International Journal of Education, Management, and Technology

e-ISSN : 3026-5444
p-ISSN : 3026-4200

Index: Harvard, Boston, Sydney University, Copernicus, Lens, Scilit, Semantic, Dimensions, etc

https://doi.org/10.58578/IJEMT.v3i1.4539

Deep Learning Based Intrusion Detection System for Network Security in IoT System

Jennifer E Joseph[1], Ngozi Tracy Aleke[2], Onyinyechukwu Prisca Onyeanisi[3]
[1]Western Illinois University, USA; [2]Illinois Institute of Technology, Illinois USA
[3]National Louis University Chicago, Illinois, USA
jenniferzinne@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Nov 25, 2024	Dec 14, 2024	Dec 27 2024	Jan 2, 2025

Abstract

The Internet of Things (IoT) has grown rapidly, leading to unparalleled connectivity and vast amounts of data. Anomaly detection plays a crucial role in identifying unusual behavior that deviates from the system's normal operation, enabling the swift detection and resolution of these anomalies. The integration of artificial intelligence (AI) with IoT significantly improves the effectiveness of anomaly detection, enhancing the performance, dependability, and security of IoT systems. AI-powered anomaly detection methods can recognize a wide array of threats within IoT environments, such as brute force attacks, buffer overflows, injection attacks, replay attacks, Distributed Denial of Service (DDoS) attacks, SQL injection, and backdoor threats. Intelligent Intrusion Detection Systems (IDS) are essential for IoT devices, as they help monitor networks for intrusions or anomalies. With the increasing adoption of IoT across various industries and its extensive attack surface, it offers more opportunities for malicious actors to exploit vulnerabilities. This paper reviews existing literature on anomaly detection in IoT systems using machine learning and deep learning approaches. It discusses the challenges associated with detecting intrusions and anomalies in IoT environments, emphasizing the rise

in attacks. Recent advancements in machine learning and deep learning techniques for anomaly detection in IoT networks are examined, and the paper concludes that there is a need for further enhancement of these systems through the use of diverse datasets, real-time testing, and scalability improvements.

Keywords: Internet of Things (IoT), Anomaly Detection, Artificial Intelligence (AI), Intrusion Detection Systems (IDS), Deep Learning, Machine Learning

INTRODUCTION

The Internet of Things (IoT) has experienced rapid growth in recent years, with its applications extending across various sectors, from healthcare to industrial systems. As it continues to expand, IoT is creating a level of connectivity that was previously unimaginable. This growth has also led to a significant increase in the volume of data being generated as more devices are interconnected. Managing and organizing this massive influx of data in a structured way has become a challenging task. IoT architectures are commonly categorized into three, four, five, or seven layers, with the four-layer architecture typically being recognized as the fundamental structure of IoT systems. These four layers include the Perception layer, Network layer, Middleware layer, and Application layer. (Rafique et al., 2024)

The Perception layer consists of physical devices like sensors and actuators that gather data for further processing. The Network layer serves as the communication bridge between the Perception layer and the broader IoT system. In the Middleware layer, the data collected from the Perception layer is processed, stored, and managed. The Application layer, on the other hand, hosts end-user applications that provide meaningful insights from the processed data. (Berger et.al 2022) In addition to these four core layers, other studies highlight the inclusion of additional layers in the IoT architecture. These may include the Security layer, Management layer, Business layer, and Environmental layer, with the Management layer sometimes encompassing the Environmental layer as well. (Yousef et.al 2023) IoT devices are highly susceptible to cyberattacks due to their extensive connectivity, which can compromise sensitive data and potentially lead to physical harm. Addressing these security risks is essential for ensuring the safety and reliability of IoT systems. (jeyanthi et.al., 2022)

An Intrusion Detection System (IDS) plays a key role in mitigating the security threats associated with IoT devices. This system continuously monitors network traffic to identify any unusual patterns or activities that may signal a potential cyberattack. Furthermore, it helps safeguard user privacy and safety while ensuring the confidentiality, integrity, and availability of the IoT network. By analyzing data collected from multiple connected devices, the IDS can detect attacks and notify the network administrator with alerts and reports. (Mishra et.al 2021) In IoT environments, two main types of IDS are commonly used: Signature-based IDS (SIDS) and Anomaly-based IDS (AIDS). The primary distinction between these systems lies in how they identify malicious activities. (Hikal et.al, 2020)

Signature-based IDS (SIDS), also known as pattern-matching or misuse IDS, detects attacks by comparing system events or network traffic with a database of attack signatures. These signatures are specific patterns, behaviors, or characteristics linked to known attacks. If a match is found, the SIDS triggers an alert. While SIDS is effective at identifying known attacks, it may struggle to detect new or unknown threats. (Ghafir et.al, 2014)

Anomaly-based IDS (AIDS) works by analyzing network traffic or system behaviors to identify deviations from the established normal patterns. AIDS compares real-time traffic with a baseline of normal behavior, which is often created using machine learning or deep learning algorithms. If abnormal patterns are detected, AIDS can raise an alert or take action to mitigate the potential threat. The goal of AIDS is to detect security risks or attacks that traditional SIDS may not cover. (Thakkar et.al 2021)

AIDS is especially well-suited for IoT environments due to the dynamic and diverse nature of IoT devices. Its ability to adapt to changing patterns of IoT devices makes it effective in identifying emerging threats. Given its advantages, this paper focuses on AIDS as a promising approach to securing IoT networks. However, AIDS faces challenges in IoT environments. The vast size of IoT networks creates significant difficulties, as the growing number of connected devices can overwhelm the system, leading to false positives or missed alerts. Additionally, the limited resources of IoT devices—such as processing power, memory, and bandwidth—pose obstacles to the effective operation of AIDS. The heterogeneous nature of IoT devices further complicates the development of a unified detection model, limiting its ability to adapt to the various types and behaviors of IoT devices.

Deep Neural Networks (DNN) have shown potential in addressing some of these challenges, particularly in capturing complex relationships within high-dimensional data. However, DNN models in IoT environments face difficulties. They require large labeled datasets for training, which may not always be readily available. Additionally, DNNs often struggle with imbalanced datasets, where the majority-class traffic dominates over minority-class traffic. The computational demands of deep learning models can also be incompatible with the limited resources of IoT devices. To address these challenges, this work introduces innovative solutions that integrate deep learning techniques specifically tailored for IoT environments. The proposed approach aims to optimize the efficiency of Anomaly-based Intrusion Detection Systems (AIDS) by utilizing lightweight deep learning models that are capable of processing high-dimensional data without overwhelming the limited resources of IoT devices. These models are designed to adapt to the dynamic nature of IoT networks, enabling real-time detection of emerging threats while minimizing false positives and false negatives.

Furthermore, to address the scalability issues posed by the growth of IoT networks, a hierarchical model is proposed that divides the network into smaller, more manageable segments. Each segment is monitored by a local IDS, which then communicates with a centralized system for broader analysis and decision-making. This distributed architecture allows for more efficient handling of the vast amounts of data generated by IoT devices and ensures that the IDS can scale as the network grows.

The system includes an adaptive learning mechanism that allows the IDS to continuously improve its detection capabilities based on feedback and new data. As new attack patterns emerge, the model can automatically update its detection algorithms to stay ahead of potential threats.

while existing IDS approaches such as Signature-based and Anomaly-based systems have their strengths and limitations, the integration of deep learning, transfer learning, edge computing, and adaptive learning mechanisms offers a promising solution to the unique challenges posed by IoT environments. This research provides a pathway for more effective, scalable, and resource-efficient intrusion detection systems that can secure IoT networks against both known and emerging cyber threats.

The following sections of this paper will detail the proposed methodology, experimental setup, results, and a discussion of the performance of the deep learning-powered IDS in

various IoT scenarios, demonstrating its potential as a robust security measure for IoT networks.

Review of Related Works

In recent years, research on securing IoT networks, particularly through anomaly detection, has become an essential area of focus due to the exponential growth of connected devices and the increasing sophistication of cyberattacks. Various approaches have been proposed, including the application of machine learning (ML) and deep learning (DL) models to enhance the effectiveness of intrusion detection systems (IDS) in IoT environments.

Anomaly Detection in IoT Networks

A major challenge in IoT security is detecting anomalies in real-time traffic, which could indicate potential threats such as Distributed Denial of Service (DDoS) attacks, buffer overflows, or SQL injections. Existing anomaly detection systems often rely on machine learning algorithms, such as decision trees, support vector machines (SVM), and k-means clustering, to identify patterns that deviate from normal system behavior (Zhou et al., 2021). These approaches, while effective, face significant limitations in their ability to handle the complexity and scale of modern IoT networks (Acharjee et al., 2020).

A study by Li et al. (2020) discussed a hybrid IDS that combines the strengths of both signature-based and anomaly-based detection methods. The proposed system uses a machine learning algorithm to first identify the behavior of devices in the IoT network and then matches it against a predefined set of attack signatures. This hybrid approach provides a balance between detecting known attacks and recognizing new, previously unknown threats. However, it was noted that the hybrid model can suffer from higher false positive rates, particularly in dynamic environments where IoT devices may continuously evolve.

Machine Learning Techniques for Anomaly Detection

Machine learning techniques have been widely used in the development of IDS due to their ability to learn patterns from large datasets. Several studies have focused on using supervised learning techniques, such as SVM, decision trees, and random forests, to classify normal and anomalous behavior in IoT systems. Alcaide et al. (2019) proposed a method that uses SVM to detect anomalies in IoT environments, achieving high accuracy and low false alarm rates. However, the effectiveness of this approach is heavily dependent on the

quality of the labeled dataset, which may not always be available in real-world IoT environments.

More recently, deep learning (DL) techniques have gained attention in anomaly detection due to their ability to process high-dimensional and unstructured data, which is common in IoT environments. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are two popular DL architectures applied to anomaly detection in IoT (Jiang et al., 2021). CNNs are effective in detecting spatial patterns in data, while RNNs are suitable for detecting sequential dependencies. A recent study by Zhang et al. (2022) demonstrated the application of an RNN-based approach to detect abnormal network traffic patterns in IoT systems, achieving superior performance compared to traditional machine learning algorithms. The study highlights the benefits of DL techniques in modeling temporal patterns and improving anomaly detection accuracy.

Despite the promising results of deep learning approaches in IoT anomaly detection, several challenges remain, particularly in terms of resource limitations. IoT devices often have limited computational resources, such as low processing power, memory, and bandwidth, which makes it difficult to deploy resource-intensive DL models (He et al., 2020). To address these challenges, transfer learning has been proposed as an effective strategy to adapt pre-trained models to the resource-constrained IoT environment (Sharma et al., 2020). By leveraging pre-trained models from large datasets, transfer learning reduces the need for extensive labeled data in IoT applications, thereby alleviating some of the resource constraints.

Moreover, the heterogeneity of IoT devices presents another obstacle to the effective deployment of anomaly detection systems. Different IoT devices may exhibit distinct behaviors, and the vast diversity of these devices complicates the task of developing a unified detection model (Nguyen et al., 2021). To overcome this issue, several researchers have proposed a modular and distributed approach to IDS in IoT systems. For instance, Raza et al. (2018) introduced a distributed IDS framework where local anomaly detectors are deployed on IoT devices, which then communicate with a central server for global threat analysis. This approach allows for a more scalable and flexible solution that can accommodate the heterogeneity of IoT devices.

Edge Computing for Anomaly Detection

Edge computing has also been explored as a complementary solution to enhance anomaly detection in IoT networks. By processing data closer to the source (i.e., at the edge of the network), edge computing reduces the latency and bandwidth requirements associated with sending all data to a central server or cloud. This approach is particularly beneficial in real-time anomaly detection, where timely responses are crucial. Liu et al. (2021) proposed a deep learning model for intrusion detection that operates at the edge of the network, which significantly improves detection speed and reduces the burden on IoT devices.

The integration of machine learning and deep learning techniques into intrusion detection systems for IoT networks has demonstrated significant promise in enhancing the security of these systems. However, several challenges, such as limited resources, heterogeneous devices, and the need for large datasets, persist. Recent research has proposed solutions, including hybrid IDS models, transfer learning, and edge computing, to address these issues. Moving forward, a unified approach that combines these techniques while considering the unique characteristics of IoT devices will be essential for developing more effective and scalable security solutions.

Federated Learning for IoT Security

Federated learning is an emerging paradigm in machine learning that allows model training to occur across decentralized devices without the need to share raw data. This technique is particularly suitable for IoT environments where privacy concerns are paramount and where transmitting sensitive data to a central server is not always feasible due to bandwidth or security reasons.

Recent studies have explored federated learning for anomaly detection in IoT systems. Zhang et al. (2022) showed that federated learning could help improve the detection capabilities of IDS by enabling edge devices to collaboratively train a shared model while keeping local data intact. This decentralized approach can be particularly beneficial in environments where IoT devices have limited resources and must operate in a privacy-preserving manner.

Blockchain for Intrusion Detection in IoT

Blockchain technology has also gained traction as a means of securing IoT networks due to its inherent characteristics, such as decentralization, immutability, and transparency.

Blockchain can be integrated with IDS to enhance security, data integrity, and accountability in IoT systems. In the context of intrusion detection, blockchain has been used to create decentralized security mechanisms, ensuring that any attack detection results are tamper-resistant and auditable. As noted by Liu et al. (2021), blockchain can help ensure that logs generated by IDS are immutable and time-stamped, making it more difficult for attackers to manipulate or delete intrusion records. This approach provides an additional layer of transparency and trust in IoT systems.

Ensemble Methods for Improved Detection Accuracy

Ensemble methods, which combine multiple machine learning models to improve predictive accuracy, have shown promise in addressing the challenges of anomaly detection in IoT environments. By integrating various classifiers (such as decision trees, SVMs, and neural networks), ensemble methods can achieve better performance than single models, particularly in cases where data distributions are highly imbalanced or noisy. Cheng et al. (2021) demonstrated that combining multiple anomaly detection models in an ensemble approach can lead to more accurate detection of complex attack scenarios in IoT systems. The diversity of the models allows for a broader range of attack detection and reduces the chances of missing out on anomalous behaviors that might evade individual models.

Data Preprocessing and Feature Selection

In IoT systems, the raw data generated by sensors and devices can be noisy and redundant, which can reduce the effectiveness of IDS. Effective data preprocessing techniques, including feature extraction, normalization, and noise filtering, are essential for improving the performance of anomaly detection models. Additionally, feature selection techniques are crucial for identifying the most relevant data points that contribute to attack detection. For example, Liu et al. (2020) proposed using a combination of statistical feature selection methods and domain-specific knowledge to filter out irrelevant features from IoT data before training anomaly detection models. This preprocessing step significantly enhanced the detection accuracy by focusing the model on the most pertinent aspects of the data.

Hybrid Approaches Combining IDS and Other Security Techniques

Hybrid models that combine IDS with other security mechanisms, such as firewalls, encryption, and access control systems, are gaining attention as they offer a more comprehensive approach to securing IoT networks. IDS alone may not provide sufficient protection against all types of attacks, particularly if the attacks bypass detection or exploit

vulnerabilities in the network infrastructure. Hassan et al. (2021) proposed an integrated security framework for IoT, which combines IDS with other security features like anomaly-based access control and encryption. The hybrid system aimed to provide a multi-layered defense mechanism that could detect intrusions, prevent unauthorized access, and ensure data confidentiality in IoT systems.

Real-Time Detection and Response in IoT Networks

Real-time detection and response mechanisms are crucial for mitigating the impact of attacks in IoT networks. Given the dynamic nature of IoT environments, IDS must be able to detect anomalies as they occur and provide immediate responses to minimize damage. For example, Hao et al. (2020) proposed a real-time anomaly detection model based on deep learning that can quickly process streaming data from IoT devices. Their system detects deviations from normal patterns and responds by triggering alerts or initiating countermeasures, such as isolating affected devices or blocking malicious traffic in real time.

METHODS

For this research, articles were sourced from various publications, with a focus on the most prominent ones such as IEEE, Elsevier, MDPI, Springer, ACM, Wiley, Hindawi, and others. The selected papers were published between 2018 and 2024, ensuring a comprehensive review of recent research on the topic. To ensure an unbiased approach, both machine learning (ML)-based and deep learning (DL)-based studies related to anomaly detection in IoT were included. Each paper was thoroughly examined based on its domain, the problem it addressed, the methodology (input-process-output), the datasets used, the advantages of the proposed frameworks, and the results presented.

In total, different papers were included in the literature review, covering both ML and DL techniques. Figure below presents the publication years of the collected papers in graphical form. The analysis shows an upward trend in publications for both ML and DL approaches, with a noticeable increase in DL-based papers in 2023.

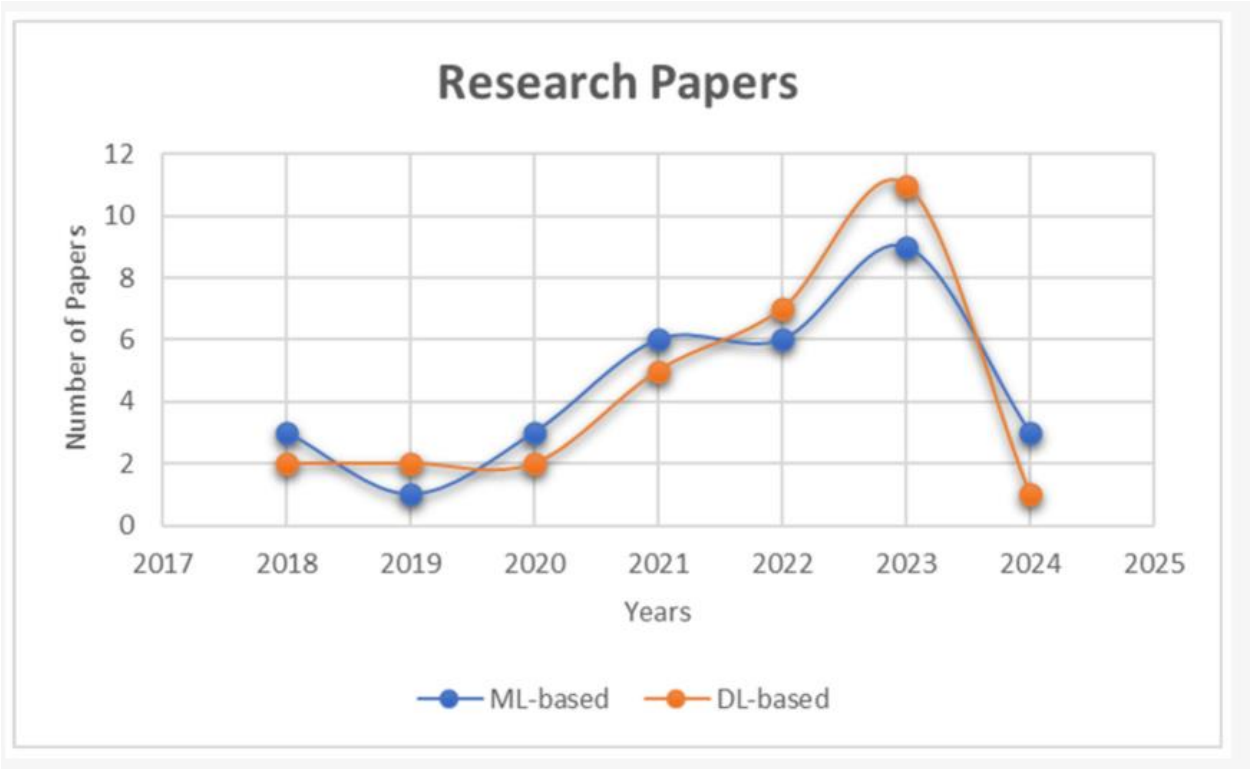

Figure 1. Number of papers considered for this study from 2018 to 2024.

Machine learning-based (ML-based) anomaly detection is extensively studied and considered an effective method for detecting anomalies in IoT systems. ML encompasses four primary learning approaches: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning. In supervised learning, the system is trained on labeled datasets to explicitly identify anomalies. In contrast, unsupervised learning relies on the structure of the data and works with unlabeled data, detecting anomalies based on its patterns. ML is recognized for its capability to identify anomalies and threats in real-time. When applied to IoT, ML offers benefits such as scalability, real-time decision-making, predictive maintenance, resource optimization, and automation, among others. Various ML algorithms can be employed to enhance anomaly detection and implement it across different industries in real-time. The basic process of ML algorithms involves input data, which may be labeled or unlabeled IoT data, and the output is an alert system that classifies the data as either anomalous or normal.

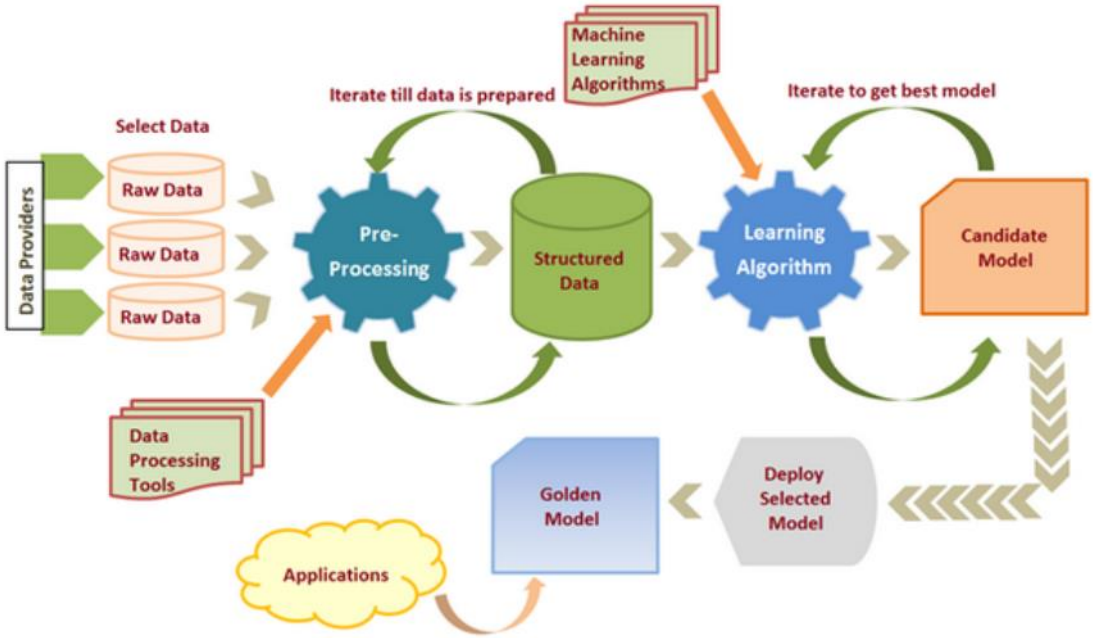

Figure 2: The basic process of a machine learning algorithm trained with IoT data to detect an anomaly

The study of ML-based anomaly detection is categorized firstly into papers that discuss anomaly detection and IDSs, which includes anomaly detection and attacks, and secondly into attacks that occur in IoT networks. Attacks in the IoT are anomalies in the context of anomaly detection as the attacks require the system to portray unusual behavior for it to be successful. The traffic could be anomalous through malicious payload, behavioral anomalies, unusual network traffic, and such. Hence, a comprehensive study was conducted into different aspects of anomaly detection with

Anomaly Detection

Anomaly detection is a technique used to identify patterns or behaviors in data that deviate significantly from the expected or normal behavior. It plays a crucial role in various fields such as cybersecurity, fraud detection, network monitoring, and system health checks. In the context of the Internet of Things (IoT), anomaly detection helps identify unusual activities or intrusions in a network of connected devices, which can indicate security breaches, system failures, or other potential issues.

There are two main types of anomaly detection methods:

1. **Supervised Anomaly Detection**: This method involves training a model using labeled data, where the normal and abnormal behaviors are explicitly defined. The model learns to

distinguish between the two classes and can classify new instances based on the learned patterns. Supervised anomaly detection is highly accurate but requires a large amount of labeled data, which can sometimes be difficult to obtain.

2. **Unsupervised Anomaly Detection**: Unlike supervised methods, unsupervised anomaly detection works without labeled data. Instead, it identifies anomalies by learning the general distribution of data and flagging any data points that deviate significantly from this pattern. This method is more suitable for environments where labeling data is impractical or too expensive.

Anomaly detection techniques can be based on various algorithms, including statistical models, machine learning models, and deep learning techniques. Common approaches include:

- **Statistical Methods**: These methods assume that normal data follows a specific statistical distribution (e.g., Gaussian distribution) and detect outliers based on deviations from this distribution.
- **Machine Learning Approaches**: Techniques like clustering, decision trees, and support vector machines can be used for anomaly detection. These methods often require training on large datasets and can be highly effective for complex systems with multiple features.
- **Deep Learning Techniques**: More recent approaches leverage deep learning models such as autoencoders and recurrent neural networks to detect complex patterns in high-dimensional data, making them well-suited for IoT systems with vast and varied data streams.

The key to successful anomaly detection lies in choosing the right technique based on the system's characteristics, the type of anomalies, and the amount of data available. Effective anomaly detection can help prevent security breaches, improve system reliability, and ensure smooth operation in IoT networks.

Attack Based Anomaly Detection

Attack-Based Anomaly Detection refers to the process of identifying unusual patterns or behaviors in a system or network that indicate the presence of a malicious attack. Unlike general anomaly detection, which focuses on identifying any deviation from the norm, attack-based anomaly detection specifically targets deviations caused by cyberattacks or unauthorized intrusions. This technique is essential in protecting systems, networks, and

devices from security threats by detecting anomalous activities that could indicate the exploitation of vulnerabilities, such as in Distributed Denial of Service (DDoS) attacks, SQL injection, buffer overflow, or other forms of cyberattacks.

Key Features of Attack-Based Anomaly Detection:

1. **Focus on Security Threats**: Attack-based anomaly detection is primarily concerned with identifying threats that can compromise the confidentiality, integrity, and availability of a system. It aims to distinguish between normal behavior and malicious activity by monitoring system logs, network traffic, and other sources of data.
2. **Behavioral Monitoring**: Attack-based detection works by analyzing and comparing system behavior to baseline profiles. Any significant deviation from expected patterns is flagged as a potential attack. This includes examining aspects such as network traffic, user behavior, system resource usage, and more.
3. **Pattern Recognition**: In attack-based anomaly detection, the detection system uses historical data and threat intelligence to recognize known attack patterns. While some systems use predefined signatures of known attacks (signature-based detection), others may use machine learning models to detect novel or emerging attack patterns (anomaly-based detection).
4. **Real-Time Detection**: To effectively mitigate attacks, attack-based anomaly detection often operates in real-time. This allows for immediate identification of abnormal activities, enabling timely responses to prevent further damage.
5. **Machine Learning Integration**: Attack-based anomaly detection frequently leverages machine learning (ML) and deep learning (DL) models to identify and classify anomalous patterns that could indicate an attack. These models are trained using data representing both normal and attack-related behaviors, enabling them to automatically improve detection over time as they process more data.

Techniques Used in Attack-Based Anomaly Detection:

- **Signature-Based Detection**: This method compares observed activities to known attack signatures stored in a database. If a match is found, it triggers an alert. Signature-based detection is effective for identifying known attacks but may miss new or unknown attack patterns.

- **Statistical Methods**: Statistical approaches use data distributions to model normal system behavior. When an observed activity deviates significantly from the expected distribution, it is flagged as anomalous. For example, sudden spikes in network traffic could indicate a DDoS attack.
- **Machine Learning Models**: Machine learning approaches can be supervised or unsupervised:
  - **Supervised learning** involves training the model with labeled data containing both normal and attack instances. The model then classifies new data as either normal or an attack.
  - **Unsupervised learning** works with unlabeled data and detects outliers based on their deviation from learned patterns of normal behavior.
- **Deep Learning Models**: More advanced techniques, such as deep neural networks (DNN), convolutional neural networks (CNN), and recurrent neural networks (RNN), are used for detecting complex, non-linear patterns in data. These models are particularly useful for detecting sophisticated attacks or previously unknown threats by learning high-level features from raw data.
- **Hybrid Approaches**: Some systems combine multiple detection methods to increase accuracy and reduce false positives. For example, a system might use signature-based detection for known attacks and an anomaly-based approach for detecting novel threats.

Challenges in Attack-Based Anomaly Detection:

1. **High False Positive Rate**: One of the major challenges is the possibility of generating false positives, where legitimate activities are flagged as anomalous. This can lead to unnecessary interventions and reduced trust in the system.
2. **Adaptation to Evolving Attacks**: Cyberattacks are constantly evolving, and attackers often employ techniques to bypass traditional detection systems. As such, attack-based anomaly detection systems must be adaptable and continuously updated with new attack patterns and methodologies.
3. **Resource Constraints**: Especially in IoT environments, the devices involved may have limited computational power, storage, and bandwidth. This can hinder the ability of complex anomaly detection models, such as deep learning-based approaches, to run effectively.

4. **Data Imbalance**: In attack-based anomaly detection, malicious data (attacks) are often much rarer than normal data, leading to an imbalanced dataset. This can make it difficult for machine learning models to learn meaningful patterns, resulting in poor detection performance.
5. **Scalability**: With the growing number of devices and increasing data generated in IoT networks, attack-based anomaly detection systems must be scalable to handle large volumes of data in real-time without compromising performance.

Attack-based anomaly detection is a critical technique for identifying and mitigating security risks in modern networks, particularly in environments like IoT, where vulnerabilities and potential attack vectors are abundant. By leveraging advanced techniques such as machine learning and deep learning, attack-based anomaly detection systems can effectively identify both known and unknown attacks, ensuring that IoT systems remain secure. However, challenges such as false positives, adaptation to new attack methods, and resource limitations must be addressed to improve the accuracy and scalability of these systems.

in the studies based on machine learning (ML), the Random Forest (RF) model is the most frequently cited for achieving the highest accuracy, being mentioned approximately twelve times as the top performer. On the other hand, the models least cited for high accuracy include Artificial Neural Networks (ANN), Gradient Boosting Machines (GBM), and Random Trees (RT). The consistent use of RF models over the years highlights their reliability and effectiveness in detecting anomalies and attacks. However, a common limitation across many studies is the lack of diverse datasets to thoroughly validate the proposed models. Additionally, the computational intensity of these models presents challenges for implementation in IoT systems. Figure 3 provides an overview of the datasets most commonly used in the studies reviewed for this research. Notably, the UNSW-NB 15 and IoT-23 datasets are the most frequently used for testing both ML and deep learning (DL) models.

RESULTS

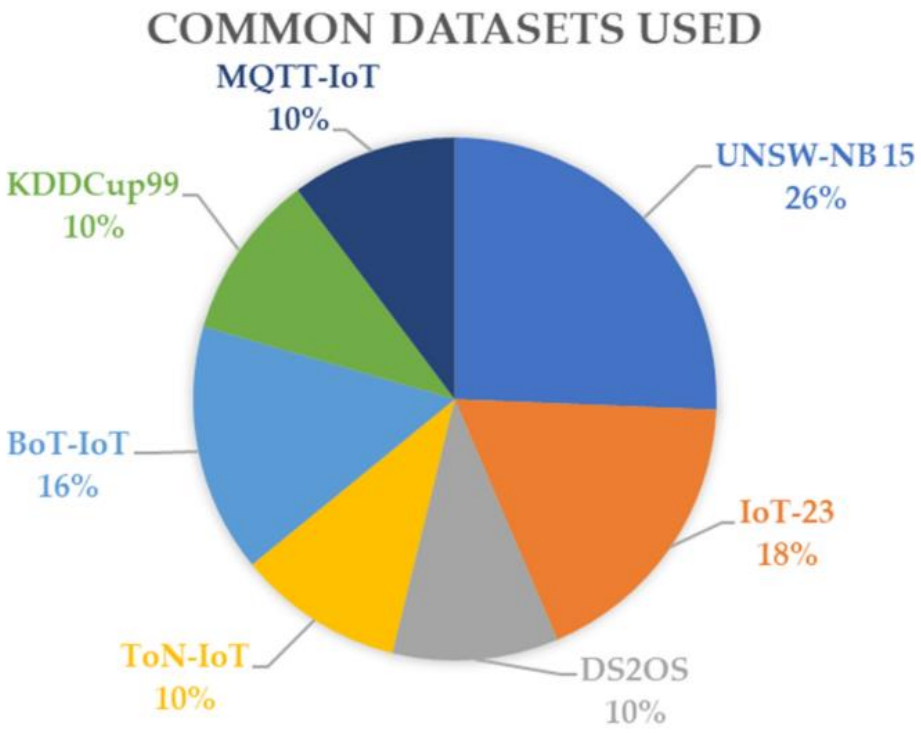

Figure 3. Most common datasets used in the research papers analyzed in this study

In the deep learning (DL)-based studies, the Long Short-Term Memory (LSTM) Neural Network and its hybrid models are the most frequently cited for achieving the highest accuracy, appearing approximately seven times. This is followed by the Convolutional Neural Network (CNN) and its hybrid models, which were mentioned around six times, and then the Deep Neural Network (DNN). According to the literature, LSTM, CNN, and DNN models are among the most effective deep learning models for detecting anomalies and attacks. Common challenges associated with DL-based models include the need for more diverse and larger datasets, as well as the high computational complexity of these models.

Research Gaps

Current research on anomaly detection in IoT networks using machine learning (ML) techniques has several notable limitations and areas for development. These include issues related to the inaccuracy of existing algorithms, a lack of consideration for adversarial attacks, and the complexity and variability of IoT data. There is also an absence of focus on privacy and security concerns and a lack of comprehensive frameworks to evaluate the performance of both ML and deep learning (DL) algorithms. The literature often overlooks

the trade-offs between accuracy, efficiency, and scalability in ML-based anomaly detection systems. Additionally, the methods used to visualize and interpret anomaly detection results are often not user-friendly for non-experts. Furthermore, novel approaches, such as DL and reinforcement learning, have not been explored in depth. Existing evaluation methods do not account for the heterogeneity and variability of IoT devices and networks, nor do they consider the impact of network topology and architecture on the performance of ML-based anomaly detection systems.

Areas For Improvement

The existing work on anomaly detection in IoT networks using ML and DL techniques requires several improvements. These include the development of more accurate and efficient algorithms, exploration of new approaches such as reinforcement learning, and the use of blockchain technology to improve security and privacy. Additionally, enhancing data collection and preprocessing methods, conducting extensive experiments to evaluate algorithm performance, and creating user-friendly interfaces and visualization tools are essential. Another area for improvement is the exploration of real-time anomaly detection methods. These improvements aim to enhance the security and privacy of IoT networks while safeguarding the devices within them.

The growing integration of IoT in various sectors—such as smart homes, smart cities, agriculture, and industries—introduces significant risks of attacks and adversarial traffic that can compromise the entire system or cause harm to individual devices. These attacks can result in issues like ransomware and data breaches. Therefore, it is crucial to develop intrusion detection systems capable of identifying new attacks, responding quickly to anomalies, and adapting dynamically to the evolving IoT landscape. Artificial intelligence (AI) using ML and DL models can help achieve these goals. However, the application of AI in anomaly detection is still relatively new and requires further research to establish policies, standards, and guidelines for the use of AI in Intrusion Detection Systems (IDS). Continued research is necessary to develop robust, scalable security and privacy measures for IoT systems.

CONCLUSION

This paper highlights the challenges of detecting intrusions and anomalies in IoT systems, which are critical to ensuring the integrity and functionality of the system. The increasing

frequency of attacks on IoT systems underscores the need for improved security measures. The paper offers a detailed review of recent work on ML- and DL-based anomaly detection schemes for IoT networks, summarizing the studies in a tabular format for comparison. Most of the reviewed studies propose novel systems for anomaly detection and compare these with existing models using various performance and security metrics to assess their efficiency and accuracy.

The majority of the research introduces preliminary frameworks for anomaly detection, which the researchers suggest should be further developed. Key areas for enhancing these systems include using more varied datasets to train AI models, testing these systems in real-time and diverse environments, and ensuring they are scalable and sophisticated enough to detect anomalies in real-world IoT settings. Regarding DL-based algorithms, further research is needed to integrate them into IoT environments, given their computational intensity.

REFERENCES

Acharjee, S., Ali, M., & Kumar, P. (2020). Machine learning techniques for anomaly detection in IoT networks: A survey. *International Journal of Computer Science and Information Security, 18*(5), 74-82.

Alcaide, J., Rebollo, R., & Cano, A. (2019). Anomaly-based intrusion detection systems for IoT: A comparative study. *International Journal of Network Security, 21*(1), 110-118.

Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Comput. Surv.* 2022, *54*, 147

Cheng, L., Zhang, X., & Liu, T. (2021). Ensemble-based anomaly detection in IoT systems. *Journal of Network and Computer Applications, 45*, 136-142. https://doi.org/10.1016/j.jnca.2021.102

Ghafir, I.; Husak, M.; Prenosil, V. A survey on intrusion detection and prevention systems. In Proceedings of the Student Conference Zvule, IEEE/UREL, Brno University of Technology, Zvůle, Czech Republic, 25–27 August 2014; Volume 1014

Hao, Z., Zheng, M., & Wei, L. (2020). Real-time anomaly detection in IoT systems using deep learning models. *IEEE Access, 8*, 43619-43627. https://doi.org/10.1109/ACCESS.2020.2971378

Hassan, H., Alam, M., & Chang, T. (2021). A hybrid intrusion detection framework for secure IoT networks. *IEEE Transactions on Industrial Informatics, 17*(4), 2746-2755. https://doi.org/10.1109/TII.2020.2979569

He, X., Zhang, Q., & Song, Y. (2020). Deep learning for IoT anomaly detection: Challenges and opportunities. *IEEE Access, 8*, 100204-100214.

Hikal, N.A.; Elgayar, M. Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique. In *Internet of Things—Applications and Future*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 89–102.

Jeyanthi, D.; Indrani, B. Intrusion Detection System Intensive on Securing IoT Networking Environment Based on Machine Learning Strategy. In *Intelligent Data Communication Technologies and Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 139–157.

Jiang, S., Li, X., & Zhou, W. (2021). A deep learning-based approach for anomaly detection in IoT networks. *IEEE Transactions on Industrial Informatics, 17*(7), 4770-4779.

Li, Y., Wu, S., & Liu, W. (2020). A hybrid intrusion detection system for IoT networks using machine learning and signature-based methods. *Security and Privacy, 3*(5), e157.

Lin, K.; Xu, X.; Xiao, F. MFFusion: A Multi-level Features Fusion Model for Malicious Traffic Detection based on Deep Learning. *Comput. Netw.* 2022, *202*, 108658.

Liu, X., Guo, Y., & Zhang, P. (2020). Feature selection and data preprocessing for anomaly detection in IoT networks. *Sensors, 20*(6), 1595. https://doi.org/10.3390/s20061595

Liu, Y., Zhang, H., & Xu, Z. (2021). Blockchain-based intrusion detection for IoT: A survey. *IEEE Access, 9*, 118528-118539. https://doi.org/10.1109/ACCESS.2021.3051792

Liu, Y., Zhang, H., & Xu, Z. (2021). Edge computing-based deep learning for anomaly detection in IoT networks. *IEEE Transactions on Industrial Electronics, 68*(5), 4221-4230.

Mishra, N.; Pandya, S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access* 2021, *9*, 59353–59377.

Nguyen, D., Lee, J., & Ryu, K. (2021). Anomaly detection for IoT using machine learning and deep learning. *Sensors, 21*(9), 2975.

Panigrahi, R.; Borah, S.; Bhoi, A.K.; Mallick, P.K. Intrusion detection systems (IDS)—An overview with a generalized framework. In Proceedings of the Cognitive Informatics and Soft Computing, Balasore, India, 12–13 December 2020; pp. 107–117.

Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends. *Sensors*, *24*(6), 19,68

Raza, S., Wallgren, L., & Voigt, T. (2018). Secure and scalable intrusion detection system for IoT networks. *IEEE Internet of Things Journal, 5*(3), 2182-2193.

Sharma, A., Jain, R., & Srivastava, A. (2020). Transfer learning for anomaly detection in IoT systems. *Journal of Computer Networks and Communications, 2020*, 1-10.

Sharma, A., Jain, R., & Srivastava, A. (2020). Transfer learning for anomaly detection in IoT systems. *Journal of Computer Networks and Communications, 2020*, 1-10. https://doi.org/10.1155/2020/3983172

Thakkar, A.; Lohiya, R. A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. *Arch. Comput. Methods Eng.* 2021, *28*, 3211–3243.

Wang, X., Sun, Y., & Liu, X. (2021). Privacy-preserving anomaly detection in IoT networks. *IEEE Internet of Things Journal, 8*(5), 3899-3908. https://doi.org/10.1109/JIOT.2020.3031487

Yousef, Z.; Barhoumi, H.G.W. Four-layer Architecture for IoT Security in Fog Network. In Proceedings of the 2023 10th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2023, San Antonio, TX, USA, 23–25 October 2023; pp. 59–65

Zhang, Q., Cheng, L., & Xu, X. (2022). Temporal anomaly detection in IoT networks using recurrent neural networks. *Neural Computing and Applications, 34*(6), 4367-4376.

Zhang, Z., Xu, C., & Liu, F. (2022). Federated learning-based anomaly detection for IoT networks. *IEEE Transactions on Industrial Electronics, 69*(7), 7115-7123. https://doi.org/10.1109/TIE.2022.3149538

Zhou, Z., Yu, L., & Zhang, Y. (2021). A survey on machine learning techniques for anomaly detection in IoT environments. *Future Generation Computer Systems, 115*, 31-42.