Volume 19, Issue 2, 192526 (1-12)

Majlesi Journal of Electrical Engineering (MJEE)

https://doi.org/10.57647/j.mjee.2025.1902.26

Advances in network security and new anomaly detection techniques

Sajad Balali Dehkordi[1], Saeed Nasri[1,2,*], Sina Dami[3]

[1]*Department of Electrical Engineering, Na.C., Islamic Azad University, Najafabad, Iran.*
[2]*Digital Processing and Machine Vision Research Center, Na.C., Islamic Azad University, Najafabad, Iran.*
[3]*Department of Computer Engineering, WT.C., Islamic Azad University, Tehran, Iran.*

[*]**Corresponding author:** saeed.nasri@iau.ac.ir

Review Paper

Received:
2 February 2025
Revised:
31 March 2025
Accepted:
27 April 2025
Published online:
1 June 2025

Abstract:

Anomaly detection in diverse domains is confronted with the challenges posed by the increasing volume, velocity, and complexity of data. This paper presents a comprehensive review of recent advancements and research trends in anomaly detection across various domains, including high-dimensional big data, sensor systems, information and communication technology, IoT data, energy consumption, and real-time networks amidst cyber-attacks. Through a systematic analysis of recent literature, this review synthesizes key findings, methodologies, and challenges, providing insights into current strategies and future directions for anomaly detection technology. The reviewed papers highlight the importance of addressing domain-specific challenges, fostering interdisciplinary collaboration, and advancing methodological innovation to develop robust, scalable, and effective anomaly detection solutions capable of meeting the evolving demands of today's data-driven world.

Keywords: Anomaly detection; Network security; IoT; Energy consumption

1. Introduction

Network security is crucial in protecting data integrity, confidentiality, and availability. As cyber threats become more sophisticated, traditional anomaly detection methods face challenges in identifying anomalies effectively [1]. These approaches generally depend on pre-established rules and signatures, which may not effectively adjust to novel or developing threats. Precious data continually attracts the focus of enemies and is therefore susceptible to significant network penetration. Intrusion entails the deliberate action of an adversary transmitting malevolent packets to a host system or compromising a network with the intention of pilfering or modifying confidential data. Intrusion Detection Systems (IDS) are commonly classified into two basic categories: Signature IDS and Anomaly IDS. Signature-based intrusion detection systems rely on the comparison of incoming data with pre-established signatures of known assaults stored in a database [1]. Nevertheless, these systems lack the capability to detect novel or unknown attacks. Anomaly-based IDS employ a statistical approach to detect actions that deviate from the regular thresholds of resource utilization and typical behavioral patterns. Anomaly-based identification continues to exhibit a high proportion of both false positives and false negatives [2].

In 1986, Dorothy E. Denning and her colleagues developed the first IDS as part of their work at SRI International [3]. Subsequently, IDS emerged as a prominent subject of investigation within the scientific community. In 2011, S. J. Horng and colleagues [4] introduced an IDS model that included a hierarchical clustering technique to select attributes and a Support Vector Machines (SVM) classifier for classification. Subsequently, the model underwent testing using the KDDcup 99 dataset. In 2012, S. Mukherjee and colleagues introduced a technique called Feature Vitality-based Reduction for evaluating attribute subsets. This approach utilizes information gain, gain ratio, and correlation-based feature selection. The system was tested using a Naïve Bayes classifier. In 2013, R. M. Elbasiony developed a hybrid strategy that combines Random Forest and weighted k-means classifiers. This approach was then evaluated using KDDcup99 data. In 2015, E. D. L. Hoz and colleagues [5] used Principal Component Analysis (PCA) and Fisher

Discriminant Ratio to pick attributes and reduce noise. In addition, it used Probabilistic Self-Organizing Maps to construct a model and identify abnormalities. In 2016, Rajni Devi and her colleagues used K-NN and NN classifiers to accurately respond to queries posed in the Hindi language. The research was conducted using diverse datasets. In 2017, Thaseen et al. [6] used a chi-square attribute evaluator to the NSL-KDD dataset and developed a model that utilized Multi-class SVMs.

The rapid exploitation of recently discovered vulnerabilities through zero-day attacks presents significant and perhaps devastating risks to network security. Researchers have devised a variety of network security measures, including firewalls, IDSs, honeypots, and other advanced technologies. An IDS is a widely used proactive defensive technique in the field of network security. The primary objective of this system is to identify and detect any unwanted access and assaults occurring in various network environments. Implementing this strategy is a highly efficient method to improve network security in modern communication networks, ensuring the safeguarding of users' data and privacy. In the field of IDSs, there are two primary categories: misuse-based IDSs and anomaly-based IDSs. Misuse-based IDSs utilize the signatures of established attacks to identify and detect any unauthorized endeavors to gain access to a network. Conventional IDSs, which rely on identifying malicious behavior, have inherent limitations. These techniques lack the ability to adapt to different application circumstances and have a limited capacity to detect previously unseen threats, leading to a high percentage of inaccurate negative identifications [7].

Anomaly-based IDSs have the capability to identify and detect novel forms of assaults, but they are prone to a significant number of false positives. Recently, there has been a significant emphasis on machine learning techniques for detecting anomalies. These methods have been shown to be effective and intelligent in detecting network intrusions [8]. This study investigates the utilization of machine learning techniques for identifying irregularities in network data. Using network data to identify network attacks holds potential, as attackers frequently launch attacks using network connections. Detecting anomalies in network traffic is crucial for identifying network intrusions. The main goal of anomaly detection in network data is to achieve maximum precision while minimizing the rates of false positives and false negatives. This paper focuses on the problem of identifying anomalies in network data, with a particular emphasis on solutions that use classification techniques. The topic is essentially addressed as a binary classification problem. Network traffic data is categorized as either normal or abnormal. Artificial neural networks are a type of supervised machine learning techniques [9], support vector machine [10], decision tree [11], and naive Bayes [12] models, are often used for detecting aberrant network traffic. In addition, ensemble learning models, such as random forest [13] and Gradient Boosted Decision Tree (GBDT) [14], have been introduced because of their higher results in comparison to single classifiers. In the context of real detection problems, accurately labeling a large amount of traffic data might be challenging. Therefore, unsupervised detection models have been introduced. Therefore, unsupervised detection models have been introduced. Feature extraction often involves the use of Restricted Boltzmann Machine (RBM) and other unsupervised models, such as those described by [15]. Traffic data is usually classified by employing a blend of supervised and unstructured models. The detection models consist of three standard phases that form the core process. The initial phase is the data transformation process, in which the raw traffic data is turned into mathematical vectors. Moreover, a separate machine learning model is trained to serve as the traffic classifier, utilizing the obtained vectors as input. Subsequently, the classifier classifies the unidentified traffic data into two categories: normal or anomalous.

This systematic study seeks to provide a methodical analysis of the novel anomaly detection strategies described in recent research. Through analyzing the ideas presented in this important book, our goal is to clarify how these new strategies may be put into practice and explain the theoretical foundations behind them. This will provide readers with a thorough grasp of how these techniques can enhance network security measures. In addition, this study emphasizes the originality of the methodologies addressed, highlighting their divergence from conventional methods and their connection with modern breakthroughs in machine learning, artificial intelligence, and big data analytics. This inquiry aims to offer cybersecurity professionals and researchers practical insights to efficiently navigate the ever-changing realm of cyber dangers. Ultimately, it seeks to contribute to the continuous improvement of network security protocols.

2. Novel anomaly detection techniques

The primary objective of a network anomaly detection system is to accurately and systematically identify various forms of harmful traffic patterns that may go unnoticed by traditional firewall systems. Creating an effective and robust intrusion detection system involves tackling three fundamental difficulties. The three obstacle are: i) Solving the issue of high dimensionality in input observations. ii) Selecting the suitable machine learning technique that avoids problems like overfitting and underfitting. iii) Determining the appropriate distance measure (or similarity measure) to evaluate the similarity between any two network observations. Feature selection, feature representation, and dimensionality reduction methods have been thoroughly investigated and extensively discussed in numerous research papers focusing on text classification, data fusion, image fusion, medical data classification, and various applications of machine learning and data mining. These approaches have been widely studied and addressed in the field. Feature reduction techniques are used in the literature for the development of IDS [16]. Multiple research are also conducted to determine the optimal selection and implementation of a classifier for constructing an effective network intrusion detection system [17]. The effectiveness of NIDS is directly influenced by the use of distance measurements [18] used by IDS to determine whether an incoming observation is normal or abnormal. Researchers make little effort to develop novel distance functions [18] that may be used by NIDS for effective intrusion and anomaly detection. Recent research, such as CANN [19], CLAPP [20], and UTTAMA [21], have used feature reduction strategies to enhance the accuracy and detection rates of Intrusion Detection Systems (IDS). The distance metric used by CANN is the Euclidean distance function. The CLAPP and UTTAMA methods use membership functions in their learning process. However, these research did not provide new similarity metrics for doing unsupervised feature learning and supervised learning tasks. While CANN [19] has decreased the time required by classifiers, it has not yielded satisfactory detection accuracies for the U2R and R2L classes. For instance, the detection accuracies for the U2R and R2L classes in the context of CANN are almost nonexistent. While CLAPP and UTTAMA have made efforts to enhance the accuracy of detecting U2R and R2L attack classes, their techniques were only focused on the application of membership functions. Essentially, the contribution discussed in our study is primarily driven by the findings of these investigations.

Ullah et al. [22] proposed IDS-INT, an Intrusion Detection System utilizing transformer-based transfer learning to address imbalanced network traffic. By leveraging detailed attack information and semantic feature representation, IDS-INT aimed to effectively identify and categorize network attacks. The integration of SMOTE for data balancing and CNN-LSTM models for attack detection showcases a comprehensive approach to improving network security. Overall, the study presented a promising methodology for enhancing intrusion detection systems in complex network environments. Wu et al. [23] proposed a Robust Transformer-based Intrusion Detection System (RTIDS) that reconstructed feature representations to address challenges in cyber security, leveraging positional embedding for sequential feature association and employing self-attention for network traffic classifications. Extensive experiments demonstrated the effectiveness of RTIDS on real traffic datasets, achieving high F1-Scores of 99.17% and 98.48% on CICIDS2017 and CIC-DDoS2019, respectively. A comparative study was conducted, showcasing the superiority of RTIDS over classical and deep learning algorithms like SVM, RNN, FNN, and LSTM in intrusion detection accuracy. Liu et al. [24] introduced an innovative Transformer-based intrusion detection model, addressing challenges of training time, class overlap, and multi-class accuracy. It employed stacked auto-encoder dimension reduction and hybrid sampling (KNN-based undersampling and Borderline-SMOTE) for data balancing, enhancing model performance. Furthermore, the model utilized improved position encoding and a two-stage learning strategy, achieving competitive accuracy (88.7% binary, 84.1% multi-class) and outperforming existing models in speed and effectivenes. Xiang et al. [25] proposed a novel NIDS model using Transformer-based fusion architecture, integrating GAN-Cross for minority class expansion and Transformer modules for enhanced feature encoding. Through experiments with UNSW-NB15 datasets, the model achieved an impressive accuracy of 0.903, showcasing improved detection of complex network attacks and enhanced generalization capabilities. The study's approach effectively addressed imbalanced data issues and contributes to advancing network intrusion detection systems. Dutta et al. [26] presented an intrusion detection mechanism utilizing Deep AutoEncoder and Deep Decoders for unsupervised classification, incorporating various network topology setups for comparison. The efficiency of these topologies was validated on established benchmark datasets (UNSW-NB15 and NetML-2020), analyzing results in terms of classification accuracy, detection rate, false-positive rate, negative predictive value, Matthews correlation coefficient, and F1-score. Additionally, it compared against state-of-the-art methods commonly employed in network intrusion detection. He et al. [27] introduced a new Deformable Vision Transformer (DE-VIT) method for network intrusion detection, demonstrating improved effectiveness with a focus on relevant areas and reduced computational complexity. Experimental simulations on public datasets showed DE-VIT surpassing previous models, achieving 99.5% and 97.5% accuracy on CIC IDS2017 and UNSW-NB15, respectively, marking an 8.5% and 9.1% increase in performance. Jiang et al. [28] proposed the BBO-CFAT model, integrating BBO for feature selection and enhancing the Transformer model to preserve context and reduce computational space. Experimental evaluations showed promising accuracies on CIC-IDS2017 and NSL-KDD datasets, achieving 99.1% and 97.5% accuracy respectively, surpassing comparative experiments. BBO-CFAT addressed critical challenges in intrusion detection, improving feature extraction, computational efficiency, and training accuracy. Long et al. [29] presented a novel NIDS algorithm leveraging Transformer models for cloud environments, promising adaptability to evolving threats and reduced false positives. The design integrated network intrusion detection with Transformer's attention mechanism, enhancing detection accuracy by examining input feature relationships. Experimental results demonstrated over 93% accuracy, comparable to CNN-LSTM models, highlighting the efficacy of this approach for cloud security enhancement. Chen et al. [30] proposed a hybrid deep learning model that aimed to mitigate issues with false-positive and false-negative attacks by addressing imbalanced data through random undersampling and synthetic minority oversampling. Convolutional neural networks (CNNs) were utilized to extract local and spatial features, while a transformer encoder extracted global and temporal features, resulting in increased recognition accuracy compared to existing models. Testing on benchmark datasets showed higher classification accuracy and lower false-positive rates, demonstrating significant improvements in detecting low-frequency attacks. Melícias et al. [31] evaluated the effectiveness of data augmentation techniques, including GPT-based and SMOTE variations, on enhancing intrusion detection models for IIoT networks. The study compared five intrusion detection algorithms trained with augmented datasets against non-augmented ones. Findings demonstrated varied impacts across algorithms, with deep neural networks benefiting from data augmentation while XGBoost showing no performance improvement with synthetic data. The evaluation noted that GPT-based methods like GReaT generated invalid data, leading to performance

degradation in multiclass classification. More related works are also compared in Tables 1- 3 based on the methodology and novelty.
According to Table 2, the studies presented in the table collectively highlight innovative approaches to enhance anomaly detection and security in IoT networks through various machine learning and optimization techniques. For instance, Guo et al. [37] introduce EGNN, which combines a Subgraph Generation Algorithm and graph attention mechanism to achieve both accurate and energy-efficient anomaly detection in IoT multivariate time series data. Their experimental results indicate that EGNN, particularly with Mode Switching (GMS), excels in both accuracy and energy efficiency under conditions of infrequent anomalies. Similarly, Alangari [38] employs an Advanced Hybridized Optimization Technique (AHGFFA) for securing IoT-based sensor

Table 1. Comparision of the related works in the recent years.

No.	References	Aim	Method	Remark
1	(Patcha & Park, 2007) [32]	To provide a comprehensive survey of anomaly detection systems and hybrid intrusion detection systems, highlighting recent technological trends and identifying open problems and challenges in the field.	The paper discusses the growing threat from spammers, attackers, and criminal enterprises in cyberspace and the limitations of current signature-based intrusion detection systems, advocating for anomaly detection systems as a more effective approach. It reviews recent past and present anomaly detection systems and hybrid intrusion detection systems, analyzing technological trends and addressing existing challenges.	Anomaly detection systems are positioned as more effective in detecting both known and unknown attacks compared to signature-based systems, but technological hurdles such as high false alarm rates and scalability issues need to be addressed for widespread adoption.
2	(Ul Islam et al., 2018) [33]	To propose a new belief-rule-based association rule (BRBAR) algorithm capable of handling various uncertainties in sensor data and compare its reliability with existing anomaly detection algorithms using data from domains such as rainfall, temperature, and cancer cells.	The paper addresses the challenge of erroneous sensor data in Internet of Things (IoT) systems and proposes BRBAR as a solution to filter out anomalies before feeding into decision-making systems. The algorithm is evaluated against Gaussian, binary association rule, and fuzzy association rule algorithms using receiver operating characteristic curves with sensor data from different domains.	BRBAR demonstrates superior accuracy and reliability in detecting anomalies in sensor data under uncertainty compared to existing algorithms, enhancing the reliability and accuracy of decision-making systems. Its application in predicting flooding showcases its potential in various domains beyond anomaly detection.
3	(Saeedi Emadi & Mazinani, 2018) [34]	To address anomaly detection in Wireless Sensor Networks (WSNs) by proposing an algorithm that extracts features such as temperature, humidity, and voltage from network traffic, clusters data using the density-based spatial clustering of applications with noise (DBSCAN) algorithm, trains a support vector machine using normal data, and removes anomalies from the network data.	The paper focuses on unsupervised anomaly detection in WSNs and outlines a multi-step approach involving feature extraction, clustering with DBSCAN, analysis of input data accuracy, training of a support vector machine, and removal of anomalies. The proposed algorithm is evaluated using the Intel Berkeley Research Lab (IRLB) dataset.	By leveraging coefficient correlation to address DBSCAN's parameter selection problem, the proposed algorithm offers advantages such as the use of soft computing methods, simple implementation, and improved detection accuracy through simultaneous analysis of temperature, humidity, and voltage features.

Continued of Table 1.

No.	References	Aim	Method	Remark
4	(Agrawal et al., 2022) [35]	To develop a novel deep learning-based Intrusion Detection System (IDS) for Controller Area Network (CAN) protocol in vehicular electronics, addressing vulnerabilities to security attacks and ensuring safety on roads.	The paper introduces a system incorporating thresholding and error reconstruction approaches, utilizing multiple neural network architectures to detect anomalies. It evaluates the system's performance on various attacks-Denial of Service (DoS), Fuzzy, RPM Spoofing, and Gear Spoofing-using Precision, Recall, and F1-Score metrics. Additionally, reconstruction-error distribution plots provide qualitative insights into the system's ability to differentiate between genuine and anomalous sequences.	The proposed IDS offers a novel approach to detecting security attacks in vehicular electronics, leveraging deep learning techniques and evaluation metrics to assess its effectiveness across different attack scenarios. The inclusion of reconstruction-error distribution plots enhances understanding of the system's performance in distinguishing between normal and anomalous behavior.
5	(Sarmadi & Karamodin, 2020) [36]	To propose a novel anomaly detection method, AMSD-kNN, for structural health monitoring (SHM) under varying environmental conditions, addressing limitations of the Mahalanobis-squared distance (MSD) approach such as inappropriate threshold determination and inaccurate covariance matrix estimation.	The article introduces AMSD-kNN, which combines adaptive Mahalanobis-squared distance and one-class kNN rule, utilizing a two-stage procedure to mitigate environmental variability and estimate local covariance matrices. A multivariate normality hypothesis test is employed to identify sufficient nearest neighbors, ensuring well-conditioned covariance matrix estimates. Additionally, the method incorporates generalized extreme value distribution modeling by the block maxima (BM) method for accurate threshold determination, with an optimal block number selected via a Kolmogorov-Smirnov hypothesis test.	AMSD-kNN offers a novel unsupervised learning strategy for SHM, addressing challenges of environmental variability and non-Gaussianity in data. The inclusion of the BM method and goodness-of-fit measure enhances threshold determination accuracy. Comparative studies validate the effectiveness of the proposed methods, demonstrating superior performance in detecting damage under varying environmental conditions.

systems in Mobile Adhoc Networks (MANET), demonstrating significant improvements in mitigating Blackhole and Grayhole attacks through simulations using Network Simulator-3 (NS-3).

Other studies also contribute to the field with diverse methodologies. Altulaihan et al. [39] focus on enhancing security against Denial of Service (DoS) attacks by utilizing various machine learning classifiers and feature selection algorithms, finding that Decision Tree and Random Forest classifiers, when optimized with Genetic Algorithm-selected features, offer the best performance. Inuwa & Das [40] compare multiple machine learning methods for detecting cyber anomalies, concluding that ANN outperform other models. Alsalman [41] presents FusionNet, an ensemble model that combines several algorithms to achieve high accuracy and precision in anomaly detection, while Mishra et al. (2024) [42] propose a weighted stacked ensemble of DCGAN and Bi-LSTM for enhanced classification and security. Tahir et al. [43] emphasize the proactive use of machine learning-based anomaly detection and adaptive defense mechanisms, identifying Gradient Boosting as the most precise model for enhancing IoT security. Together, these studies underscore the significant advancements and potential of machine learning and optimization techniques

Table 2. Comparision of the related works in 2024.

No.	References	Aim	Method	Result
1	(Guo et al., 2024) [37]	To develop an accurate and energy-efficient anomaly detection method (EGNN) for IoT multivariate time series data, focusing on reducing computational heaviness and energy consumption at the network edge.	The study proposes EGNN, which integrates a Subgraph Generation Algorithm (SGA) for exploring correlations between sensory data from IoT devices, utilizing a multi-layer perceptron for anomaly detection on subgraph centers and a graph attention mechanism for accurate anomaly detection when anomalies are detected.	Experimental validation on real-world IoT datasets shows that EGNN with Mode Switching (GMS) outperforms existing methods in terms of both accuracy and energy-efficiency, especially under conditions of infrequent anomalies.
2	(Alangari, 2024) [38]	To enhance security in IoT-based sensor systems, specifically addressing vulnerabilities in Mobile Ad-hoc Networks (MANET), through the implementation of an advanced hybridized optimization technique called AHGFFA.	The study employs Secure Certificate-based Group Formation (SCGF) to organize the network, Recommended Action K-means (K-RF means) Filtering for trust-based recommendation filtering, and an Advanced Hybridized Optimization Technique (AHGFFA) combining Genetic Algorithm (GA) and Firefly Algorithm (FA) for selecting secure routes, all evaluated using Network Simulator-3 (NS-3).	The AHGFFA approach effectively mitigates threats like Blackhole and Grayhole attacks, demonstrating improved performance and security in IoT sensor networks as validated through simulations with NS-3.
3	(Altulaihan et al., 2024) [39]	To develop an Intrusion Detection System (IDS) for IoT networks to enhance security against Denial of Service (DoS) attacks using anomaly detection based on machine learning algorithms.	Employing four supervised classifier algorithms (Decision Tree, Random Forest, K Nearest Neighbor, Support Vector Machine) and two feature selection algorithms (Correlation-based Feature Selection, Genetic Algorithm) to analyze network traffic from the IoTID20 dataset, focusing on detecting anomalous activities indicative of DoS attacks.	The Decision Tree (DT) and Random Forest (RF) classifiers, particularly when trained with features selected by the Genetic Algorithm, demonstrated the best performance in terms of detecting DoS attacks in IoT networks, outperforming other algorithms in metrics such as accuracy and efficiency.
4	(Inuwa & Das, 2024) [40]	Evaluate machine learning methods for detecting cyber anomalies in IoT systems.	Employing SVM, ANN, DT, LR, and k-NN to classify cyber attacks on IoT devices.	ANN demonstrated superior performance compared to SVM, DT, LR, and k-NN in detecting IoT cyber anomalies.
5	(Alsalman, 2024) [41]	Introduce FusionNet, an ensemble model combining Random Forest, K-Nearest Neighbors, Support Vector Machine, and Multi-Layer Perceptron, for improved anomaly detection across various applications.	FusionNet's architecture leverages the strengths of these diverse machine learning algorithms to enhance anomaly detection accuracy and precision, evaluated on Dataset 1 and Dataset 2, and compared against SVM, KNN, and RF.	FusionNet consistently outperforms traditional models (SVM, KNN, RF) in terms of accuracy, precision, recall, and F1 score, achieving 98.5% accuracy on Dataset 1 and 99.5% accuracy on Dataset 2, highlighting its robust performance and potential for real-world applications.

Continued of Table 2.

No.	References	Aim	Method	Result
6	(Mishra et al., 2024) [42]	Develop an advanced model to enhance security and classification in IoT networks.	Proposing a weighted stacked ensemble of DCGAN and Bi-LSTM, regularized and tuned for optimal performance.	Achieve significant performance improvement in accuracy, precision, recall, and F1-score across multiple IoT datasets.
7	(Tahir et al., 2024) [43]	Enhancing IoT security through the proactive use of machine learning-based anomaly detection and adaptive defense mechanisms, addressing current and future cyber threats.	The study employs data from specified sources, preprocesses it, and applies Random Forest, Decision Tree, SVM, and Gradient Boosting algorithms for anomaly detection. It combines anomaly negotiation and self-adaptive defense procedures to fortify IT ecosystems dynamically.	The study demonstrates that Gradient Boosting achieves the highest precision of 89.34% among the models tested, underscoring its effectiveness in enhancing IoT security through machine learning.

in fortifying IoT networks against various threats.

The studies summarized in Table 3 highlight various innovative methods for detecting anomalies in IoT environments, each addressing specific security threats while presenting unique limitations. Nimmy et al. (2023) [44] aim to detect anomalies caused by DDoS attacks using a smart camera prototype based on Raspberry Pi, which gathers power consumption traces. Their approach, while effective in a controlled setup, may not fully capture the real-world variability found in smart home environments. Protogerou et al. (2021) [45] enhance IoT anomaly detection using a multi-agent system with GNNs. This method, though fostering collaborative intelligence to combat threats like DDoS attacks, faces challenges related to complexity and resource overhead, potentially limiting its scalability in extensive IoT settings.

Other studies focus on improving scalability and efficiency in different IoT applications. Wang et al. (2020) [46] address scalability I ssues in anomaly detection for massive machine-type communication (mMTC) in wireless software-defined networks (SDN) with a localized scheme (SEE-ADS) that aims to balance energy consumption and detection accuracy. However, the effectiveness of their localized evolving semi supervised learning-based heavyweight anomaly detection (LESLA) could vary with network conditions and attack types Shanmuganathan & Suresh (2023) [47] combine Markov models and LSTM networks for real-time anomaly detection in IoT sensor data, enhancing accuracy but facing constraints due to the computational limitations and power consumption of edge devices. Lawal et al. (2020) [48] explore the use of GNNs for anomaly detection in IIoT sectors, acknowledging the potential complexity and computational demands of such implementations. Ma (2020) [49] proposes an optimized RNN algorithm for cloud computing systems, which may face challenges in generalizability across different environments. Lastly, Yahyaoui et al. (2021) [50] introduce the READ-IoT framework for reliable event and anomaly detection in critical applications, but highlight the vulnerability of the detection system itself to failures and attacks, which could compromise its overall effectiveness.

Durai et al. [51] presented an ontology-based model (SQLIO) aimed at preventing and detecting SQL Injection Attacks (SQLIA) in web applications. The authors implemented ontology creation and prediction rule-based vulnerabilities to enhance security in a cloud environment. Their approach addressed SQLIA vulnerabilities to a significant extent, demonstrating its effectiveness in safeguarding web applications. Gupta et al. [52] presented a comparative review of various side-channel attacks and their countermeasures, highlighting the successful breaches of robust cryptographic operations through side-channel analysis. It discussed the inadvertent leakage of information exploited by these attacks and proposed a new approach to enhance network security. The primary objective was to summarize progress in side-channel attack research and identify future challenges. He et al. [53] explored the fundamental concepts and applications of cloud computing, emphasizing the security concerns intrinsic to its open and distributed nature. They proposed a security-enhancing algorithm using data mining and decision tree techniques, noted for its low computational demand and independence from the number of clients, facilitating practical implementation. Mishra et al. [54] explored the transformation of urban centers into smart cities through the integration of ICT, IoT, and AI technologies, focusing on enhancing urban efficiency and reducing costs. They proposed a novel architecture that combined these technologies with distributed cloud computing, aiming for autonomous city management and environmental sustainability. The study highlighted the economic benefits, implementation challenges, and the potential for smart cities to maintain ecological balance using solar energy. Almaiah et al. [55] introduced a novel data-fusion method paired with an emotional-intelligence-inspired enhanced dynamic Bayesian network (EDBN) for secure healthcare data transmission. They demonstrated superior performance over existing methods like DCNN, FRCNN, and CNN in terms of accuracy, precision, recall, and F1 scores. The proposed approach effectively improved patient care and data security. Another work [56] xplored the use of ma-

Table 3. Comparision of the related works in the recent years.

No.	References	Aim	Method	Weakness
1	(Nimmy et al., 2023) [44]	Detecting anomalies caused by DDoS attacks, limiting its scope to specific types of security threats.	The study involves prototyping a smart camera with Raspberry Pi to gather normal and attack-related power consumption traces, followed by evaluating various machine learning models, including a deep feed-forward neural network, for anomaly detection	Reliancind on a controlled experimental setup, which may not fully capture real-world variability in smart home environments.
2	(Protogerou et al., 2021) [45]	Improve IoT anomaly detection using a multi-agent system with Graph Neural Networks, fostering collaborative intelligence to combat network threats like DDoS attacks.	It involves deploying agents with Graph Neural Networks on IoT nodes and network devices to localize anomaly detection, using simulated datasets for training and evaluation.	Complexity and resource overhead of the multi-agent system, which could limit scalability in extensive IoT environments.
3	(Wang et al., 2020) [46]	Addressing scalability issues in anomaly detection for massive machine-type communication (mMTC) in wireless software-defined networks (SDN) while minimizing energy consumption and controller overload.	Proposing a localized anomaly detection scheme (SEE-ADS) that includes modules for lightweight predetection, dynamic strategy selection, and a localized evolving semisupervised learning-based heavyweight anomaly detection (LESLA) to detect attacks effectively without continuous high-energy consumption.	LESLA's performance could vary based on network conditions and attack types, potentially affecting detection accuracy.
4	(Shanmuganathan & Suresh, 2023) [47]	Developing an efficient anomaly detection method for real-time IoT sensor data using a Markov and LSTM-based network to enhance security and accuracy in smart environments.	The proposed methodology utilizes a combination of Markov models and Long Short-Term Memory (LSTM) networks to detect and remove outliers in real-time data from DHT sensors monitoring room temperature and humidity.	The study's approach, while effective, may still be constrained by the computational limitations and power consumption of edge-based IoT devices.
5	(Lawal et al., 2020) [48]	Investigating the use of graph neural networks (GNNs) for anomaly detection in IIoT-enabled smart transportation, smart energy, and smart factory sectors.	Analyzing point, contextual, and collective anomalies using GNN-empowered solutions and discussing related datasets, challenges, and open issues.	The potential complexity and computational demands of implementing GNNs in real-world IIoT systems.

chine learning, specifically generative adversarial network technology, to detect credit card fraud online. They identified and analyzed characteristics and sources of fraudulent activities, enabling real-time and accurate fraud detection. The research significantly advanced methods for preventing cyber fraud and enhancing network security. Praveen et al. [57] discussed the challenges and opportunities associated with using cloud computing in the healthcare sector, particularly emphasizing the need to secure sensitive medical data. The research highlighted the DACAR platform as a solution, which used a rule-based information sharing policy and a scalable cloud infrastructure to enhance data security, accuracy, and efficiency. The platform also aimed to address issues of large-scale deployment and service integration in healthcare systems [58] a blockchain-enabled decentralized FL framework for IoT anomaly detection, aiming to enhance efficiency and resilience. It pioneered an improved differentially private FL approach using generative adversarial nets to optimize data utility, marking a novel advancement in privacy-preserving techniques. Simulation results underscored its superior performance in robustness, accuracy, and convergence speed, while ensuring stringent privacy and security safeguards were maintained. Ullah & Mahmoud [59] focused on leveraging deep learning for IoT network anomaly detection, employing LSTM, BiLSTM, and GRU techniques. A hybrid model combining CNN and RNN was also proposed for enhanced performance. Various datasets were utilized to validate the models, demonstrating superior accuracy, precision, recall, and F1 scores compared to existing implementations. Deep learning emerged as a promising approach in combating evolving cybersecurity threats in IoT environments.

3. Challenges and solutions

The reviewed literature collectively underscores the multi-faceted nature of anomaly detection, reflecting its significance in diverse domains grappling with burgeoning data volumes and evolving threat landscapes. Each paper illuminates distinct dimensions of this complex landscape, emphasizing the criticality of addressing challenges unique to respective domains. For instance, Thudumu et al. [60] highlight the "curse of big dimensionality" prevalent in high-dimensional big data, urging for innovative approaches to mitigate its impact on detection accuracy and performance. Similarly, Fernandes et al. [61] delve into anomaly detection within information and communication technology, emphasizing the need to combat network anomalies and intrusion threats. These discussions underscore the urgency for tailored solutions that acknowledge the nuances of specific domains while striving for robust anomaly detection.

Moreover, the surveyed literature converges on the necessity of methodological diversity and technological adaptation to effectively tackle anomalies. From conventional techniques to cutting-edge deep learning methods, researchers explore a spectrum of approaches tailored to their respective contexts. Erhan et al. [62] exemplify this adaptability by discussing anomaly detection in sensor systems, where the fusion of traditional and data-driven techniques alongside considerations for computing architectures reflects a nuanced approach to anomaly detection. Similarly, Cook et al. navigate the challenges of applying anomaly detection to IoT data by drawing on diverse methodologies across domains, highlighting the need for interdisciplinary collaboration and methodological synthesis to address complex detection requirements.

Furthermore, the identified research gaps and future directions outlined in these papers serve as guiding beacons for advancing anomaly detection technology. Whether it's the quest for unified performance metrics in energy consumption anomaly detection frameworks as outlined by Himeur et al. [63], or the pressing need for real-time anomaly detection amidst cyber-attacks as articulated by Ariyaluran Habeeb et al. [64], the collective discourse underscores the imperative of continual innovation and interdisciplinary collaboration. As the data landscape evolves and threat vectors diversify, the pursuit of novel methodologies, robust frameworks, and adaptive technologies remains paramount in fortifying anomaly detection systems against emerging challenges.

S. Thudumu et al. [60] aimed to tackle the complexities of anomaly detection in high dimensional big data, a crucial issue given the increasing volume and velocity of data in various domains. The authors proposed a triangular model to structure the survey, focusing on three vertices: the problem of big dimensionality, the techniques and algorithms for anomaly detection, and the tools used in big data applications and frameworks. The researchers reviewed relevant literature that aligns directly with these vertices or is closely related, providing a comprehensive analysis of current strategies and limitations in handling high dimensional data. The authors also discussed recent techniques and applications that optimize anomaly detection in big data scenarios, highlighting the need for innovative approaches to overcome the "curse of big dimensionality" that impacts both performance and accuracy in traditional methods. L. Erhan et al. [62] reviewed state-of-the-art methods for anomaly detection in sensor systems, focusing on challenges such as information fusion, data volume, speed, and network/energy efficiency. The authors provided a taxonomy of conventional and data-driven techniques, analyzed their impact across different computing architectures (Cloud, Fog, Edge), and highlighted the method's strengths in intelligent sensing along with identifying future research challenges. H. Wang et al. [65] aimed to present a comprehensive review of outlier detection methods from 2000 to 2019, categorizing techniques such as distance-, clustering-, density-, ensemble-, and learning-based methods. The authors discussed the performance, pros, cons, and challenges of each method, providing a clear path for future research and a better understanding of current outlier detection techniques. G. Pang et al. [66] aimed to survey the advancements in deep anomaly detection, providing a comprehensive taxonomy across three high-level and eleven fine-grained categories of methods. They reviewed key intuitions, objective functions, assumptions, advantages, and disadvantages of each method, discussing how they address existing challenges and identifying future opportunities and perspectives for further research. G. Fernandes et al. [61] addressed to review the most critical aspects of anomaly detection in information and communication technology, focusing on network traffic anomalies, network data types, intrusion detection system categories, detection methods and systems, and open issues. The authors provided a structured analysis of the most relevant techniques and systems, concluding with a summary of unsolved problems and final remarks on future research directions.

A. A. Cook et al. [67] intended to review the challenges of applying anomaly detection techniques to IoT data, discussing various approaches developed across different domains and providing examples from the literature. They summarized the current challenges in the anomaly detection domain and identified potential research opportunities for future exploration. Y. Himeur et al. [63] presented a comprehensive review of existing anomaly detection frameworks for building energy consumption, utilizing artificial intelligence techniques. The authors introduced a detailed taxonomy for classifying algorithms based on various parameters and modules, highlighting the lack of precise definitions for anomalous power consumption, annotated datasets, unified performance metrics, reproducibility platforms, and privacy preservation measures. Despite these challenges, the researchers presented this article as a valuable reference for understanding the current state and future directions of anomaly detection technology in energy consumption. R. A. Ariyaluran Habeeb et al. [64] addressed the pressing need for effective anomaly detection in real-time networks amidst the proliferation of cyber-attacks facilitated by connected devices and the internet. The researchers investigated state-of-the-art real-time big data processing technologies and associated machine learning algorithms, emphasizing the inadequacy of current approaches in handling the massive data volumes generated by connected devices. By elucidating essential contexts and taxonomies, reviewing big data processing technologies, and discussing research challenges, this paper lays the groundwork for future advancements in real-time anomaly detection.

4. Conclusion

In conclusion, the surveyed papers underscore the critical role of anomaly detection in diverse domains, ranging from cybersecurity to structural health monitoring. While traditional signature-based intrusion detection systems have been the norm, the research showcases the limitations of such approaches, particularly in identifying unknown attacks. Anomaly detection systems emerge as a promising alternative, leveraging advanced techniques such as deep learning and belief-rule-based association rules to detect deviations from normal behavior. These systems offer greater adaptability and accuracy in detecting both known and unknown threats, paving the way for enhanced security measures and more reliable decision-making processes. The proposed algorithms and methodologies demonstrate significant advancements in addressing the challenges associated with anomaly detection. From handling uncertainties in sensor data to mitigating environmental variability in wireless sensor networks, the research presents innovative solutions that improve detection accuracy and reliability. Furthermore, the integration of machine learning techniques and statistical methods not only enhances anomaly detection but also contributes to the development of more robust and efficient systems for safeguarding critical infrastructures and ensuring the integrity of data. Overall, the findings highlight the importance of continuous research and innovation in anomaly detection to meet the evolving threats and challenges in today's dynamic technological landscape.Moreover, interdisciplinary collaboration and knowledge sharing are essential for accelerating progress in anomaly detection. Researchers across domains should engage in cross-disciplinary dialogue, sharing insights, methodologies, and best practices to foster a holistic understanding of anomaly detection challenges and solutions. Furthermore, the development of standardized evaluation metrics, benchmark datasets, and reproducibility platforms is crucial for facilitating comparative analyses and benchmarking of anomaly detection methods. By establishing common frameworks and evaluation criteria, the anomaly detection community can foster transparency, rigor, and reproducibility in research outcomes. In essence, the future of anomaly detection lies in collaborative innovation, methodological diversity, and technological adaptability. By addressing domain-specific challenges, fostering interdisciplinary collaboration, and establishing common standards, researchers can propel the field towards more robust, scalable, and effective anomaly detection solutions capable of meeting the evolving demands of today's data-driven world.

Authors contributions
Authors have contributed equally in preparing and writing the manuscript.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflict of interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] G. A. Marin. "**Network security basics**.". 3(6):68–72, 2005.
DOI: https://doi.org/10.1109/MSP.2005.153.

[2] S. Aljawarneh, M. Aldwairi, and M. B. Yassein. "**Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model**.". *J. Comput. Sci.*, 25:152–160, 2018.
DOI: https://doi.org/10.1016/j.jocs.2017.04.009.

[3] D. E. Denning. "**An intrusion-detection model**.". *IEEE Trans. Softw. Eng.*, SE-13(2):222–232, 1987.
DOI: https://doi.org/10.1016/j.procs.2016.09.346.

[4] S.-J. Horng et al. "**A novel intrusion detection system based on hierarchical clustering and support vector machines**.". *Expert Syst. Appl.*, 38(1):306–313, 2011.
DOI: https://doi.org/10.5815/ijcnis.2016.01.07.

[5] E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto. "**PCA filtering and probabilistic SOM for network intrusion detection**.". *Neurocomputing*, 164:71–81, 2015.
DOI: https://doi.org/10.1016/j.neucom.2014.09.083.

[6] I. S. Thaseen and C. A. Kumar. "**Intrusion detection model using fusion of chi-square feature selection and multi class SVM**.". *J. King Saud Univ.-Comput. Inf. Sci.*, 29(4):462–472, 2017.
DOI: https://doi.org/10.1016/j.procs.2019.11.170.

[7] M. V. Mahoney and P. K. Chan. "**Learning rules for anomaly detection of hostile network traffic**.". *3rd IEEE Int. Conf. Data Mining*, 2003.
DOI: https://doi.org/10.1109/ICDM.2003.1250987.

[8] C. Sinclair, L. Pierce, and S. Matzner. "**An application of machine learning to network intrusion detection**.". *15th Annu. Comput. Secur. Appl. Conf. (ACSAC'99)*, 1999.
DOI: https://doi.org/10.1016/j.gltp.2021.08.017.

[9] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida. "**A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection**.". *Comput. Secur.*, 75:36–58, 2018.
DOI: https://doi.org/10.1016/j.cose.2018.01.023.

[10] A. F. M. Agarap. "**A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data**.". *10th Int. Conf. Mach. Learn. Comput.*, 2018.
DOI: https://doi.org/10.48550/arXiv.1709.03082.

[11] M. M. Rathore et al. "**Intrusion detection using decision tree model in high-speed environment**.". *Int. Conf. Soft-Comput. Netw. Secur. (ICSNS)*, 2018.
DOI: https://doi.org/10.1109/ICSNS.2018.8573631.

[12] B. Cui, S. He, and H. Jin. "**Multi-layer anomaly detection for Internet traffic based on data mining**.". *9th Int. Conf. Innov. Mobile Internet Serv. Ubiquitous Comput.*, 2015.
DOI: https://doi.org/10.1109/IMIS.2015.43.

[13] P. A. A. Resende and A. C. Drummond. "**A survey of random forest based methods for intrusion detection systems**.". *ACM Comput. Surv.*, 51(3):1–36, 2018.
DOI: https://doi.org/10.1145/3178582.

[14] H. Feng, M. Li, X. Hou, and Z. Xu. "**Study of network intrusion detection method based on SMOTE and GBDT**.". *Appl. Res. Comput.*, 34(12):3745–3748, 2017.
DOI: https://doi.org/10.1145/3290480.3290505.

[15] J. Yang, J. Deng, S. Li, and Y. Hao. "**Improved traffic detection with support vector machine based on restricted Boltzmann machine**.". *Soft Comput.*, 21(11):3101–3112, 2017.
DOI: https://doi.org/10.1007/s00500-015-1994-9.

[16] S. A. Aljawarneh and R. Vangipuram. "**GARUDA: Gaussian dissimilarity measure for feature representation and anomaly detection in Internet of things**.". *J. Supercomput.*, 76(6):4376–4413, 2020.
DOI: https://doi.org/10.1145/3460620.3460757.

[17] J.-Y. Jiang, R.-J. Liou, and S.-J. Lee. "**A fuzzy self-constructing feature clustering algorithm for text classification**.". *IEEE Trans. Knowl. Data Eng.*, 23(3):335–349, 2010.
DOI: https://doi.org/10.1109/TKDE.2010.122.

[18] D. J. Weller-Fahy, B. J. Borghetti, and A. A. Sodemann. "**A survey of distance and similarity measures used within network intrusion anomaly detection**.". *IEEE Commun. Surv. Tutor.*, 17(1):70–91, 2014.
DOI: https://doi.org/10.1109/COMST.2014.2336610.

[19] W.-C. Lin, S.-W. Ke, and C.-F. Tsai. "**CANN: An intrusion detection system based on combining cluster centers and nearest neighbors**.". *Knowl.-Based Syst.*, 78:13–21, 2015.
DOI: https://doi.org/10.1016/j.knosys.2015.01.009.

[20] R. K. Gunupudi, M. Nimmala, N. Gugulothu, and S. R. Gali. "**CLAPP: A self constructing feature clustering approach for anomaly detection**.". *Future Gener. Comput. Syst.*, 74:417–429, 2017.
DOI: https://doi.org/10.1016/j.future.2016.12.040.

[21] A. Nagaraja, B. Uma, and R. k. Gunupudi. "**UTTAMA: An intrusion detection system based on feature clustering and feature transformation**.". *Found. Sci.*, 25(4):1049–1075, 2020.
DOI: https://doi.org/10.1007/s10699-019-09589-5.

[22] F. Ullah, S. Ullah, G. Srivastava, and J. C.-W. Lin. "**IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic**.". *Digit. Commun. Netw.*, 10(1): 190–204, 2024.
DOI: https://doi.org/10.1016/j.dcan.2023.03.008.

[23] Z. Wu, H. Zhang, P. Wang, and Z. Sun. "**RTIDS: A robust transformer-based approach for intrusion detection system**.". *IEEE Access*, 10:64375–64387, 2022.
DOI: https://doi.org/10.1109/ICACCS60874.2024.10717109.

[24] Y. Liu and L. Wu. "**Intrusion detection model based on improved transformer**.". *Appl. Sci.*, 13(10):6251, 2023.
DOI: https://doi.org/10.3390/app13106251.

[25] Z. Xiang and X. Li. "**RETRACTED ARTICLE: Fusion of transformer and ML-CNN-BiLSTM for network intrusion detection**.". *EURASIP J. Wireless Commun. Netw.*, 2023(1):71, 2023.
DOI: https://doi.org/10.1186/s13638-023-02279-8.

[26] V. Dutta, M. Pawlicki, R. Kozik, and M. Choras. "**Unsupervised network traffic anomaly detection with deep autoencoders**.". *Logic J. IGPL*, 30(6):912–925, 2022.
DOI: https://doi.org/10.1093/jigpal/jzac002.

[27] K. He, W. Zhang, X. Zong, and L. Lian. "**Network intrusion detection based on feature image and deformable vision transformer classification**.". *IEEE Access*, 12:44335–44350, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3376434.

[28] T. Jiang, X. Fu, and M. Wang. "**BBO-CFAT: Network intrusion detection model based on BBO algorithm and hierarchical transformer**.". *IEEE Access*, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3386405.

[29] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng. "**A transformer-based network intrusion detection approach for cloud security**.". *J. Cloud Comput.*, 13(1):5, 2024.
DOI: https://doi.org/10.1186/s13677-023-00574-9.

[30] H. Chen, G.-R. You, and Y.-R. Shiue. "**Hybrid intrusion detection system based on data resampling and deep learning**.". *Int. J. Adv. Comput. Sci. Appl.*, 15(2), 2024.
DOI: https://doi.org/10.14569/IJACSA.2024.0150214.

[31] F. S. Melıcias et al. "**GPT and interpolation-based data augmentation for multiclass intrusion detection in IIoT**.". *IEEE Access*, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3360879.

[32] A. Patcha and J.-M. Park. "**An overview of anomaly detection techniques: Existing solutions and latest technological trends**.". *Comput. Netw.*, 51(12):3448–3470, 2007.
DOI: https://doi.org/10.1016/j.comnet.2007.02.001.

[33] R. Ul Islam, M. S. Hossain, and K. Andersson. "**A novel anomaly detection algorithm for sensor data under uncertainty**.". *Soft Comput.*, 22(5):1623–1639, 2018.
DOI: https://doi.org/10.1007/s00500-016-2425-2.

[34] H. Saeedi Emadi and S. M. Mazinani. "**A novel anomaly detection algorithm using DBSCAN and SVM in wireless sensor networks**.". *Wireless Pers. Commun.*, 98(2):2025–2035, 2018.
DOI: https://doi.org/10.1007/s11277-017-4961-1.

[35] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola, and A. Benslimane. "**NovelADS: A novel anomaly detection system for intra-vehicular networks**.". *IEEE Trans. Intell. Transp. Syst.*, 23(11):22596–22606, 2022.
DOI: https://doi.org/10.1109/TITS.2022.3146024.

[36] H. Sarmadi and A. Karamodin. "**A novel anomaly detection method based on adaptive Mahalanobis-squared distance and one-class kNN rule for structural health monitoring under environmental effects**.". *Mech. Syst. Signal Process.*, 140:106495, 2020.
DOI: https://doi.org/10.1016/j.ymssp.2019.106495.

[37] H. Guo, Z. Zhou, D. Zhao, and W. Gaaloul. "**EGNN: Energy-efficient anomaly detection for IoT multivariate time series data using graph neural network**.". *Future Gener. Comput. Syst.*, 151: 45–56, 2024.
DOI: https://doi.org/10.1016/j.future.2023.09.028.

[38] S. Alangari. "**An unsupervised machine learning algorithm for attack and anomaly detection in IoT sensors**.". *Wireless Pers. Commun.*, pages 1–25, 2024.
DOI: https://doi.org/10.1007/s11277-023-10811-8.

[39] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman. "**Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms**.". *Sensors*, 24(2):713, 2024.
DOI: https://doi.org/10.3390/s24020713.

[40] M. M. Inuwa and R. Das. "**A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks**.". *Internet Things*, 26:101162, 2024.
DOI: https://doi.org/10.1016/j.iot.2024.101162.

[41] D. Alsalman. "**A Comparative Study of Anomaly Detection Techniques for IoT Security using AMoT (Adaptive Machine Learning for IoT Threats)**.". *IEEE Access*, 2024.
DOI: https://doi.org/10.3390/s24020713.

[42] A. K. Mishra, S. Paliwal, and G. Srivastava. "**Anomaly detection using deep convolutional generative adversarial networks in the internet of things**.". *ISA Trans.*, 145:493–504, 2024.
DOI: https://doi.org/10.1016/j.isatra.2023.12.005.

[43] U. Tahir, M. K. Abid, M. Fuzail, and N. Aslam. "**Enhancing IoT security through machine learning-driven anomaly detection**.". *VFAST Trans. Softw. Eng.*, 12(2):1–13, 2024.
DOI: https://doi.org/10.21015/vtse.v12i1.1766.

[44] K. Nimmy, M. Dilraj, S. Sankaran, and K. Achuthan. "**Leveraging power consumption for anomaly detection on IoT devices in smart homes**.". *J. Ambient Intell. Humaniz. Comput.*, 14(10): 14045–14056, 2023.
DOI: https://doi.org/10.1007/s12652-022-04110-6.

[45] A. Protogerou, S. Papadopoulos, A. Drosou, D. Tzovaras, and I. Refanidis. "**A graph neural network method for distributed anomaly detection in IoT**.". *Evolving Syst.*, 12(1):19–36, 2021.
DOI: https://doi.org/10.1007/s12530-020-09347-0.

[46] H. Wang, Q. Bao, Z. Shui, L. Li, and H. Ji. "**A novel approach to credit card security with generative adversarial networks and security assessment**.". 2024.
DOI: https://doi.org/10.53469/wjimt.2024.07(02).03.

[47] V. Shanmuganathan and A. Suresh. "**LSTM-Markov based efficient anomaly detection algorithm for IoT environment**.". *Appl. Soft Comput.*, 136:110054, 2023.
DOI: https://doi.org/10.1016/j.asoc.2023.110054.

[48] M. A. Lawal, R. A. Shaikh, and S. R. Hassan. "**Security analysis of network anomalies mitigation schemes in IoT networks**.". *IEEE Access*, 8:43355–43374, 2020.
DOI: https://doi.org/10.1109/ACCESS.2020.2976624.

[49] W. Ma. "**Analysis of anomaly detection method for Internet of things based on deep learning**.". *Trans. Emerg. Telecommun. Technol.*, 31(12):e3893, 2020.
DOI: https://doi.org/10.1002/ett.3893.

[50] A. Yahyaoui, T. Abdellatif, S. Yangui, and R. Attia. "**READ-IoT: Reliable event and anomaly detection framework for the Internet of Things**.". *IEEE Access*, 9:24168–24186, 2021.
DOI: https://doi.org/10.1109/ACCESS.2021.3056149.

[51] K. N. Durai, R. Subha, and A. Haldorai. "**A novel method to detect and prevent SQLIA using ontology to cloud web security**.". 117 (4):2995–3014, 2021.
DOI: https://doi.org/10.1007/s11277-020-07243-z.

[52] S. Gupta et al. "**A novel approach toward the prevention of the side channel attacks for enhancing the network security**.". 2022.
DOI: https://doi.org/10.21203/rs.3.rs-1334345/v1.

[53] Q. He and H. He. "**A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining**.". *Sustainability*, 13(1):101, 2021.
DOI: https://doi.org/10.3390/su13010101.

[54] K. N. Mishra and C. Chakraborty. "**A novel approach toward enhancing the quality of life in smart cities using clouds and IoT-based technologies. In: Digital Twin Technologies and Smart Cities**.". *Springer*, page 19–35, 2020.
DOI: https://doi.org/10.1007/978-3-030-18732-3_2.

[55] M. A. Almaiah et al. "**A novel approach for improving the security of IoT–medical data systems using an enhanced dynamic Bayesian network**.". *Electronics*, 12(20):4316, 2023.
DOI: https://doi.org/10.3390/electronics12204316.

[56] B. Wang, Y. Sun, and X. Xu. "**A scalable and energy-efficient anomaly detection scheme in wireless SDN-based mMTC networks for IoT**.". *IEEE Internet Things J.*, 8(3):1388–1405, 2020.
DOI: https://doi.org/10.1109/JIOT.2020.3011521.

[57] S. P. Praveen et al. "**A novel approach for enhance fusion based healthcare system in cloud computing**.". *J. Inf. Secur. Internet Things*, 9(1):84–96, 2023.
DOI: https://doi.org/10.54216/JISIoT.090106.

[58] L. Cui et al. "**Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures**.". *IEEE Trans. Ind. Informat.*, 18(5):3492–3500, 2021.
DOI: https://doi.org/10.1109/TII.2021.3107783.

[59] I. Ullah and Q. H. Mahmoud. "**Design and development of RNN anomaly detection model for IoT networks**.". *IEEE Access*, 10: 62722–62750, 2022.
DOI: https://doi.org/10.1109/ACCESS.2022.3176317.

[60] S. Thudumu, P. Branch, J. Jin, and J. Singh. "**A comprehensive survey of anomaly detection techniques for high dimensional big data**.". *J. Big Data*, 7(1):42, 2020.
DOI: https://doi.org/10.1186/s40537-020-00320-x.

[61] G. Fernandes et al. "**A comprehensive survey on network anomaly detection**.". 70(3):447–489, 2019.
DOI: https://doi.org/10.1007/s11235-018-0475-8.

[62] L. Erhan et al. "**Smart anomaly detection in sensor systems: A multi-perspective review**.". *Inf. Fusion*, 67:64–79, 2021.
DOI: https://doi.org/10.1016/j.inffus.2020.10.001.

[63] Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira. "**Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives**.". *Appl. Energy*, 287:116601, 2021.
DOI: https://doi.org/10.1016/j.apenergy.2021.116601.

[64] R. A. Ariyaluran Habeeb, F. Nasaruddin, A. Gani, I. A. Targio Hashem, E. Ahmed, and M. Imran. "**Real-time big data processing for anomaly detection: A survey**.". *Int. J. Inf. Manage.*, 45:289–307, 2019.
DOI: https://doi.org/10.1016/j.ijinfomgt.2018.08.006.

[65] H. Wang, M. J. Bah, and M. Hammad. "**Progress in outlier detection techniques: A survey**.". *IEEE Access*, 7:107964–108000, 2019.
DOI: https://doi.org/10.1109/ACCESS.2019.2932769.

[66] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel. "**Deep learning for anomaly detection: A review**.". *ACM Comput. Surv.*, 54(2):1–38, 2021.
DOI: https://doi.org/10.1145/3439950.

[67] A. A. Cook, G. Mısırlı, and Z. Fan. "**Anomaly detection for IoT time-series data: A survey**.". *IEEE Internet Things J.*, 7(7): 6481–6494, 2020.
DOI: https://doi.org/10.1109/JIOT.2019.2958185.