Data Anomaly Detection in the Internet of Things: A Review of Current Trends and Research Challenges

Min Yang[1]*, Jiajie Zhang[2]
Department of Information Engineering, Shandong Communication & Media College, Jinan 250200, Shandong, China[1]
School of Intelligent Transportation, Shandong Technician Institute, Jinan 250200, Shandong, China[2]

***Abstract*—The Internet of Things (IoT) has revolutionized how we interact with the physical world, bringing a new era of connectivity. Billions of interconnected devices seamlessly communicate, generating an unprecedented volume of data. However, the dramatic growth of IoT applications also raises an important issue: the reliability and security of IoT data. Data anomaly detection plays a pivotal role in addressing this critical issue, allowing for identifying abnormal patterns, deviations, and malicious activities within IoT data. This paper discusses the current trends, methodologies, and challenges in data anomaly detection within the IoT domain. In this paper, we discuss the strengths and limitations of various anomaly detection techniques, such as statistical methods, machine learning algorithms, and deep learning methods. IoT data anomaly detection carries unique characteristics and challenges that must be carefully considered. We explore these intricacies, such as data heterogeneity, scalability, real-time processing, and privacy concerns. By delving into these challenges, we provide a holistic understanding of the complexity associated with IoT data anomaly detection, paving the way for more targeted and effective solutions.**

***Keywords*—Internet of things; anomaly detection; security; machine learning**

I. Introduction

The Internet of Things (IoT) is a network of connected objects, systems, and devices that gather, share, and react to data. It facilitates device-to-human communication utilizing sensors, software, and internet connectivity [1]. IoT facilitates diverse applications and services, spanning from intelligent residences and urban environments to industrial automation and healthcare surveillance [2]. By seamlessly integrating physical objects into the digital realm, IoT enhances operational effectiveness, refines decision-making processes, and enables unprecedented levels of automation and connectivity across various facets of our everyday experiences [3]. The IoT structure typically consists of three main layers: perception, network, and application. The perception layer, also known as the sensing layer or physical layer, is the lowest layer of the IoT architecture. It comprises physical devices and sensors that capture data from the physical world. The network layer, also known as the communication layer, facilitates the connection and transmission of data between IoT devices and systems employing Wi-Fi, Bluetooth, Zigbee, cellular networks, or even IoT-specific protocols such as MQTT and CoAP. The application layer is the topmost layer in the IoT-layered structure. This layer utilizes data from IoT devices to provide valuable insights and services. It processes and analyzes the data for various purposes, including data visualization, decision-making, automation, and control [4, 5].

Smart cities, healthcare, industrial automation, and transportation are among the sectors that have benefited greatly from IoT's rapid growth. Since IoT devices generate huge amounts of data, ensuring the integrity and reliability of this data is crucial [6]. There is a significant threat to security and efficiency in IoT systems due to anomalous data patterns, deviations, and outliers [7]. Detecting data anomalies in the IoT is crucial for several reasons. Firstly, anomalies can indicate system malfunctions, faults, or cyberattacks that may disrupt normal operations or compromise the safety and privacy of individuals and organizations [8]. Early detection of anomalies enables proactive measures and timely responses to mitigate potential risks. Secondly, anomaly detection is crucial in optimizing system performance, enhancing decision-making processes, and ensuring data quality. Organizations can improve operational efficiency, optimize resource allocation, and gain valuable insights from the collected data by identifying unusual patterns or outliers in the data [9, 10].

The significance of data anomaly detection in the IoT lies in its potential to enhance system reliability, security, and overall performance. Through traditional monitoring approaches it identifies critical events, anomalies, or irregularities that may go unnoticed [11]. Machine learning and advanced analytics can identify data anomalies in IoT systems to enable real-time insights and preventive maintenance [12]. This not only boosts operational efficiency within the IoT landscape but also ensures the safety, security, and sustainability of the infrastructure. Given the dynamic nature of IoT deployments and the diverse range of IoT devices and applications, effective data anomaly detection techniques are required. These techniques must be scalable, adaptable, and capable of handling high volumes of data [13].

The detection of abnormal patterns or behaviors within data flows generated by IoT sensors is of utmost importance, especially in fields that largely rely on IoT technology, such as education and agriculture. Within these industries, the seamless integration of devices results in a substantial amount of data that facilitates improvements in operational effectiveness and fosters innovation. Nevertheless, the increase in data volume also exposes these fields to possible vulnerabilities, hence emphasizing the significance of identifying atypical or unsuitable patterns to uphold integrity and ensure security. Through the utilization of sophisticated anomaly detection methods, educators and agricultural practitioners have the ability to protect against malevolent behaviors, deviations, and

anomalies that have the potential to disrupt systems or jeopardize confidential data. This process not only guarantees the dependability of IoT-driven processes but also emphasizes the crucial significance of anomaly detection in strengthening the fundamental aspects of Education and Agriculture. This enables these sectors to effectively utilize the advantages offered by IoT technology while maintaining the integrity of data and achieving operational excellence.

Consequently, there is a growing interest in anomaly detection algorithms, innovative data preprocessing techniques, and integrating anomaly detection with real-time analytics and decision-making systems. In order to deploy IoT systems across various domains reliably and securely, advanced data anomaly detection techniques are needed [14]. This study makes the following major contributions:

- To conduct a comprehensive review of the current trends and techniques used for data anomaly detection in the context of the IoT.
- To identify and analyze the major research challenges and limitations associated with data anomaly detection in IoT environments.
- To explore and evaluate existing anomaly detection methods and algorithms, including statistical approaches, machine learning techniques, and anomaly-scoring mechanisms.
- To investigate the impact of different IoT data characteristics, such as high dimensionality, heterogeneity, and dynamic nature, on the performance of anomaly detection methods.
- To propose potential solutions and strategies for enhancing the accuracy, efficiency, and scalability of data anomaly detection in IoT applications.
- To highlight the open research issues and future directions in the field of data anomaly detection in IoT, providing insights for researchers and practitioners.

The reminder of the paper is organized in the following manner. Data anomaly detection strategies are reviewed in Section II. Challenging problems in IoT data anomaly detection are outlined in Section III. Discussion in Section IV and future research directions are highlighted in Section V. Finally, Section VI concludes the paper.

II. Data Anomaly Detection Strategies in IoT

Anomaly detection in the context of IoT involves identifying unusual or abnormal behavior in the data generated by IoT devices. Statistical methods support IoT anomaly detection by leveraging various statistical techniques to detect deviations from expected patterns [15]. These methods analyze the data collected from IoT devices and apply statistical models to identify anomalies that could indicate potential security breaches, system failures, or other abnormal events [16]. One widely used statistical method for IoT anomaly detection is the use of probability distributions [17]. This approach assumes that the data generated by IoT devices follow a specific probability distribution, such as Gaussian or Poisson distribution. By fitting the observed data to these distributions, statistical parameters can be estimated, allowing for the identification of anomalies based on deviations from the expected distribution [18]. For example, if the data deviate significantly from the mean or exhibit unusually high or low values, it could indicate the presence of anomalies. Time series analysis is another statistical method commonly employed in IoT anomaly detection [19]. IoT data often exhibit temporal dependencies, where the measurements captured by devices are collected over time. Time series analysis techniques, such as Autoregressive Integrated Moving Average (ARIMA) or exponential smoothing models, can be used to model and forecast the expected behavior of the data. Anomalies are then detected by comparing the observed and predicted values, and any significant deviations from the expected pattern are flagged as anomalies [20].

An anomaly can be described as a data point that exhibits a substantial deviation from the expected behavior within a modeled system. Anomalies are generally regarded as infrequent events or observations that significantly deviate from known patterns of behavior. These aberrations have the potential to occur in a single data point, a particular context or temporal segment, or even over the whole dataset. Anomalies, at their core, are frequently ascribed to extraneous variables, such as sensor faults or external assaults [21]. The main goal of a detection algorithm is to accurately identify occurrences of abnormalities, while also classifying or deducing their root causes. The careful selection of an approximation model that closely matches with the expected behavior of the data is crucial in the domain of binary classification for anomalies. Furthermore, the complexities inherent in various situations frequently require customized detection approaches that are specifically designed for each specific application. Fig. 1 illustrates a visual representation of several abnormalities as examples. The categorization of an IoT anomaly detection approach is derived by integrating the classifications presented in prior scholarly works, including [22]. The categorization of algorithms is determined by their problem-solving technique, application, method type, and algorithmic delay. Fig. 2 provides a visual representation of the four categories, offering a comprehensive and explanatory perspective.

A prevalent categorization of anomalies comprises three primary types: point, contextual, and collective anomalies. Point anomaly pertains to situations where a single data point diverges significantly from the anticipated behavior. An illustrative example involves the detection of credit card fraud [23]. In contextual anomaly, an instance could be regarded as anomalous within a particular context. Comparing multiple perspectives of the same data point might not consistently reveal anomalous behavior. Detection of contextual anomalies hinges upon considering both contextual and behavioral attributes together. For instance, anomalies related to traffic violations differ based on geo-location information [24]. Unlike point or contextual anomalies, the collective anomaly examines the entire dataset. A prime example of this type involves the use of electrocardiograms to monitor and identify anomalies or irregularities in the human heart's functioning [25].

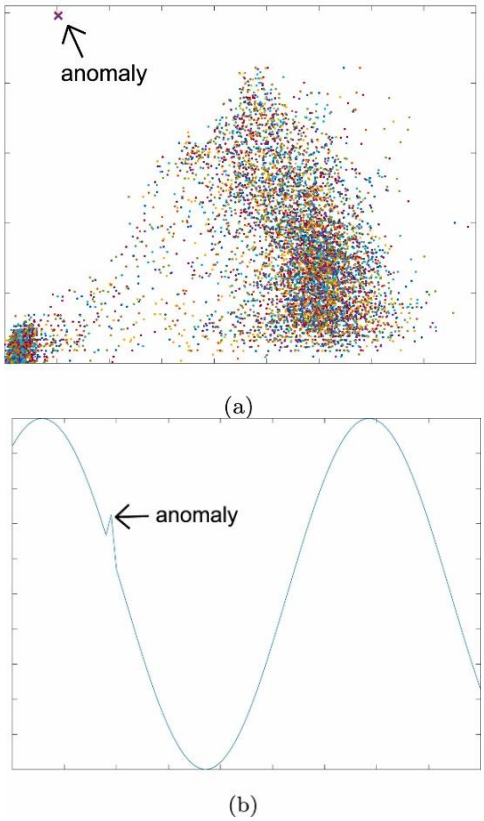

Fig. 1. Visual representations of anomalous occurrences.

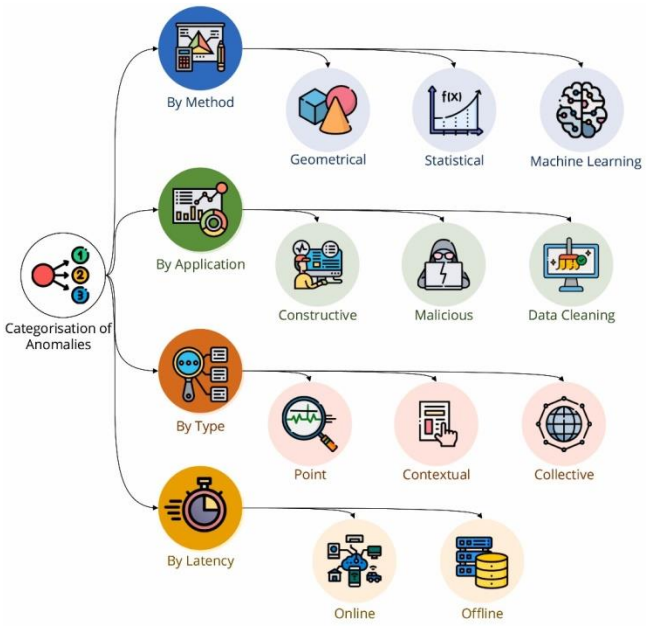

Fig. 2. An overview of anomaly classification.

Anomaly categorization by application can be classified into three distinct routes: constructive, destructive, and data cleaning. Constructive applications are inherently productive and contribute value to various domains. Examples include monitoring the daily activities of the elderly to prevent falls using image descriptors [26]. These applications encompass evaluating the performance of classifiers like multilayer perceptron (MLP), k-nearest neighbors (k-NN), and support vector machines (SVM). Another instance involves the utilization of reinforcement learning by Lu, et al. [27] for diverse unmanned aerial vehicle (UAV) applications, such as smart farming. Additionally, Nguyen, et al. [28] employ a federated learning approach for smart home applications. Destructive applications are devised to disrupt regular operations, often for dubious financial gains or with intentions to inflict harm upon networks, application data flowing through IoT networks, or critical business practices. These applications have a detrimental impact on society. For instance, Alsheikh, et al. [29] conducted a survey on IoT cyberattacks, shedding light on the latest advancements in IoT security. Solutions to counter such applications, such as RAPPER [30] and NBaIoT [31] employing autoencoders (AEs), focus on prevention or preemptive measures taken before an illicit incident, as well as detection or actions executed after an incident. Data cleaning or data cleansing applications, like DeepAnT [32], employ deep convolutional neural networks (CNNs) to eliminate unwanted data spikes and sensor noise from input signals. These applications play a pivotal role in enhancing the quality of data used in various contexts.

The latency and scalability characteristics of a detection algorithm play a pivotal role in determining its execution timeline, whether it operates on the fly during data collection or at a later storage stage. Online algorithms operate in a serial manner, processing information either one data point at a time or within a window. These algorithms function without requiring access to the entire input dataset. Traditional online methods encompass geometrical and statistical approaches, including distance-based, density-based, and deviation-based techniques. Illustrative examples of online methods are the IoT-Keeper by Hafeez, et al. [33], employing fuzzy C-means, and Bosman, et al. [34] adopt an ensemble approach. Offline algorithms, in contrast, have access to the complete dataset. These algorithms tend to be computationally intensive and sophisticated, aimed at solving complex problems within a reasonable timeframe. It is important to highlight that recent advancements have blurred the distinction between online and offline methods. For instance, [35] utilizes LSTM and Gaussian Naive Bayes, along with other aforementioned models, to perform model training offline and subsequently deploy the model online. This integration allows for more flexibility in the deployment process.

The methods employed can be categorized into geometrical, statistical, or machine learning approaches. Geometrical methods operate under the premise that when employing distance-based or density-based strategies to depict a dataset, the anticipated and anomalous data points become distinguishable. Within a dataset, the underlying principle of isolation or density-based techniques revolves around the notion that anomalies tend to manifest within sparse regions. These techniques utilize a threshold, denoted as ‘t’, either statically or dynamically on the calculated distance 'd' to classify anomalies. This threshold-driven classification is represented by the following equation:

$$d = \begin{cases} < t, & Normal\ (under\ threshold) \\ > t, & Anomaly (above\ threshold) \end{cases}$$

Statistical methods, exemplified by the minimal volume technique in [36], aim to model normal data patterns through mathematical models and distributions. The minimal volume approach constructs an n-dimensional simplex around the provided data cloud (considered as ground truth). The objective is to minimize the volume enclosed by the simplex while maximizing the inclusion of ground truth data points. Any data point that does not conform to the simplex is classified as an anomaly. Another example is the forecasting technique known as exponential smoothing [37], which predicts future data points using previous data and a smoothing parameter. Anomalous data detected via statistical methods are those that significantly diverge from the established model.

The third subcategory encompasses machine learning and deep learning models, which have seen an uptick in publication frequency in recent years. The choice of model is contingent on the inherent characteristics of the supplied data [38]. For instance, when dealing with sequential data inputs like audio, video, and time series, models like long short-term memory (LSTM) and transformer models tend to be preferred [39]. Conversely, non-sequential data types, such as image inputs, align well with convolutional neural networks (CNN) and autoencoders (AE) [40, 41]. These algorithms endeavor to discern between normal and anomalous behaviors by establishing a decision boundary. Examples include the utilization of SVM classifiers [42] to delineate such boundaries or employing LSTM networks [35] for future value forecasting in streaming data [43]. The nature of the task dictates whether these approaches fall under the categories of supervised, semi-supervised, self-supervised, or completely unsupervised learning [22, 44], depending on the availability of training labels.

Machine learning algorithms also are crucial to statistical methods for IoT anomaly detection. These algorithms learn patterns and relationships from the data and use them to classify normal and abnormal events. Supervised learning techniques, such as SVM or random forests, excel in scenarios where labeled data is available. By training on labeled data, where anomalies are specifically identified, these techniques generate models capable of automatically detecting anomalies in new, unlabeled data. On the other hand, unsupervised learning techniques, including clustering or outlier detection algorithms, prove valuable in identifying abnormal data points without the need for labeled training data.

Furthermore, statistical methods for IoT anomaly detection often involve thresholds or rule-based approaches. These methods establish predefined thresholds or rules based on the statistical properties of the data. Any data point that exceeds these thresholds or violates the predefined rules is considered an anomaly. For example, if the temperature readings from a temperature sensor exceed a certain predefined range, it could indicate a malfunction or abnormal condition. Statistical methods for IoT anomaly detection encompass a range of techniques, including probability distributions, time series analysis, machine learning algorithms, and threshold-based approaches. By leveraging statistical models and algorithms, these methods can effectively detect anomalies in the data generated by IoT devices, enabling proactive monitoring, early detection of abnormal events, and mitigation of potential risks in various IoT applications [45].

A. Machine Learning Algorithms for Anomaly Detection

Machine learning algorithms enable the automated and efficient detection of abnormal events in the vast amount of data generated by IoT devices [46, 47]. As IoT systems become increasingly complex and interconnected, traditional rule-based or threshold-based approaches may not be sufficient to capture anomalies' diverse and evolving patterns. Machine learning algorithms can learn from historical data, identify hidden patterns, and adapt to changing conditions, making them well-suited for IoT anomaly detection. One key advantage of machine learning algorithms in IoT anomaly detection is their ability to handle large-scale and heterogeneous data [48]. IoT environments generate various data types, including sensor readings, network traffic data, and system logs. Machine learning algorithms can process and analyze this data to identify abnormal patterns that may indicate security breaches, system failures, or other abnormal behavior. These algorithms can handle the high volume, velocity, and variety of IoT data, making them scalable and applicable to real-time monitoring and analysis [49].

Machine learning algorithms are also capable of detecting anomalies that may not be recognized explicitly or anticipated in advance [50]. The capabilities of machine learning algorithms differ from those of rule-based approaches because they can learn from historical data and detect anomalies that may not be apparent to humans. This allows for proactive anomaly detection and early warning of potential issues, reducing the risk of system downtime or security breaches. Machine learning algorithms also offer the advantage of adaptability to changing IoT environments. As IoT systems evolve and new anomalies emerge, machine learning algorithms can continuously learn and update their models to capture these changes. This adaptability is crucial in dynamic IoT environments where anomalies manifest in various forms and evolve over time. By continuously analyzing and updating their models, machine learning algorithms can effectively detect and respond to emerging anomalies, ensuring the reliability and security of IoT systems.

Automated anomaly detection in the realm of IoT is made possible through the utilization of machine learning algorithms. This approach significantly reduces the need for manual inspections and analysis [51]. Manual analysis of IoT data is known to be a time-consuming, error-prone, and inefficient process, particularly in large-scale deployments. By employing machine learning algorithms, data streams from IoT devices can be continuously and efficiently monitored in real time. This empowers human operators to focus their attention on more critical tasks, such as investigating anomalies, taking appropriate actions, or fine-tuning the anomaly detection system. In IoT anomaly detection, machine learning algorithms are indispensable for handling large-scale, heterogeneous data, detecting previously unseen anomalies, adjusting to changing environments, and automating the process. By leveraging machine learning, IoT systems become more secure, reliable, and efficient by proactively detecting and mitigating abnormal events.

B. Deep Learning Algorithms for Anomaly Detection

The power of neural networks allows deep learning algorithms to detect IoT anomalies by analyzing the data generated by IoT devices and learning complex patterns and representations [52]. Deep learning algorithms, specifically deep neural networks (DNNs), have shown impressive performance in a variety of domains, such as computer vision, natural language processing, and speech recognition. Their ability to automatically extract hierarchical features and model intricate relationships makes them well-suited for detecting anomalies in IoT data. One key advantage of deep learning algorithms in IoT anomaly detection is their ability to handle high-dimensional and unstructured data. IoT environments generate vast amounts of data, often in the form of images, sensor readings, or textual information. Deep learning algorithms can effectively process and analyze this data, capturing subtle and nuanced patterns that may indicate anomalies. Convolutional neural networks (CNNs) excel at analyzing images or sensor data, while recurrent neural networks (RNNs) can handle sequential or time series data. These architectures enable deep learning algorithms to learn highly relevant representations for anomaly detection.

Another crucial aspect of deep learning algorithms is their ability to automatically learn from data without relying on explicit feature engineering. Traditional machine learning algorithms often require manual extraction of relevant features, which can be time-consuming and challenging, especially in the context of IoT data. Deep learning algorithms can autonomously learn and extract relevant features directly from raw data, alleviating the need for extensive domain knowledge and manual feature engineering. This enables them to uncover intricate and non-linear relationships in the data, improving the accuracy and robustness of anomaly detection. Furthermore, deep learning algorithms offer the advantage of transfer learning and knowledge sharing across different IoT domains. Pretrained deep neural networks, trained on large-scale datasets from other domains, can be fine-tuned and adapted to specific IoT anomaly detection tasks. This knowledge transfer allows deep learning algorithms to leverage the learned representations and patterns from other domains, even when labeled training data is limited or unavailable in the IoT domain. Transfer learning facilitates faster model convergence, improves generalization, and enhances anomaly detection performance in IoT environments.

Deep learning algorithms also exhibit the potential for anomaly detection in real-time or streaming IoT data. Recurrent neural networks, such as LSTM or gated recurrent units (GRU), are well-suited for modeling sequential dependencies in time series data. This makes them effective for detecting anomalies in streaming IoT data, where anomalies can occur in real-time. By analyzing the temporal patterns and dependencies in the data, deep learning algorithms can provide timely detection and response to abnormal events, enabling proactive monitoring and mitigation. Deep learning algorithms, with their ability to handle high-dimensional data, automatically learn relevant features, facilitate transfer learning, and analyze sequential dependencies, are instrumental in IoT anomaly detection. By leveraging deep neural networks, IoT systems can effectively detect anomalies in complex and diverse data generated by IoT devices. The role of deep learning algorithms extends to enhancing the security, reliability, and operational efficiency of IoT systems by enabling proactive anomaly detection and timely mitigation of abnormal events.

C. Comparative Analysis of the Different Techniques

Table I presents a side-by-side comparison of the machine and deep learning algorithms for IoT data anomaly detection. SVM is known for its high accuracy and effectiveness in handling linearly separable data. It is robust against overfitting and can handle high-dimensional data. However, SVMs can be computationally intensive for large datasets, and selecting appropriate kernel functions requires careful consideration. Random Forests offer high accuracy and are robust against overfitting. They handle high-dimensional data well and provide feature importance rankings. However, they are less interpretable compared to individual decision trees. k-NN is a simple and intuitive algorithm that detects local anomalies. It is non-parametric and adaptive, making it suitable for handling noisy data. However, k-NN is sensitive to the choice of distance metric and requires careful selection of the value for k.

TABLE I. AN OVERVIEW OF THE MACHINE AND DEEP LEARNING ALGORITHMS FOR IOT DATA ANOMALY DETECTION

Algorithm	Performance	Strengths	Limitations	References
Support Vector Machines (SVM)	High accuracy Effective for linearly separable data	Robust against overfitting Can handle high-dimensional data	Computationally intensive for large datasets Requires careful selection of kernel functions	[42, 53-59]
Random Forests (RF)	High accuracy Robust against overfitting	Handles high-dimensional data Provides feature importance rankings	Less interpretable compared to individual decision trees	[8, 60-62]
k-Nearest Neighbors (k-NN)	Simple and intuitive Effective for local anomalies	Non-parametric and adaptive Handles noisy data	Sensitive to the choice of distance metric Requires careful selection of k value	[7, 63-66]
Recurrent Neural Networks (RNN)	Captures sequential dependencies in time series data	Handles variable-length sequences Suitable for streaming data	Can suffer from vanishing/exploding gradients Computationally intensive training	[67-74]
Long Short-Term Memory (LSTM)	Captures long-term dependencies in sequential data	Robust against vanishing gradients Suitable for modeling time series data	Requires more training time compared to traditional RNNs	[75-77]
Convolutional Neural Networks (CNN)	Effective for image or sensor data analysis	Automatically learns hierarchical features Robust to spatial variations	It may require large amounts of labeled training data Computationally intensive for large images	[78-81]

Recurrent Neural Networks (RNNs) capture sequential dependencies in time series data, making them suitable for IoT anomaly detection. They can handle variable-length sequences and are well-suited for streaming data. However, RNNs can suffer from vanishing or exploding gradients during training and can be computationally intensive. LSTM networks are a type of RNN that can capture long-term dependencies in sequential data. They are robust against vanishing gradients and are suitable for modeling time series data. However, LSTM networks generally require more training time compared to traditional RNNs. Convolutional Neural Networks (CNNs) are particularly effective for analyzing image or sensor data in IoT applications. They automatically learn hierarchical features from the data and are robust to spatial variations. CNNs can capture local patterns and spatial dependencies, making them suitable for anomaly detection in image-based IoT data. However, CNNs often require large amounts of labeled training data to achieve optimal performance. Training large CNN models can also be computationally intensive, especially when dealing with high-resolution images or large-scale datasets.

III. Challenges in Data Anomaly Detection for IoT

Data anomaly detection in IoT is challenging due to the unique characteristics of IoT data and the constraints imposed by IoT environments. Some of the key challenges are as follows:

- High dimensionality: IoT data is often high-dimensional, consisting of multiple sensors, devices, and data sources. This high dimensionality increases the complexity of anomaly detection, as the algorithms need to handle a large number of features and capture complex relationships between them. Dimensionality reduction techniques may be required to mitigate this challenge.
- Scalability: IoT systems generate massive amounts of data in real-time. Anomaly detection algorithms must scale to handle the high data volume and velocity. Processing such large-scale data in real-time requires efficient algorithms and infrastructure capable of handling the computational and storage demands.
- Imbalanced data: IoT datasets often suffer from imbalanced class distributions, where the number of normal instances significantly outweighs the number of anomalies. This imbalance can lead to biased models that favor the majority class and fail to detect anomalies accurately. Specialized techniques, such as oversampling or undersampling, must address this challenge and improve the detection of rare anomalies.
- Concept drift: IoT environments are dynamic and subject to concept drift, where the statistical properties of the data change over time. Anomaly detection models trained on historical data may become less effective when faced with new data patterns. Continuous model updating and adaptation are necessary to cope with concept drift and ensure the detection of evolving anomalies.
- Lack of labeled data: Anomaly detection typically requires labeled data for training supervised learning algorithms. However, acquiring labeled data for anomalies can be challenging in IoT settings, as anomalies are rare and may not be explicitly labeled. Obtaining a sufficient amount of accurately labeled data for training can be a significant obstacle, necessitating the exploration of unsupervised or semi-supervised techniques.
- Privacy and security: IoT data often contains sensitive information, making privacy and security crucial concerns. Anomaly detection algorithms must operate in a privacy-preserving manner, ensuring that sensitive data is not exposed or compromised during the detection process. This requires carefully designing algorithms and techniques to balance anomaly detection accuracy with privacy protection.
- Real-time detection: Many IoT applications require real-time anomaly detection for timely response and mitigation. Achieving real-time detection poses challenges due to the computational complexity of certain algorithms and the need to process and analyze data in near real-time. Efficient algorithms and scalable infrastructure are necessary to enable real-time anomaly detection in IoT environments.
- Interpretability: Understanding why a certain instance is flagged as an anomaly is important for effective anomaly management and decision-making. However, some advanced machine learning and deep learning algorithms, while powerful in detecting anomalies, may lack interpretability. Balancing accuracy and interpretability becomes crucial, especially in applications requiring explainability.

Addressing the mentioned challenges in data anomaly detection for IoT requires the development of innovative algorithms, techniques, and frameworks for detecting high-dimensional, streaming data effectively, adjusting to dynamic environments, maintaining privacy, and enabling detection in real-time. Such solutions should also be energy efficient and easily scalable to accommodate large-scale networks. Finally, they should be able to detect anomalies caused by malicious activities, natural phenomena, and human errors.

IV. Discussion

Various case studies demonstrate the diverse applications of IoT data anomaly detection across industries, ranging from manufacturing and home security to healthcare. Organizations can achieve improved operational efficiency, enhanced security, and proactive decision-making in various IoT-enabled environments by leveraging anomaly detection algorithms. Table II shows an overview of case studies of IoT data anomaly detection. IoT sensors are deployed across machinery and equipment in a manufacturing plant to collect data on parameters such as temperature, vibration, and energy consumption. Anomaly detection algorithms are applied to this data to identify deviations from normal behavior that may indicate potential failures or malfunctions. By detecting anomalies in real-time, maintenance teams can proactively

schedule repairs or replacement of components before costly breakdowns occur. This approach is employed by companies like General Electric (GE) for their industrial IoT applications, resulting in shorter downtime, longer equipment lifetime, and reduced costs.

TABLE II. CASE STUDIES OF IOT DATA ANOMALY DETECTION

Industry	Case study	Key benefits	References
Manufacturing	Predictive maintenance	Reduced downtime Increased equipment lifespan Cost savings	[82-85]
Smart home	Security	Improved home security Real-time anomaly detection Mitigation of potential security risks	[86-89]
Healthcare	Patient monitoring	Early detection of health issues Personalized healthcare monitoring Timely intervention	[90-93]

Smart homes use IoT devices, such as cameras, motion sensors, doors, and windows, to generate data on activities and events within the home. Anomaly detection algorithms are applied to this data to identify abnormal behaviors or potential intrusions. This allows homeowners to receive real-time alerts and take appropriate actions to mitigate security risks. Companies like Ring and Nest have implemented IoT data anomaly detection techniques in their smart home security systems, providing homeowners with improved security and peace of mind. IoT devices and wearables in healthcare generate vast amounts of patient data, including vital signs, activity levels, and medication adherence. Anomaly detection algorithms are applied to this data to identify deviations from normal patterns, indicating potential health issues or abnormal behavior. Healthcare providers can receive alerts and take timely interventions, leading to early detection of health issues and personalized patient care. Companies like Philips and Medtronic utilize IoT data anomaly detection in their healthcare monitoring solutions to improve patient outcomes and enhance healthcare delivery.

V. FUTURE RESEARCH DIRECTIONS

Future research in IoT data anomaly detection is expected to address several key challenges and explore novel techniques to improve the effectiveness and efficiency of anomaly detection in IoT systems. Here are some potential research directions:

- Real-time and edge-based anomaly detection: As the IoT ecosystem continues to grow, there is a need for more real-time and edge-based anomaly detection methods. Research efforts will aim to develop lightweight algorithms and models to efficiently process and analyze IoT data at the edge, reducing latency and enabling timely anomaly detection and response.
- Robustness to evolving IoT environments: IoT environments are dynamic, with device changes, data distributions, and system configurations. Future research will focus on developing anomaly detection techniques that adapt to evolving IoT environments. This includes techniques for transfer learning, online learning, and incremental learning, allowing anomaly detection models to learn and adapt to new patterns and anomalies continuously.
- Multi-modal anomaly detection: IoT systems generate data from diverse sources, including sensors, images, audio, and video streams. Future research will explore multi-modal anomaly detection techniques that can effectively integrate and analyze data from different modalities to detect complex anomalies that may not be apparent when analyzing each modality individually.
- Explainable AI for anomaly detection: Explainability and interpretability are critical for building trust and understanding in anomaly detection systems. Future research will focus on developing explainable AI techniques for anomaly detection in IoT data. This includes methods to provide interpretable explanations for detected anomalies, visualizations of anomaly patterns, and feature importance analysis to enhance the transparency and usability of anomaly detection models.
- Privacy-preserving anomaly detection: IoT data often contain sensitive and personal information. Future research will explore privacy-preserving anomaly detection techniques that can detect anomalies without compromising the privacy of individuals or revealing sensitive data. This includes techniques such as federated learning, secure multi-party computation, and differential privacy to ensure data privacy and security in anomaly detection processes.
- Adversarial anomaly detection: As IoT systems become more interconnected and susceptible to attacks; future research will investigate adversarial anomaly detection techniques. These techniques aim to detect anomalies caused by malicious activities, such as data poisoning or evasion attacks. Research efforts will focus on developing robust anomaly detection models to detect and mitigate adversarial attacks on IoT data.

By addressing these research directions, IoT data anomaly detection can advance to effectively handle the complexities and challenges of large-scale IoT systems, leading to more reliable anomaly detection, enhanced security, and improved operational efficiency.

VI. CONCLUSION

Data anomaly detection plays a crucial role in the IoT ecosystem, enabling the detection of abnormal behavior, potential failures, and security breaches in IoT systems. This paper comprehensively reviews current trends and research challenges in IoT data anomaly detection. We have discussed utilizing machine learning and deep learning algorithms, such as ensemble methods, RNNs, and CNNs, in IoT anomaly detection. These algorithms offer advanced capabilities in

handling IoT data's complexity and high dimensionality, leading to more accurate and efficient anomaly detection. Additionally, unsupervised learning approaches and real-time processing have emerged as prominent trends, enabling the detection of anomalies without the need for labeled data and facilitating timely responses to detected anomalies.

Furthermore, integrating multiple data sources and pursuing explainable AI techniques have been identified as important trends in IoT data anomaly detection. By leveraging diverse sources of IoT data and providing interpretable explanations for detected anomalies, organizations can enhance anomaly detection systems' reliability, usability, and trustworthiness. However, several research challenges remain in the field. These include the development of real-time and edge-based anomaly detection methods, addressing the robustness of anomaly detection models in evolving IoT environments, and exploring multi-modal anomaly detection techniques. Privacy-preserving and adversarial anomaly detection are crucial areas requiring further research to ensure data privacy, security, and resilience against malicious activities.

REFERENCES

[1] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy‐efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, p. e6959, 2022.

[2] A. Zhu, M. Ma, S. Guo, and Y. Yang, "Adaptive Access Selection Algorithm for Multi-Service in 5G Heterogeneous Internet of Things," IEEE Transactions on Network Science and Engineering, vol. 9, no. 3, pp. 1630-1644, 2022.

[3] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9326-9337, 2019.

[4] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23-34, 2017.

[5] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," Measurement, vol. 151, p. 107198, 2020.

[6] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, pp. 1-21, 2019.

[7] A. M. F. Al-Sammarrie and M. Çevik, "Anomaly detection of web traffic between IoT Devices," in 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022: IEEE, pp. 1-3.

[8] A. Alzahrani, T. Baabdullah, and D. B. Rawat, "Attacks and Anomaly Detection in IoT Network Using Machine Learning," in HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part II 23, 2021: Springer, pp. 465-472.

[9] H. Liu, C. Zhong, A. Alnusair, and S. R. Islam, "FAIXID: A framework for enhancing ai explainability of intrusion detection results using data cleaning techniques," Journal of network and systems management, vol. 29, no. 4, p. 40, 2021.

[10] H. Hoorfar, N. Taheri, H. Kosarirad, and A. Bagheri, "Efficiently Guiding K-Robots Along Pathways with Minimal Turns," EAI Endorsed Transactions on AI and Robotics, vol. 2, 2023.

[11] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes, and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT," Future Generation Computer Systems, 2022.

[12] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," IEEE Communications Surveys & Tutorials, 2023.

[13] L. Yang and A. Shami, "IoT data analytics in dynamic environments: From an automated machine learning perspective," Engineering Applications of Artificial Intelligence, vol. 116, p. 105366, 2022.

[14] E. Şengönül, R. Samet, Q. Abu Al-Haija, A. Alqahtani, B. Alturki, and A. A. Alsulami, "An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey," Applied Sciences, vol. 13, no. 8, p. 4956, 2023.

[15] Y. Liu, H. Wang, X. Zheng, and L. Tian, "An efficient framework for unsupervised anomaly detection over edge-assisted internet of things," ACM Transactions on Sensor Networks, 2023.

[16] W. Jia, R. M. Shukla, and S. Sengupta, "Anomaly detection using supervised learning and multiple statistical methods," in 2019 18th IEEE International Conference On Machine Learning and Applications (ICMLA), 2019: IEEE, pp. 1291-1297.

[17] S. Maleki, S. Maleki, and N. R. Jennings, "Unsupervised anomaly detection with LSTM autoencoders using statistical data-filtering," Applied Soft Computing, vol. 108, p. 107443, 2021.

[18] J. Pei, K. Zhong, M. A. Jan, and J. Li, "Personalized federated learning framework for network traffic anomaly detection," Computer Networks, vol. 209, p. 108906, 2022.

[19] A. A. Cook, G. Mısırlı, and Z. Fan, "Anomaly detection for IoT time-series data: A survey," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6481-6494, 2019.

[20] J. E. Zhang, D. Wu, and B. Boulet, "Time series anomaly detection for smart grids: A survey," in 2021 IEEE Electrical Power and Energy Conference (EPEC), 2021: IEEE, pp. 125-130.

[21] H. Hoorfar, H. Kosarirad, N. Taheri, F. Fathi, and A. Bagheri, "Concealing Robots in Environments: Enhancing Navigation and Privacy through Stealth Integration," EAI Endorsed Transactions on AI and Robotics, vol. 2, 2023.

[22] M. Fahim and A. Sillitti, "Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review," IEEE Access, vol. 7, pp. 81664-81681, 2019.

[23] P. Srikanth, "An efficient approach for clustering and classification for fraud detection using bankruptcy data in IoT environment," International Journal of Information Technology, vol. 13, no. 6, pp. 2497-2503, 2021.

[24] S. Asoba, S. Supekar, T. Tonde, and J. A. Siddiqui, "Advanced traffic violation control and penalty system using IoT and image processing techniques," in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020: IEEE, pp. 554-558.

[25] H. Li and P. Boulanger, "A survey of heart anomaly detection using ambulatory electrocardiogram (ECG)," Sensors, vol. 20, no. 5, p. 1461, 2020.

[26] Y. M. Galvão, V. A. Albuquerque, B. J. Fernandes, and M. J. Valença, "Anomaly detection in smart houses: Monitoring elderly daily behavior for fall detecting," in 2017 IEEE Latin American Conference on Computational Intelligence (LA-CCI), 2017: IEEE, pp. 1-6.

[27] H. Lu, Y. Li, S. Mu, D. Wang, H. Kim, and S. Serikawa, "Motor anomaly detection for unmanned aerial vehicles using reinforcement learning," IEEE internet of things journal, vol. 5, no. 4, pp. 2315-2322, 2017.

[28] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DÏoT: A federated self-learning anomaly detection system for IoT," in 2019 IEEE 39th International conference on distributed computing systems (ICDCS), 2019: IEEE, pp. 756-767.

[29] M. Alsheikh, L. Konieczny, M. Prater, G. Smith, and S. Uludag, "The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders," IEEE Consumer Electronics Magazine, vol. 11, no. 3, pp. 59-68, 2021.

[30] M. Alam, S. Sinha, S. Bhattacharya, S. Dutta, D. Mukhopadhyay, and A. Chattopadhyay, "Rapper: Ransomware prevention via performance counters," arXiv preprint arXiv:2004.01712, 2020.

[31] Y. Meidan et al., "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12-22, 2018.

[32] M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, "DeepAnT: A deep learning approach for unsupervised anomaly detection in time series," Ieee Access, vol. 7, pp. 1991-2005, 2018.

[33] I. Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge," IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 45-59, 2020.

[34] H. H. Bosman, G. Iacca, A. Tejada, H. J. Wörtche, and A. Liotta, "Ensembles of incremental learners to detect anomalies in ad hoc sensor networks," ad hoc networks, vol. 35, pp. 14-36, 2015.

[35] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5244-5253, 2019.

[36] C. O'Reilly, A. Gluhak, and M. A. Imran, "Distributed anomaly detection using minimum volume elliptical principal component analysis," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 9, pp. 2320-2333, 2016.

[37] S. Mahajan, L.-J. Chen, and T.-C. Tsai, "Short-term PM2. 5 forecasting using exponential smoothing method: A comparative analysis," Sensors, vol. 18, no. 10, p. 3223, 2018.

[38] A. S. Charles, "Interpreting deep learning: The machine learning rorschach test?," arXiv preprint arXiv:1806.00148, 2018.

[39] Z. Chen, D. Chen, X. Zhang, Z. Yuan, and X. Cheng, "Learning graph structures with transformer for multivariate time-series anomaly detection in IoT," IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9179-9189, 2021.

[40] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT healthcare analytics: The importance of anomaly detection," in 2016 IEEE 30th international conference on advanced information networking and applications (AINA), 2016: IEEE, pp. 994-997.

[41] C. Han and X. Fu, "Challenge and Opportunity: Deep Learning-Based Stock Price Prediction by Using Bi-Directional LSTM Model," Frontiers in Business, Economics and Management, vol. 8, no. 2, pp. 51-54, 2023.

[42] K. Yang, S. Kpotufe, and N. Feamster, "An efficient one-class SVM for anomaly detection in the Internet of Things," arXiv preprint arXiv:2104.11146, 2021.

[43] M. Dunne, G. Gracioli, and S. Fischmeister, "A comparison of data streaming frameworks for anomaly detection in embedded systems," in Proceedings of the 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), Orlando, FL, USA, 2018.

[44] J. Webber, A. Mehbodniya, Y. Hou, K. Yano, and T. Kumagai, "Study on idle slot availability prediction for WLAN using a probabilistic neural network," in 2017 23rd Asia-Pacific Conference on Communications (APCC), 2017: IEEE, pp. 1-6.

[45] R. Al-amri, R. K. Murugesan, M. Man, A. F. Abdulateef, M. A. Al-Sharafi, and A. A. Alkahtani, "A review of machine learning and deep learning techniques for anomaly detection in IoT data," Applied Sciences, vol. 11, no. 12, p. 5320, 2021.

[46] G. Han, J. Tu, L. Liu, M. Martinez-Garcia, and Y. Peng, "Anomaly detection based on multidimensional data processing for protecting vital devices in 6G-enabled massive IIoT," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5219-5229, 2021.

[47] S. N. H. Bukhari, J. Webber, and A. Mehbodniya, "Decision tree based ensemble machine learning model for the prediction of Zika virus T-cell epitopes as potential vaccine candidates," Scientific Reports, vol. 12, no. 1, p. 7810, 2022.

[48] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered Federated Learning Architecture for Network Anomaly Detection in Large Scale Heterogeneous IoT Networks," Computers & Security, p. 103299, 2023.

[49] R. Singh et al., "Analysis of Network Slicing for Management of 5G Networks Using Machine Learning Techniques," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[50] J. Roldán, J. Boubeta-Puig, J. L. Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks," Expert Systems with Applications, vol. 149, p. 113251, 2020.

[51] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for iot security attacks," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 2021.

[52] Y. Yue, S. Li, P. Legg, and F. Li, "Deep learning-based security behaviour analysis in IoT environments: A survey," Security and Communication Networks, vol. 2021, pp. 1-13, 2021.

[53] I. Razzak, K. Zafar, M. Imran, and G. Xu, "Randomized nonlinear one-class support vector machines with bounded loss function to detect of outliers for large scale IoT data," Future Generation Computer Systems, vol. 112, pp. 715-723, 2020.

[54] T. Ergen and S. S. Kozat, "A novel distributed anomaly detection algorithm based on support vector machines," Digital Signal Processing, vol. 99, p. 102657, 2020.

[55] C. Ioannou and V. Vassiliou, "Network attack classification in IoT using support vector machines," Journal of Sensor and Actuator Networks, vol. 10, no. 3, p. 58, 2021.

[56] J. Lesouple, C. Baudoin, M. Spigai, and J.-Y. Tourneret, "How to introduce expert feedback in one-class support vector machines for anomaly detection?," Signal Processing, vol. 188, p. 108197, 2021.

[57] A. Yahyaoui, T. Abdellatif, and R. Attia, "Hierarchical anomaly based intrusion detection and localization in IoT," in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), 2019: IEEE, pp. 108-113.

[58] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, p. 100059, 2019.

[59] A. P. Agrawal and N. Singh, "Comparative analysis of SVM kernels and parameters for efficient anomaly detection in IoT," in 2021 5th International Conference on Information Systems and Computer Networks (ISCON), 2021: IEEE, pp. 1-6.

[60] Y.-L. Tsou, H.-M. Chu, C. Li, and S.-W. Yang, "Robust distributed anomaly detection using optimal weighted one-class random forests," in 2018 IEEE International Conference on Data Mining (ICDM), 2018: IEEE, pp. 1272-1277.

[61] S. H. Khan, A. R. Arko, and A. Chakrabarty, "Anomaly Detection in IoT Using Machine Learning," in Artificial Intelligence for Cloud and Edge Computing: Springer, 2021, pp. 237-254.

[62] R. Primartha and B. A. Tama, "Anomaly detection using random forest: A performance revisited," in 2017 International conference on data and software engineering (ICoDSE), 2017: IEEE, pp. 1-6.

[63] H. Yang, S. Liang, J. Ni, H. Li, and X. S. Shen, "Secure and efficient k nn classification for industrial internet of things," IEEE Internet of Things Journal, vol. 7, no. 11, pp. 10945-10954, 2020.

[64] U. Garg, H. Sivaraman, A. Bamola, and P. Kumari, "To Evaluate and Analyze the Performance of Anomaly Detection in Cloud of Things," in 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2022: IEEE, pp. 1-7.

[65] G. E. Selim, E. E. D. Hemdan, A. M. Shehata, and N. A. El‐Fishawy, "An efficient machine learning model for malicious activities recognition in water‐based industrial internet of things," Security and Privacy, vol. 4, no. 3, p. e154, 2021.

[66] S. Narayanan and S. Uludag, "Two-Tier Anomaly Detection for an Internet of Things Network," in 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023: IEEE, pp. 325-328.

[67] I. Ullah and Q. H. Mahmoud, "Design and development of RNN anomaly detection model for IoT networks," IEEE Access, vol. 10, pp. 62722-62750, 2022.

[68] Y. Wu, H.-N. Dai, and H. Tang, "Graph neural networks for anomaly detection in industrial internet of things," IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9214-9231, 2021.

[69] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852-8859, 2020.

[70] S. Saurav et al., "Online anomaly detection with concept drift adaptation using recurrent neural networks," in Proceedings of the acm india joint

international conference on data science and management of data, 2018, pp. 78-87.

[71] Y. Wang, M. Perry, D. Whitlock, and J. W. Sutherland, "Detecting anomalies in time series data from a manufacturing system using recurrent neural networks," Journal of Manufacturing Systems, vol. 62, pp. 823-834, 2022.

[72] B. Roy and H. Cheung, "A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network," in 2018 28th international telecommunication networks and applications conference (ITNAC), 2018: IEEE, pp. 1-6.

[73] D. Gaifulina and I. Kotenko, "Selection of deep neural network models for IoT anomaly detection experiments," in 2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2021: IEEE, pp. 260-265.

[74] K. Ahmadi and R. Javidan, "Trust Based IOT Routing Attacks Detection Using Recurrent Neural Networks," in 2022 Sixth International Conference on Smart Cities, Internet of Things and Applications (SCIoT), 2022: IEEE, pp. 1-7.

[75] R. Xu, Y. Cheng, Z. Liu, Y. Xie, and Y. Yang, "Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services," Future Generation Computer Systems, vol. 112, pp. 228-242, 2020.

[76] N. Ding, H. Ma, H. Gao, Y. Ma, and G. Tan, "Real-time anomaly detection based on long short-Term memory and Gaussian Mixture Model," Computers & Electrical Engineering, vol. 79, p. 106458, 2019.

[77] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 3469-3477, 2020.

[78] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," IEEE Access, vol. 9, pp. 103906-103926, 2021.

[79] H. Asgharzadeh, A. Ghaffari, M. Masdari, and F. S. Gharehchopogh, "Anomaly-based Intrusion Detection System in the Internet of Things using a Convolutional Neural Network and Multi-Objective Enhanced Capuchin Search Algorithm," Journal of Parallel and Distributed Computing, 2023.

[80] A. Mellit, M. Benghanem, O. Herrak, and A. Messalaoui, "Design of a novel remote monitoring system for smart greenhouses using the internet of things and deep convolutional neural networks," Energies, vol. 14, no. 16, p. 5045, 2021.

[81] N. A. Bajao and J.-a. Sarucam, "Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units," Mesopotamian journal of cybersecurity, vol. 2023, pp. 22-29, 2023.

[82] P. Kamat and R. Sugandhi, "Anomaly detection for predictive maintenance in industry 4.0-A survey," in E3S web of conferences, 2020, vol. 170: EDP Sciences, p. 02007.

[83] S. K. Bose, B. Kar, M. Roy, P. K. Gopalakrishnan, and A. Basu, "ADEPOS: Anomaly detection based power saving for predictive maintenance using edge computing," in Proceedings of the 24th asia and south pacific design automation conference, 2019, pp. 597-602.

[84] E. Gultekin and M. S. Aktas, "A Business Workflow Architecture for Predictive Maintenance using Real-Time Anomaly Prediction On Streaming IoT Data," in 2022 IEEE International Conference on Big Data (Big Data), 2022: IEEE, pp. 4568-4575.

[85] A. Chehri and G. Jeon, "The industrial internet of things: examining how the IIoT will improve the predictive maintenance," in Innovation in Medicine and Healthcare Systems, and Multimedia: Proceedings of KES-InMed-19 and KES-IIMSS-19 Conferences, 2019: Springer, pp. 517-527.

[86] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, "Anomaly detection in smart home operation from user behaviors and home conditions," IEEE Transactions on Consumer Electronics, vol. 66, no. 2, pp. 183-192, 2020.

[87] A. Lara, V. Mayor, R. Estepa, A. Estepa, and J. E. Díaz-Verdejo, "Smart home anomaly-based IDS: Architecture proposal and case study," Internet of Things, vol. 22, p. 100773, 2023.

[88] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, "Anomaly detection models for smart home security," in 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2019: IEEE, pp. 19-24.

[89] X. Dai, J. Mao, J. Li, Q. Lin, and J. Liu, "HomeGuardian: Detecting Anomaly Events in Smart Home Systems," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[90] S. Hadjixenophontos, A. M. Mandalari, Y. Zhao, and H. Haddadi, "PRISM: Privacy Preserving Internet of Things Security Management," arXiv preprint arXiv:2212.14736, 2022.

[91] C.-R. Su, J. Hajiyev, C. J. Fu, K.-C. Kao, C.-H. Chang, and C.-T. Chang, "A novel framework for a remote patient monitoring (RPM) system with abnormality detection," Health Policy and Technology, vol. 8, no. 2, pp. 157-170, 2019.

[92] M. L. Sahu, M. Atulkar, M. K. Ahirwal, and A. Ahamad, "Cloud-based remote patient monitoring system with abnormality detection and alert notification," Mobile Networks and Applications, vol. 27, no. 5, pp. 1894-1909, 2022.

[93] D. Gupta, M. Gupta, S. Bhatt, and A. S. Tosun, "Detecting anomalous user behavior in remote patient monitoring," in 2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI), 2021: IEEE, pp. 33-40.