methods, LSTM, and vision transformers (ViT). The proposed IDS achieves high accuracy, precision, and AUC scores, with the ViT model reaching 100% in all metrics, demonstrating its potential for robust security in IoT networks [17].

Reviews machine learning and deep learning approaches for DDoS detection in Software Defined Networking (SDN) environments. The results show high detection accuracy (often above 99%) using models like CNN, LSTM, and hybrid techniques. Despite strong performance, issues such as scalability, real-world applicability, and dataset limitations are identified [18].

Systematic review of deep learning techniques such as CNN, RNN, and LSTM for detecting DDoS attacks in IoT networks.It highlights that deep learning models achieve high accuracy and improved detection rates compared to traditional methods. However, challenges remain in real-time deployment, dataset dependency, and handling evolving cyber threats [19].

This paper explores machine learning-based intrusion detection techniques for identifying network attacks, including DDoS. The proposed models demonstrate improved classification accuracy and effectiveness in detecting known attack patterns. Limitations include high computational cost, class imbalance, and reduced efficiency in detecting zero-day attacks [20].

This paper provides a comprehensive survey of ML-based techniques for detecting DDoS attacks in IoT environments. It analyzes models like Random Forest, SVM, and deep learning approaches across multiple datasets. The study highlights the need for lightweight, real-time IDS solutions for practical IoT deployment[21].

This systematic review explores deep learning techniques such as CNN, RNN, and LSTM for DDoS detection. It shows that deep learning models outperform traditional ML methods in detecting complex and evolving attacks. However, high computational requirements and lack of lightweight models remain major challenges[22].

This paper focuses on DDoS detection using machine learning within Software Defined Networking (SDN). It demonstrates that ML models improve detection accuracy and enable centralized control in SDN environments. The study identifies scalability and real-time implementation as key research gaps[23].

This paper presents an ensemble-based intrusion detection framework using multiple ML models such as SVM, KNN, RF, and LSTM. It evaluates performance across standard datasets to improve DDoS detection accuracy and reliability. The study emphasizes dataset diversity but lacks real-time SDN deployment validation[24].

This research proposes a hybrid ML-based approach integrated with SDN for both detection and mitigation of DDoS attacks. It uses intelligent traffic redirection to reduce attack impact and improve network performance. The model shows strong results but requires scalability testing in large distributed environments[25].

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

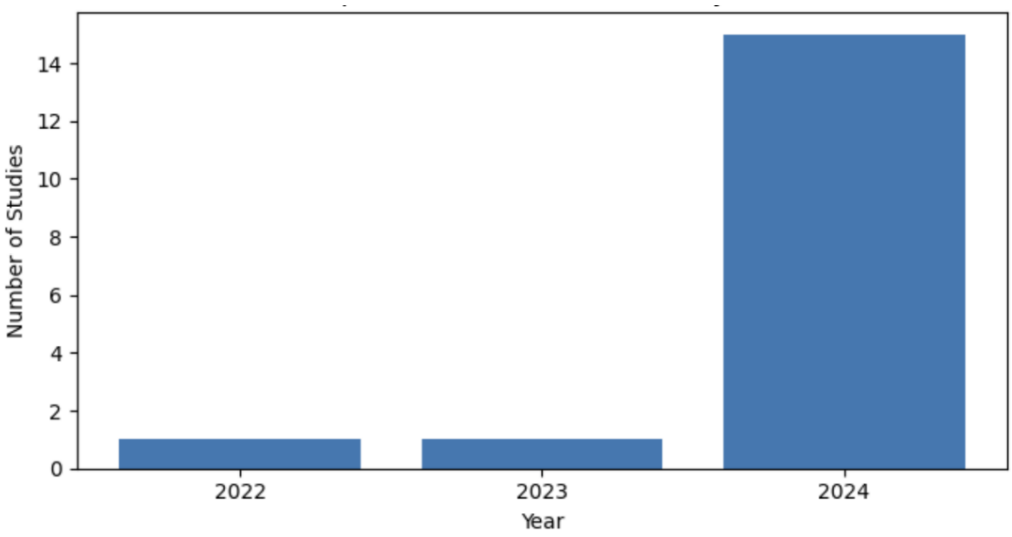

Figure 1. Distribution of Studies by Year

Figure 1 shows the publication year distribution of the selected studies in the systematic review. The figure clearly highlights that the majority of research work has been published in **2024**, indicating a rapidly growing interest in anomaly detection and cybersecurity solutions for CPS, IoT, SCADA, and cloud environments. Only a small number of studies belong to earlier years such as **2022 and 2023**, which demonstrates that many recent advancements—especially involving GANs, transformers, and hybrid deep learning—have emerged very recently. This trend confirms that anomaly detection is an actively evolving research area, driven by Industry 4.0 and increasing cyber threats.

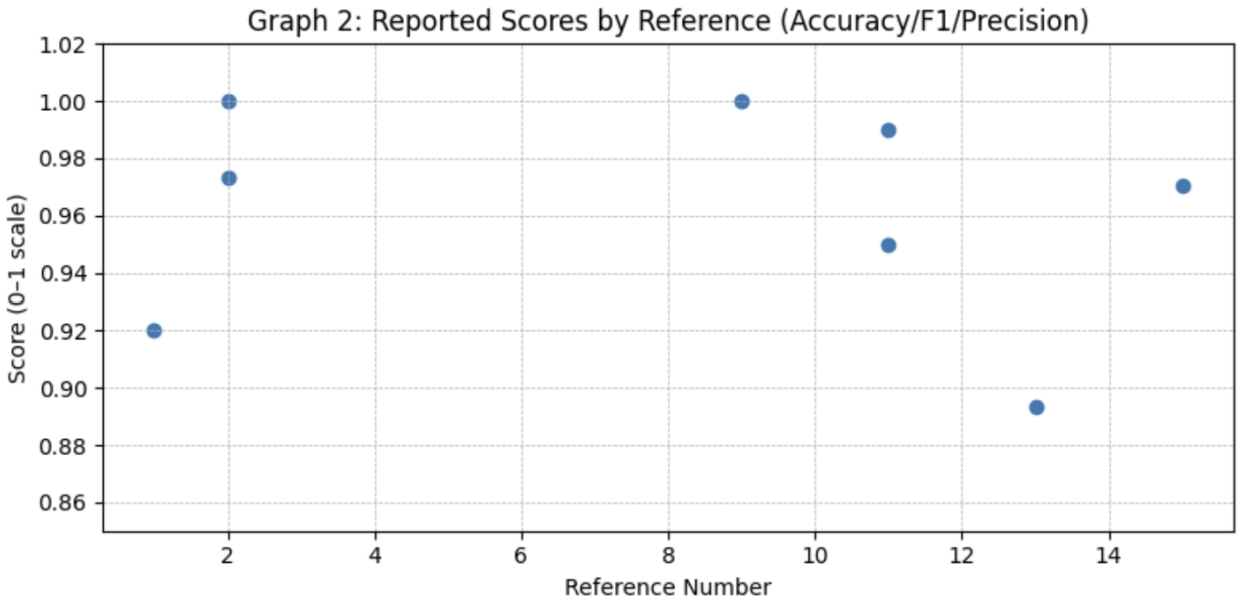

Figure 2. Reported Scores by Reference (Accuracy/F1/Precision)

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 2 presents the reported quantitative performance metrics (Accuracy, F1-score, and Precision) for studies that provided explicit numerical results. The plot reveals that several studies achieved very high performance close to **1.0 (100%)**, such as Ref [2] (CPS water system), Ref [9] (Vision Transformers for IoT), and Ref [11] (Decision Tree for SCADA DDoS). At the same time, Ref [13] shows comparatively lower performance (precision ≈ 0.8934), suggesting that IoT security challenges may require more advanced or hybrid approaches. Overall, the graph illustrates that modern deep learning and hybrid approaches tend to produce stronger detection results, but performance varies depending on domain complexity and datasets.

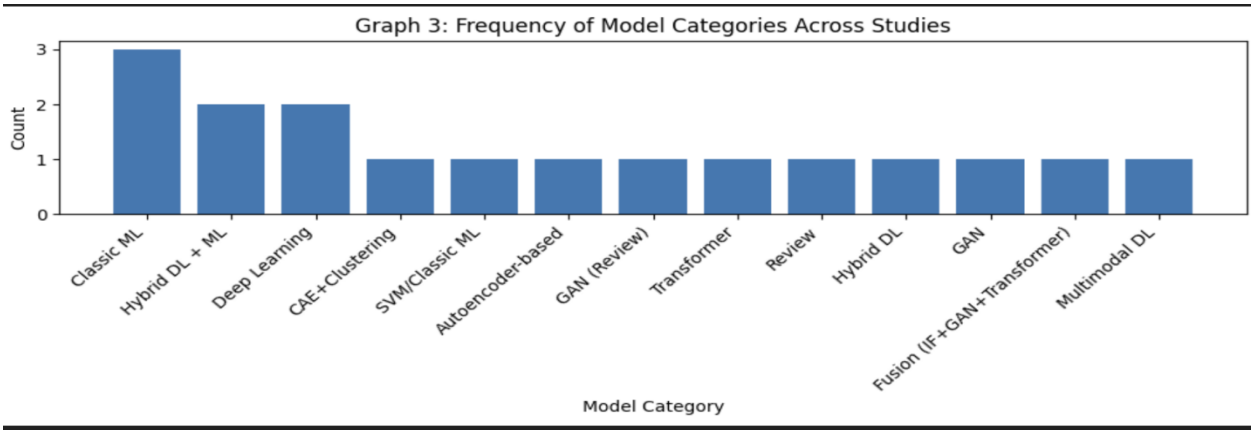

Figure 3. Frequency of Model Categories Across Studies

Figure 3 illustrates the frequency of different model categories used across the reviewed studies. The results show that **classic machine learning approaches** (such as SVM, Gradient Boosting, Random Forest) and **hybrid deep learning + ML models** appear most frequently, reflecting their wide adoption due to strong accuracy and computational efficiency. Deep learning techniques like CNNs, LSTMs, and autoencoder-based models also appear prominently, confirming their importance in learning complex patterns in cyber data. Additionally, emerging techniques such as **GAN-based anomaly detection**, **Transformers**, and fusion models (Isolation Forest + GAN + Transformer) demonstrate increasing popularity, signifying a shift toward more advanced and data-generative approaches to address data imbalance and evolving attack behaviors.

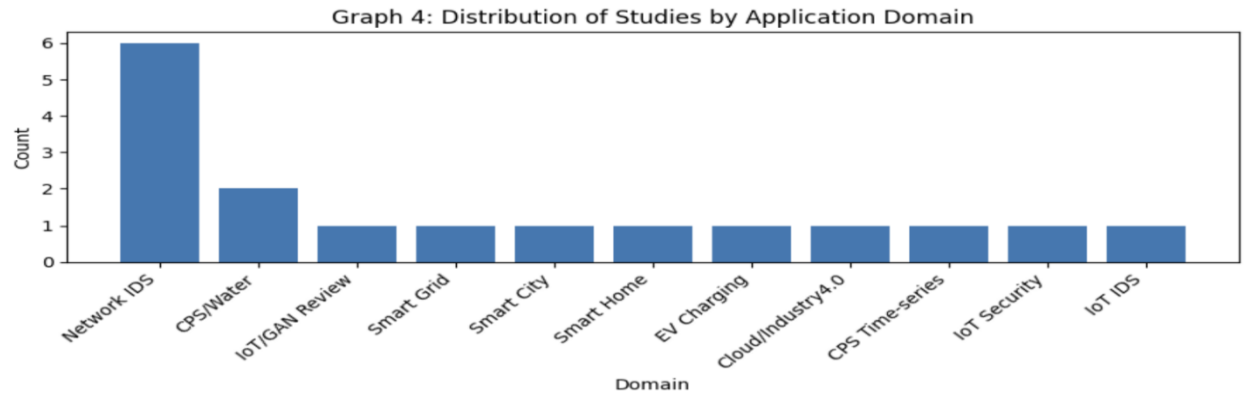

Figure 4. Distribution of Studies by Application Domain

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 4 provides a domain-wise distribution of the reviewed studies, showing where anomaly detection research is most actively applied. The figure indicates that **network intrusion detection (Network IDS)** dominates the literature, suggesting strong focus on network-level anomaly analysis. CPS and Water distribution systems also appear repeatedly, highlighting the importance of securing cyber-physical infrastructure. Other domains such as smart homes, smart grids, EV charging infrastructure, cloud environments, Industry 4.0 systems, and smart cities are represented but less frequently. This shows that although anomaly detection research is expanding into new domains, network IDS remains the most widely explored application area, while emerging domains still require deeper research and more standardized datasets.

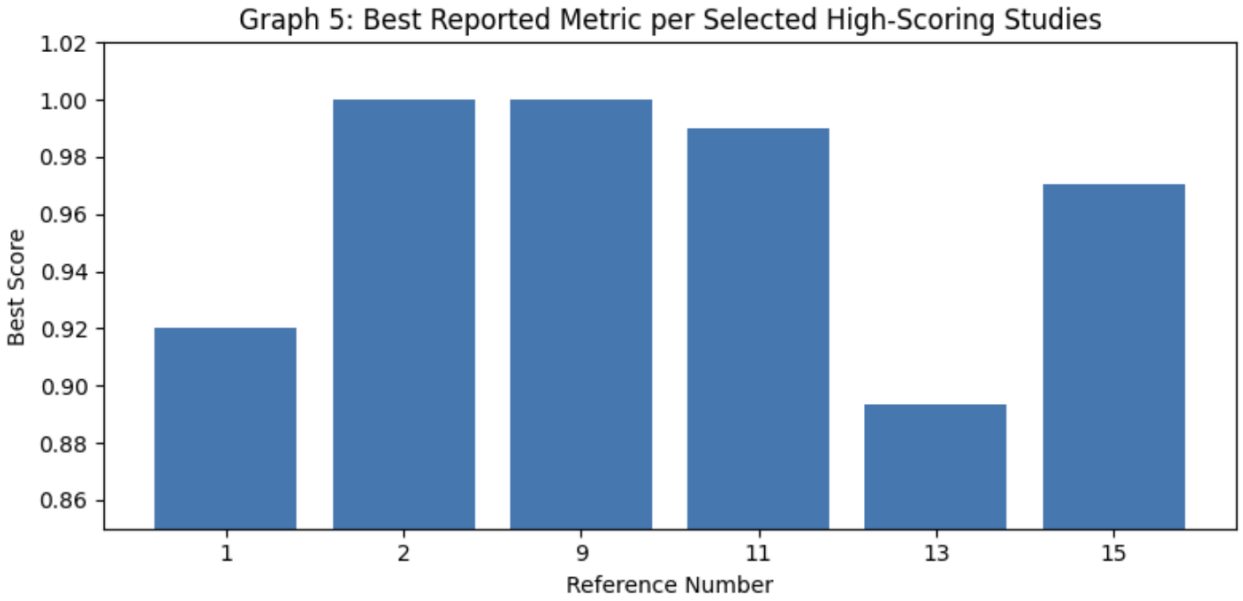

Figure 5. Best Reported Metric per Selected High-Scoring Studies

Figure 5 compares the best-reported performance metrics for selected high-performing studies, highlighting the most successful approaches in the review. The graph reveals that studies based on **Vision Transformers (Ref [9])** and hybrid CPS detection strategies (Ref [2]) achieved near-perfect performance (score = 1.0), reflecting the strong learning capability of deep transformer models and multi-level anomaly strategies. Ref [11] also performed exceptionally well with a Decision Tree model (accuracy = 0.99), suggesting that even simpler models can perform strongly in structured environments like SCADA testbeds. Meanwhile, Ref [13] shows relatively lower precision compared to others, implying that IoT anomaly detection still faces challenges such as noise, adversarial behavior, and diverse traffic patterns. Overall, this graph highlights that state-of-the-art models provide high accuracy but future research should focus on real-world deployment and generalization across environments.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1. Systematic Review

Ref. No.	Author (s)	Year	Title	Methods / Model Used	Results	Advantages	Research Gap	Future Scope
[1]	Aktar & Nur	2024	Advancing Network Anomaly Detection: Ensemble Approach Combining Optimized CAE + K-Means	Contractive Autoencoder + K-Means clustering (ensemble)	**F1 = 0.92** (NSL-KDD), +8.2% vs AE, +5.7% vs K-Means	Strong detection in unsupervised setting; improved clustering performance	Not tested on real-time/high-speed modern traffic; limited multi-class analysis	Extend to real-time IDS deployment; evaluate on modern datasets (CICIDS, IoT)
[2]	Ahmad & Petrovski	2024	Securing CPS with Two-Level Anomaly Detection Strategy	Hybrid CNN-LSTM + Gradient Boosting Machine	F1 = **100% (network)**, **97.3% (physical)** (Water Distribution Testbed)	High accuracy & strong CPS-level precision detection	Requires structured CPS datasets; unclear generalization to other CPS domains	Expand to multi-CPS environments (smart grids, manufacturing); online learning
[3]	Alghushairy et al.	2024	Efficient SVM-based Network Outlier Detection System	Optimized SVM + Gaussian Naive Bayes (NODS)	High accuracy & low false alarm rates (NSL-KDD, CICIDS2017)	Lightweight; suitable for structured anomaly detection	Performance unclear on encrypted traffic or zero-day attacks	Combine with deep learning; real-time deployment + adaptive thresholding
[4]	Gonaygunta et al.	2024	Flexible Deep Learning Model for Enhance	DNN, LSTM, Deep Sparse Autoenco	Demonstrated improved anomaly detection on IoT datasets	DL models handle complex threats;	Lack of interpretability; limited deployment feasibility	Build explainable AI + optimize for edge/low-

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			d Anomaly Detection	der		scalable	analysis	power devices
[5]	Harrou et al.	2024	Autoencoder-Based Anomaly Detection in Power Grids	Hybrid deep learning model (GRU-based stacked autoencoder + anomaly detection algorithms)	Outperformed standalone methods (IEC 60870-5-104 dataset)	Specialized for smart grid cyber defense; strong accuracy	Dataset dependency and limited attack variety	Broader smart grid datasets; hybrid defense + response automation
[6]	Hooshmand & Hosahalli	2022	Network Anomaly Detection Using Deep Learning Techniques	DNN + LSTM + Deep Sparse Autoencoder (review + method)	Outperformed traditional approaches	Comprehensive DL comparison; effective against sophisticated attacks	Older datasets may not represent modern attack behaviors	Apply on new datasets + benchmark transformers for anomaly detection
[7]	Lim et al.	2024	Future of GANs for Anomaly Detection: Review	Review of GAN-based anomaly detection	GANs effective for representation learning, data augmentation	Solves scarcity of rare attack data	Limited practical deployment frameworks	Create standardized GAN-IDS frameworks; evaluate stability + robustness
[8]	Rejito et al.	2024	ML-Based Anomaly Detection for Smart Home Networks Under Adversar	ML-based classification using traffic features	High accuracy under adversarial attacks	Strong relevance to smart homes; adversarial-aware	Doesn't address distributed or federated learning for privacy	Extend to federated learning + adversarial defense strategies

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			ial Attack					
[9]	Sana et al.	2024	Enhancing Intrusion Anomaly Detection with Vision Transformers	Optimized ML/DL IDS + Vision Transformer (ViT)	**100% accuracy, precision, AUC** (ViT)	Extremely high performance; transformer-based learning strong	Risk of overfitting; unclear compute cost & real-time feasibility	Lightweight ViT models for edge; validate across noisy/real traffic
[10]	Shamshari & Najaf	2024	ML Approaches for Anomaly Detection in Network Security	Review: supervised, unsupervised, ensemble, hybrid ML methods	Highlights ML improves accuracy and robustness	Broad classification of ML approaches	No comparative benchmark framework or dataset standards	Benchmark framework + standardized evaluation metrics across IDS datasets
[11]	Söğüt & Erdem	2023	Multi-model Proposal for Classification & Detection of DDoS on SCADA	Testbed SCADA water plant + ML models + hybrid DL	**DT=99%**, Hybrid DL=95%	SCADA-specific resilience evaluation; real testbed simulation	Limited to DDoS; no zero-day or stealthy attacks	Extend to ransomware, spoofing, insider attacks; real industrial deployment
[12]	Sun et al.	2024	MTS-DVGAN: Dual Variational GAN for CPS Anomaly Detection	Unsupervised Dual Variational GAN (MST-DVGAN)	Improved detection on SWaT, WADI, NSL-KDD	Strong multivariate time-series learning	GAN training instability + complexity	Stable GAN architectures + integration with Transformers for CPS
[13]	Tahir et al.	2024	Enhancing IoT Security	Random Forest, Gradient Boosting	Best: Gradient Boosting	Balanced security + defense	Limited exploration of deep	Hybrid ML+DL IDS;

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

			Using ML-Driven Anomaly Detection	Boosting, adaptive defense	precision **89.34%**	mechanism integration	learning and IoT traffic variability	transfer learning across device types
[14]	Usanova et al.	2024	ML for Anomaly Detection in EV Charging Networks	ML anomaly detection on charging logs	High detection accuracy; proactive maintenance support	Useful for real-world EV infrastructure	Limited adversarial/ attack scenario testing	Integrate with smart grid security; add cyberattack simulations
[15]	Vibhute & Nakum	2024	DL-Based Detection in Imbalanced Cloud Environment	Deep CNN + Random Forest feature selection	Accuracy **97.07%**, high precision/recall/F1 (CSE-CIC-IDS2018)	Strong for Industry 4.0 real-time security	No resource footprint analysis for cloud-scale streaming	Deploy optimized architecture; integrate streaming analytics (Kafka/Flink)
[16]	Wang et al.	2024	DL-Based Anomaly Detection & Log Analysis for Networks	Fusion model: Isolation Forest + GAN + Transformer	Improved accuracy, reduced false alarms	Unique log + network fusion; time-series modeling	Mostly experimental; production feasibility unclear	Real-time SOC integration; deployment-ready frameworks
[17]	Yao et al.	2024	Smart City Security Monitoring in Beijing Using Multimodal Data	Multimodal NN + transfer learning + GAN + edge computing	High accuracy; fast response; detects crowding & suspicious objects	Strong edge deployment; real-time monitoring	Limited discussion on privacy, scalability, and bias	Privacy-preserving AI + multi-city scalability + fairness evaluation
[1	Ali, Chong,	2023	Machine Learning	ML & DL techniqu	Achieved accuracy	Covers modern	Heavy reliance on	Hybrid ML-DL

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

8]	Manickam et al.		Techniques to Detect a DDoS Attack in SDN: A Systematic Review	es (CNN, LSTM, GRU, AE-SVM), SDN-based analysis	>99% on datasets like CICIDS2017 and CICDDoS2019 (MDPI)	datasets, preprocessing, evaluation metrics; strong performance comparison	benchmark datasets; limited real-world deployment; scalability issues	models, real-time SDN integration, improved scalability and efficiency
[19]	Mittal, Kumar, Behal et al.	2022	Deep Learning Approaches for Detecting DDoS Attacks (Systematic Review)	Systematic Literature Review (SLR), Deep Learning models (CNN, RNN, LSTM, DNN)	High detection accuracy, reduced false alarm rates	Comprehensive taxonomy of DL techniques; comparison of datasets, models, and metrics	Lack of real-time implementation; limited handling of evolving attacks; dataset dependency	Develop real-time IDS, adaptive learning models, and lightweight DL models for IoT environments
[20]	Makkawi et al.	2021	Intrusion Detection / DDoS Detection using ML/DL (IEEE Xplore ID: 9429678)	Machine Learning / Deep Learning (e.g., CNN, SVM, ANN-based IDS)	Improved intrusion detection accuracy and classification performance	Effective detection of known and unknown attacks; adaptable ML-based IDS	High computational cost; difficulty in detecting zero-day attacks; imbalance in datasets	Focus on lightweight IDS, edge-based detection, and better handling of unknown attacks

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[21]	Alahmadi et al.	2023	DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions	ML (RF, SVM, KNN), DL	High detection accuracy across datasets	Comprehensive survey + taxonomy	Lack of real-time deployment	Real-time IDS in IoT with lightweight ML
[22]	Mittal et al.	2022/2023	Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review	CNN, RNN, LSTM	DL models outperform traditional ML	Strong feature learning	High computational complexity	Efficient DL models for edge/IoT
[23]	Ali, Tariq et al.	2023	Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review	ML + SDN-based IDS	Improved detection in SDN environments	Integration with SDN improves control	Limited scalability testing	Scalable SDN-based IDS with AI

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[24]	Aslam et al.	2023	ONOS DDoS Defender: A Comparative Analysis of Existing DDoS Attack Datasets using Ensemble Approach	Ensemble ML (RF, SVM, KNN, LSTM)	Improved classification accuracy across datasets	Multi-dataset evaluation improves reliability	Limited real-time deployment	Real-time SDN-based DDoS defense systems
[25]	Singh et al.	2023	A Novel DDoS Detection and Mitigation Technique Using Hybrid Machine Learning Model in SDN Network	Hybrid ML + SDN + Traffic Redirection	Efficient detection and mitigation of DDoS attacks	Combines detection + mitigation	Scalability and large-scale testing issues	Scalable AI-driven SDN security frameworks

3. Research gap

1. Lack of Real-World Deployment and Industrial Validation : Although many studies report very high accuracy and F1-scores (e.g., SCADA DDoS detection, CPS water testbeds, IoT IDS using Vision Transformers), most evaluations are conducted under **controlled lab environments**, simulation testbeds, or offline datasets such as NSL-KDD, SWaT, WADI, and CICIDS. Very few studies provide evidence of successful deployment in real industrial SCADA/CPS systems where network traffic, device behavior, and attack patterns evolve dynamically. This creates a gap between academic performance and practical usability in operational environments such as smart grids, industrial plants, and public infrastructure monitoring.

2. Limited Generalization Across Datasets and Domains : A repeated gap across the reviewed literature is the weak focus on **cross-domain generalization**. Many approaches perform strongly only on specific datasets or domains (e.g., SCADA DDoS testbed, Water Distribution CPS data, IoT datasets),

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

but they are rarely validated on multiple heterogeneous datasets. Since anomaly detection models often suffer from domain shift, the real challenge is ensuring that a model trained on one environment can adapt to other environments with different traffic distributions, device types, or operational behavior. This becomes more critical as anomaly detection expands to mixed domains such as cloud + IoT + CPS interconnections.

3. Over-Reliance on Outdated or Benchmark Datasets : Several studies still use well-known datasets like **NSL-KDD**, which are widely criticized for being outdated and not reflective of modern attacks such as ransomware, advanced persistent threats (APT), insider threats, encrypted attacks, or stealthy low-rate anomalies. While newer datasets like CICIDS2017/2018 and UNSW-NB15 appear in some works, they are still limited in representing real industrial traffic. This indicates a major gap in the availability and adoption of **modern, high-fidelity datasets**representing real-world threats, particularly for SCADA, IoT smart homes, EV charging systems, and smart city surveillance networks.

4. Insufficient Focus on Zero-Day, Stealthy, and Multi-Stage Attacks : Most reviewed approaches detect known anomalies effectively, but few studies explicitly address **zero-day attacks**, stealthy anomalies, or multi-stage intrusion chains. SCADA-focused work is largely limited to DDoS scenarios, while IoT and CPS works are often validated using predefined anomalies rather than unpredictable evolving threats. This highlights the need for models capable of learning robust behavioral patterns and detecting anomalies that do not resemble previously seen attack signatures.

5. Data Imbalance and Scarcity Still Remain a Bottleneck : The anomaly detection field continues to suffer from **rare-event scarcity**, where abnormal events occur far less frequently than normal traffic. GAN-based approaches attempt to solve this by generating synthetic data; however, many GAN solutions remain theoretical or experimental, with limited discussion on training instability, mode collapse, or realism of generated anomalies. Thus, while synthetic generation is promising, there is still a significant gap in reliable, stable, and validated GAN pipelines for cybersecurity datasets, particularly for CPS multivariate time-series data.

6. High Computational Cost and Lack of Lightweight Models for Edge/Real-Time Use : Several high-performing approaches (Transformers, hybrid fusion models, deep CNN-LSTM structures, GAN + Transformer pipelines) are computationally heavy and may not be feasible for deployment in **resource-constrained environments**, especially IoT devices, edge nodes, smart meters, and smart home gateways. Only limited work considers latency, memory, and energy constraints. Therefore, a major gap exists in developing **lightweight, real-time anomaly detection models** that maintain high accuracy while being suitable for industrial edge deployment.

7. Absence of Explainability and Trust in AI-Based Security Systems : Many machine learning and deep learning approaches report excellent detection performance but provide limited explainability. In critical infrastructures like SCADA and CPS, stakeholders need to know **why an anomaly is flagged**, what features contributed, and what the response should be. Yet, explainable anomaly detection remains underexplored, and few studies propose interpretable models or explainable post-analysis techniques. This reduces trust, limits adoption, and makes auditability difficult, particularly in high-stakes environments.

8. Limited Integration with Automated Response and Defense Mechanisms : Most reviewed studies focus primarily on detection accuracy but provide minimal research on how detection outputs integrate with **automated defense, mitigation, or incident response systems**. Only a few works touch adaptive defense mechanisms. In real scenarios, anomaly detection is only useful if it triggers

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

effective countermeasures, alert prioritization, or remediation workflows. The gap lies in developing **end-to-end anomaly detection + response frameworks**, especially for IoT and CPS systems where response must be rapid and coordinated.

4. Existing methodology

The existing methodologies for anomaly detection and cybersecurity across SCADA systems, cyber-physical systems (CPS), IoT environments, smart grids, cloud infrastructures, and smart city surveillance primarily rely on machine learning (ML), deep learning (DL), hybrid modeling, and data augmentation approaches. These methodologies aim to detect abnormal events such as DDoS attacks, intrusions, network outliers, traffic irregularities, and suspicious physical activities by learning patterns from network traffic logs, multivariate time-series sensor data, or multimodal surveillance inputs. Researchers have adopted both traditional and advanced AI techniques, evaluated on benchmark datasets such as NSL-KDD, CICIDS2017/2018, UNSW-NB15, SWaT, WADI, IEC 60870-5-104, and water distribution testbeds, achieving high detection performance in many cases. The following subsections summarize the key existing methodologies used in the reviewed studies.

1. Traditional Machine Learning–Based Anomaly Detection : A large portion of existing research uses supervised and classical machine learning models due to their simplicity, interpretability, and lower computational demands. Common algorithms include **Support Vector Machines (SVM)**, **Naive Bayes**, **Random Forest**, and **Gradient Boosting**. These methods extract statistical or engineered features from network logs or traffic records and classify activities as normal or anomalous. For example, optimized SVM-based outlier detection systems and ensemble-based ML classifiers are employed to achieve high accuracy with reduced false alarms in network intrusion detection contexts. Additionally, Gradient Boosting and Random Forest models are frequently evaluated as robust detectors in IoT security settings. Such ML approaches are particularly effective when the dataset is structured and labeled, but their performance tends to degrade against complex, evolving, and zero-day attacks.

2. Deep Learning–Based Anomaly Detection : Deep learning techniques are widely used in existing work to capture complex patterns in sequential and high-dimensional data. Models such as **Deep Neural Networks (DNNs)**, **Convolutional Neural Networks (CNNs)**, **Long Short-Term Memory (LSTM)** networks, and **Autoencoders** are commonly adopted. CNN-based approaches are used for traffic classification and anomaly detection by transforming network data into structured representations and learning spatial features. LSTM networks and recurrent architectures capture time-dependent behaviors, making them suitable for CPS and IoT anomaly detection. Autoencoders, particularly sparse and contractive variants, are applied for learning compressed representations of normal traffic patterns, where reconstruction errors are used to flag anomalies. Many studies show that DL-based techniques outperform traditional ML methods on benchmark datasets; however, they often demand higher computation, extensive training data, and careful tuning.

3. Hybrid Deep Learning + Machine Learning Approaches : Hybrid models represent a dominant trend in the existing methodology, combining deep learning feature extraction with machine learning classifiers for decision-making. In this approach, deep learning models such as stacked autoencoders, CNN-LSTM architectures, or GRU-based encoders first learn abstract representations of traffic or sensor signals. These learned features are then passed to machine learning classifiers such as Gradient Boosting or anomaly detection algorithms to improve final accuracy. This strategy is widely applied in CPS and industrial networks because it leverages deep representation learning while

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

maintaining strong classification effectiveness. For example, two-level anomaly detection strategies use CNN-LSTM models for initial anomaly detection and a secondary classifier for precise anomaly categorization. Hybrid deep learning models are also used in smart grid cybersecurity by combining GRU-stacked autoencoders with additional anomaly detection techniques. Such methodologies show strong performance but remain dependent on dataset quality and require careful integration design.

4. GAN-Based and Synthetic Data Generation Methodologies : To overcome the challenge of anomaly data scarcity, researchers increasingly employ **Generative Adversarial Networks (GANs)**. GAN-based methodologies generate synthetic anomaly samples or learn more robust feature representations by modeling normal vs abnormal distributions. This is particularly useful in intrusion detection contexts where real attack traffic is rare or imbalanced. Variants such as dual variational GANs are applied for CPS anomaly detection in multivariate time-series datasets like SWaT and WADI. GANs are also integrated into hybrid pipelines where generated synthetic traffic improves model training and reduces false alarms. In many cases, GANs enhance anomaly detection sensitivity, but their reliability depends on stable training and realistic sample generation. Therefore, GAN-based methodology remains promising but still evolving.

5. Transformer and Attention-Based Anomaly Detection : Recent studies increasingly adopt transformer-based architectures because of their ability to capture long-range dependencies and complex temporal relationships. Vision Transformers (ViT) and time-series transformers have been explored for intrusion and anomaly detection. Transformer models analyze network traffic patterns and log sequences effectively, and in some reported cases they achieve extremely high performance. Additionally, transformers are combined with GAN and Isolation Forest in fusion systems for anomaly detection and log analysis, where each component provides complementary strengths: Isolation Forest detects deviations, GAN addresses data imbalance, and Transformers handle temporal sequence modeling. Transformer-based methodologies are considered state-of-the-art but may require optimization for real-time deployment due to their computational cost.

6. Domain-Specific Methodologies (SCADA and CPS Testbeds) : Several studies propose methodologies specifically tailored to SCADA and CPS environments due to their unique constraints and criticality. SCADA-specific research often involves controlled testbeds simulating industrial plants such as water distribution systems, where multiple attack scenarios (e.g., DDoS) are injected to evaluate detection resilience. CPS methodology typically uses multivariate sensor measurements and network communications together, combining network anomaly detection and physical anomaly detection frameworks. Two-level CPS models classify anomalies at a broad level first and then apply refined classifiers for precise detection. These domain-specific methodologies show strong results but often remain limited to specific scenarios and testbed environments.

7. Multimodal AI-Based Surveillance Methodologies (Smart City Security) : In smart city security monitoring, anomaly detection methodology expands beyond network logs to include multimodal data sources such as **video, audio, and thermal sensors**. Neural networks are combined with edge computing for real-time surveillance tasks like overcrowding detection, unauthorized access detection, and unattended object recognition. Transfer learning enhances adaptability across environments, while GAN-based techniques improve robustness and generalization. These systems demonstrate rapid response capabilities and high detection accuracy, but they introduce new requirements around privacy preservation, scalability, and fairness.

Journal of Information Systems Engineering and Management
2024, 9(4s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Conclusion and Future Scope

5.1 Conclusion: This systematic review shows that anomaly detection for SCADA, CPS, IoT, cloud, and smart city systems particularly for threats such as DDoS (Distributed Denial of Service) attacks has rapidly advanced, with most studies published in 2024, reflecting growing cybersecurity urgency. Traditional machine learning methods such as SVM, Random Forest, and Gradient Boosting remain widely used due to their efficiency and low false-alarm rates, while deep learning models (CNN, LSTM, Autoencoders) improve detection of complex patterns in high-dimensional and time-series data, including DDoS traffic behavior. Hybrid approaches combining deep feature extraction with ML classifiers demonstrate strong robustness, especially in CPS, IoT, and smart grid datasets under DDoS and other intrusion scenarios. Recent trends highlight GANs for addressing data imbalance and Transformers/Vision Transformers for superior accuracy, sometimes reaching near-perfect performance in detecting anomalies and DDoS patterns. However, results are largely based on benchmark datasets and testbeds, meaning real-world deployment readiness, generalization, explainability, and scalability are still limited.

5.2 Future Scope: Future work should focus on real-time deployment in operational SCADA, CPS, and IoT environments, with effective detection and mitigation of DDoS (Distributed Denial of Service) attacks, along with other encrypted, stealthy, and zero-day cyber threats. Evaluation should be carried out on modern benchmark datasets as well as live network traffic to ensure better generalization and real-world applicability. Lightweight, edge-friendly Transformer and hybrid models are needed for low-latency monitoring in smart homes, industrial networks, and cloud-connected IoT systems. Stable GAN-based pipelines should be developed for realistic synthetic generation of anomaly and DDoS traffic, particularly for multivariate CPS time-series data. Additionally, explainable AI methods must be integrated to improve trust, interpretability, and decision support, while privacy-preserving learning remains essential for secure deployment in smart city surveillance and distributed IoT ecosystems.

Reference

[1] Aktar, S. and Nur, A.Y. Advancing Network Anomaly Detection: An Ensemble Approach Combining Optimized Contractive Autoencoders and K-Means Clustering. *2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*, 2024, pp. 1-5. IEEE.

[2] Ahmad, Z. and Petrovski, A. Securing Cyber-Physical Systems with Two-level Anomaly Detection Strategy. *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*, 2024, pp. 1-6. IEEE.

[3] Alghushairy, O., Alsini, R., Alhassan, Z., Alshdadi, A.A., Banjar, A., Yafoz, A. and Ma, X. An Efficient Support Vector Machine Algorithm based Network Outlier Detection System. *IEEE Access*, 2024.

[4] Gonaygunta, H., Nadella, G.S., Pawar, P.P. and Kumar, D. Enhancing Cybersecurity: The Development of a Flexible Deep Learning Model for Enhanced Anomaly Detection. *2024 Systems and Information Engineering Design Symposium (SIEDS)*, 2024, pp. 79-84. IEEE.

[5] Harrou, F., Bouyeddou, B., Dairi, A. and Sun, Y. Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids. *Future Internet*, 16(6), 2024, p.184.

[6] Hooshmand, M.K. and Hosahalli, D. Network anomaly detection using deep learning techniques. *CAAI Transactions on Intelligence Technology*, 7(2), 2022, pp. 228-243.

[7] Lim, W., Chek, K.Y.S., Theng, L.B. and Lin, C.T.C. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security*, 139, 2024, p.103570.

[8] Rejito, J., Stiawan, D., Alshaflut, A. and Budiarto, R. Machine learning-based anomaly detection for smart

home networks under adversarial attack. *Computer Science and Information Technologies*, 5(2), 2024, pp. 122-129.

[9] Sana, L., Nazir, M.M., Yang, J., Hussain, L., Chen, Y.L., Ku, C.S., Alatiyyah, M. and Por, L.Y. Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection with Vision Transformers. *IEEE Access*, 2024.

[10] Shamshari, A. and Najaf, H. Machine Learning Approaches for Anomaly Detection in Network Security. *Eastern European Journal for Multidisciplinary Research*, 1(1), 2024, pp. 22-29.

[11] Söğüt, E. and Erdem, O.A. A multi-model proposal for classification and detection of DDoS attacks on SCADA systems. *Applied Sciences*, 13(10), 2023, p.5993.

[12] Sun, H., Huang, Y., Han, L., Fu, C., Liu, H. and Long, X. MTS-DVGAN: Anomaly detection in cyber-physical systems using a dual variational generative adversarial network. *Computers & Security*, 139, 2024, p.103570.

[13] Tahir, U., Abid, M.K., Fuzail, M. and Aslam, N. Enhancing IoT Security through Machine Learning-Driven Anomaly Detection. *VFAST Transactions on Software Engineering*, 12(2), 2024, pp. 01-13.

[14] Usanova, K.I., Rani, G.S., Mishra, N., Kaur, S. and Sidhu, J. Machine Learning for Anomaly Detection in Electric Transportation Networks. *E3S Web of Conferences*, Vol. 511, 2024, p. 01039. EDP Sciences.

[15] Vibhute, A.D. and Nakum, V. Deep learning-based network anomaly detection and classification in an imbalanced cloud environment. *Procedia Computer Science*, 232, 2024, pp. 1636-1645.

[16] Wang, S., Jiang, R., Wang, Z. and Zhou, Y. Deep Learning-based Anomaly Detection and Log Analysis for Computer Networks. *arXiv preprint arXiv:2407.05639*, 2024.

[17] Yao, Y. Neural Network-Driven Smart City Security Monitoring in Beijing Multimodal Data Integration and Real-Time Anomaly Detection. *International Journal of Computer Science and Information Technology*, 3(3), 2024, pp. 91-102.

[18] Ali, A., Chong, Y.W., Manickam, S. and others. Machine Learning Techniques to Detect DDoS Attacks in Software-Defined Networking: A Systematic Review. *Applied Sciences*, 2023.

[19] Mittal, M., Kumar, K. and Behal, S. Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review. Soft Computing, 2022.

[20] A. M. Makkawi and A. Yousif, "Machine Learning for Cloud DDoS Attack Detection: A Systematic Review," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2021, pp. 1-9.

[21] Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., Alotaibi, O. B., & Bajandouh, S. A. (2023). DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. Electronics, 12(14), 3103. MDPI.

[22] Mittal, M., Kumar, K., & Behal, S. (2023). Deep Learning Approaches for Detecting DDoS Attacks: A Systematic Review. Soft Computing, 27(18), 13039–13075. Springer.

[23] Ali, Tariq Emad, Yung-Wey Chong, and Selvakumar Manickam. 2023. "Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review" Applied Sciences 13, no. 5: 3183.

[24] Aslam, N., Srivastava, S., & Gore, M. M. (2023). ONOS DDoS Defender: A Comparative Analysis of Existing DDoS Attack Datasets using Ensemble Approach. Wireless Personal Communications. Springer.

[25] Singh, A., Kaur, H., & Kaur, N. (2023). A Novel DDoS Detection and Mitigation Technique Using Hybrid Machine Learning Model and Redirect Illegitimate Traffic in SDN Network. Cluster Computing. Springer.