DOI: http://dx.doi.org/10.26483/ijarcs.v16i4.7320

ISSN No. 0976-5697

Volume 16, No. 4, July-August 2025

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY ON IDENTIFICATION OF ANOMALIES IN IOT SYSTEMS USING AI-DRIVEN MACHINE LEARNING AND DEEP LEARNING METHODS

Dr. Parth Gautam,
Associate Professor,
Department of Computer Sciences and Applications
Mandsaur University, Mandsaur, India

***Abstract*—**The Internet of Things' (IoT) explosive growth has brought previously unheard-of connections to industry, healthcare, smart cities, and smart households. However, the complexity and heterogeneity of IoT environments make them vulnerable to anomalies arising from faults, environmental changes, or malicious activities. For systems to be reliable, secure, and operate well, anomaly detection is essential. In addition to DL architectures like CNNs, RNNs, LSTMs, GRUs, autoencoders, and GANs, supervised, unsupervised, and semi-supervised methods for anomaly detection in Internet of Things (IoT) systems are the main topics of this study's thorough examination of deep learning (DL) and machine learning (ML) models. To improve detection accuracy, reduce false positives, and adapt to shifting assault patterns, it also examines hybrid ML–DL models, which include the best aspects of both theories. This includes discussion of difficulties, including lack of resources, few datasets, interpretability of models, and resistance to hostile attacks. The paper also outlines real-world applications, comparative model analysis, and future research directions, emphasizing lightweight, privacy-preserving, and Scalable methods for anomaly detection in dynamic IoT contexts. Future work will explore integration with 5G, edge computing, and blockchain to enhance adaptability and real-time performance.

***Keywords*—**Internet of Things (IoT), Anomaly Detection, Machine Learning (ML), Deep Learning (DL), Fault Detection, Predictive Maintenance, Real-Time Monitoring

I. INTRODUCTION

The Internet of Things (IoT) has rapidly evolved into a transformative technology that connects billions of devices across a range of sectors, such as smart cities, manufacturing, healthcare, and transportation. Significant volumes of heterogeneous real-time data are continually generated by these networked devices equipped with sensors, actuators, and communication modules. The data is powering intelligent automation, predictive analytics and in-the-moment decisions, making industries more efficient and innovative [1]. Nonetheless, the connectivity that makes IoT so powerful poses risks in its operations [2]. Atypical behaviour, either insidious or unintentional, in terms of hardware, environmental changes, or maliciousness, can seriously affect the services, performance, and safety. To ensure that IoT systems can operate reliably and securely, it is necessary to have methods for identifying and addressing such anomalies before they can cause significant harm.

The anomalies that may appear in IoT systems may be various, namely, sensor faults, performance degradation, system hacking, and targeted attacks like denial-of-service or spoofing [3]. They can be serious with outcomes that include making wrong decisions, equipment failure, or loss of privacy. Detection of these anomalies is the key to performance maintenance, sensitive information protection, and the safety of operations [4]. Nevertheless, the IoT has an underlying issue concerning anomaly detection, which is that it has a very large data dimensionality, information is streaming and continuous, networks are dynamic. Most devices are limited in terms of computational and energy resources. Conventional statistical and rule-based approaches, although adept in simpler settings, tend to fail to keep up with the size, complexity and changing nature of new IoT data sets.

The study of intricate IoT contexts has made artificial intelligence (AI) one of the most important technologies, with the ability of the system to ingest massive amounts of heterogeneous real-time data and detect irregular patterns indicative of faults or security threats as one of the essential aspects of AI, machine learning (ML) [5] has become an effective way to find abnormalities in the normal behaviour through analysing both the historical and real-time data of IoT [6]. Depending on the availability of labelled data, machine learning (ML) can be used in supervised, unsupervised, or semi-supervised ways, each having unique benefits for anomaly detection. Additional capabilities Deep Learning (DL) provides (acting as a specialized subset of ML [7] are automatic extraction of hierarchical feature learning and the ability to capture high-order spatial, temporal and non-linear dependencies in IoT data streams. Hybrid ML-DL middle grounds have become prominent in recent years in attempts to leverage the interpretability of ML, combined with DL's potent feature learning capacity [8]. These group approaches have demonstrated improved detection performance, flexibility to various data sets and robustness to changing attacks. They are therefore a potential avenue to develop resilient, expandable, and smart anomaly detection systems in the context of IoT.

A. Structure of the Paper

The structure of the paper is as follows: Section II presents the basics of IoT systems and the nature of anomalies. Section III talks about machine learning approaches to anomaly detection. In Section IV, deep learning methods are discussed. Section V brings in hybrid ML-DL models and a comparison. In Section VI, a literature review is given. The paper ends with Section VII, which outlines future research directions.

II. ANOMALY DETECTION: IOT SYSTEMS

In IoT systems, anomaly detection involves finding unusual or unusual features in data generated by networked devices such as sensors and actuators. These deviations can be a sign of faults or security issues or unanticipated changes in the environment that can impact the dependability and security of IoT solutions across several fields, including smart homes, healthcare, and industrial automation.

A. *Anomalous Behavior in IoT Systems*

The Internet of Things (IoT) is a vast and diverse network of interconnected computers that automatically collects, shares, and analyses data using sensors, actuators, and communication technologies. Intelligent homes, healthcare, industrial automation, and intelligent cities are just a few of the numerous industries that employ these technologies [9], which can monitor and control in real time. In general, the architecture of the IoT may be divided into many layers: the perception layer, which consists of sensors and actuators with direct external connections, the network layer, which facilitates data transmission via Wi-Fi, Bluetooth, and cellular networks; the processing layer, which collects and processes data using cloud or edge computing; and the application layer, which offers a range of services tailored to end-user needs.

IoT systems often face abnormal behaviours, which jeopardise their performance and security, despite their potential to provide transformational outcomes. Such anomalies can be caused by sensor failures, communication interference, program errors, environmental noises and malicious cyber actions like spoofing and denial-of-service attacks. These irregularities might cause inaccurate data [10], connectivity loss, or system compromise of operations, which translates to the unreliability and safety of IoT applications [11]. Given the heterogeneity of IoT devices and the resource limitations inherent in many of them—such as constrained processing power and energy—detecting and managing these anomalies becomes a complex challenge.

Anomaly detection is extensively utilised in many different applications, such as cybersecurity detection of intrusions, detection of vulnerabilities in safety-critical systems, military monitoring of hostile activities, and detection of medical, insurance, or credit card fraud [12]. Anomalies are patterns in data that differ from a well-defined concept of usual behaviour. Demonstrates irregularities in a simple 2-dimensional data collection (Figure 1). There are two typical zones in the data since most observations fall inside them N1 and N2. Anomalies are spots that are sufficiently remote from the areas, for example, O1 and O2 areas, as well as O3 regions.

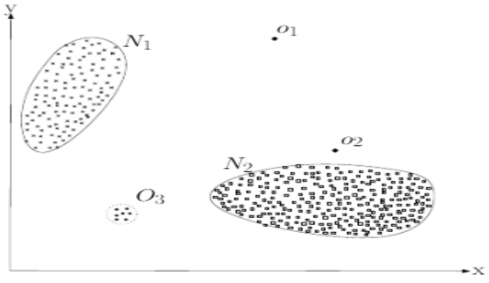

Fig. 1. A Simple Example of Anomalies in A 2-Dimensional Data Set

B. *Classification of Anomalies*

Anomalies in IoT systems are generally categorised into three main types: abnormalities that are communal, contextual, and point. Each type represents a distinct pattern of abnormal behaviour and poses unique detection challenges. Understanding this classification is essential for developing effective anomaly detection methods tailored to the diverse scenarios found in IoT environments. The detailed characteristics and examples of these anomaly types are discussed below:

1) *Point Anomaly*

A data instance that differs substantially from all or most other data points in a dataset is considered an anomaly [13]. A fundamental method in anomaly identification is point anomalies, or deviations in individual data points, which show isolated abnormalities without considering the relationships between variables. An abrupt increase in packet loss rate, for example, would be considered abnormal if it were based just on the feature's departure from the norm. Figure 2 visualizes a point anomaly, showing an isolated data point that substantially departs from the primary data distribution:

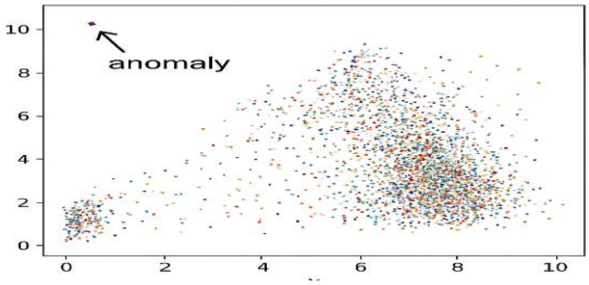

Fig. 2. Point Anomaly

2) *Contextual Anomaly*

In a use case, contextual abnormalities can be identified, such as electricity usage, which probably has time-related, context-based correlations. These anomalies happen when a data point appears normal in several contexts but is abnormal in one. Figure 3 is the Illustration of a contextual anomaly, where an unexpected deviation occurs within an otherwise regular sinusoidal pattern.

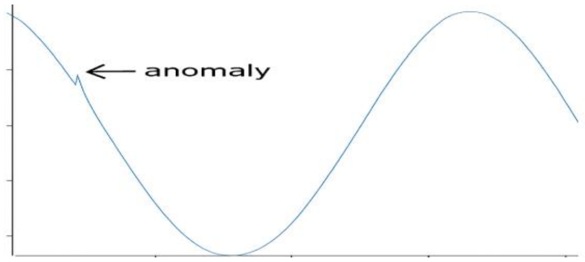

Fig. 3. Contextual Anomaly

3) *Collective Anomaly*

Collective anomaly is one of the anomaly types that shows aberrant group distributions over a certain period. These happen when a large number of continuous data points exhibit aberrant behaviour, even when they do so simultaneously and in opposition to other individual points. Linking particular places and including temporal periods with that specific point or occurrence results in a more thorough viewpoint and aids in the development of an overall understanding of the event, even though a single event or point location might not help classify the fundamental problem in locating group abnormalities across several datasets [14]. Identifying group anomalies in actual datasets becomes extremely difficult due to diverse distributions and densities. A collective anomaly is seen in Figure 4, when a collection of data points collectively behaves abnormally even though the individual points seem normal.

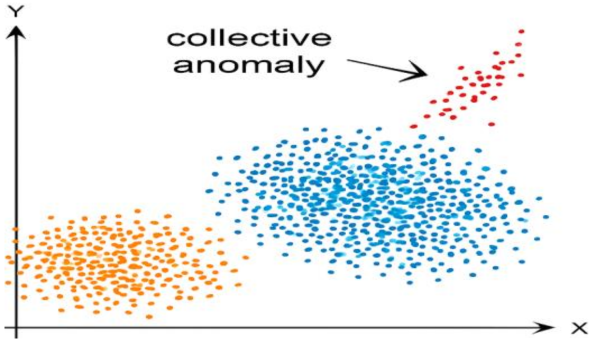

Fig. 4. Collective Anomaly

C. *Challenges in Anomaly Detection in Iot*

Several issues hinder the development of anomaly detection methods in the Internet of Things context, such as (1) a deficiency of IoT resources, (2) the challenge of identifying typical behaviours, (3) the dimensionality of data, (4) context information, and (5) the lack of reliable machine learning models. This section explains these factors.

1) *Scarcity of IoT Resources*

Device-level IoT anomaly detection could not be as effective because of constraints on power, connectivity, processing, and storage [15]. The use of the cloud as a platform for data collecting, processing, and storage can make up for this. However, the round-trip time and resource allocation caused by the cloud's distance might result in a major delay. This delay might not be permissible for the real-time requirements of suspicious IoT events.

2) *Profiling Normal Behaviours*

It is difficult to define regular activities, yet collecting enough information on the efficacy of an anomaly detection system depends on typical behaviors. Owing to their infrequent frequency, abnormal behaviors may be grouped with typical behaviors. For heavily deployed IoT devices in particular, supervised learning is not feasible due to a scarcity of datasets that cover both normal and aberrant IoT data.

3) *Dimensionality of Data*

IoT data can be multivariate (e.g., temporally correlated univariate xt = [xt1,...,]) or univariate (key-value xt). Current data is compared against previous time series to find anomalies in the Internet of Things, utilising univariate series. Multivariate-based detection, on the other hand, offers correlations between qualities at a certain moment as well as previous stream associations.

4) *Context Information:*

To detect anomalies, context information is provided by the dispersed nature of IoT devices. In big IoT deployments, when certain IoT devices act as mobile, capturing geographic contextual and temporal information at time $t1$ is connected to input at time tn. Therefore, adding context improves anomaly detection systems; yet, if the right context is not recorded, complexity rises.

5) *Lack of ML Models' Resiliency Against Adversarial Attacks:*

It is necessary to have both accurate algorithms and robust models since current machine learning models have a high false-positive rate and are vulnerable to hostile attacks while being trained and detected.

III. Machine Learning Approaches

Artificial Intelligence (AI), which enables sophisticated data analysis and pattern recognition, has emerged as a key facilitator in IoT system optimization and security. The reliability, security, and safety of complex IoT settings are improved by machine learning (ML), a core field of artificial intelligence, which is essential for spotting odd trends in IoT data streams. When given labelled data, two supervised learning methods that are useful for identifying normal and pathological behaviors are support vector machines (SVM) and decision trees. The hidden irregularities in data that are discovered with the help of unsupervised methods, such as clustering algorithms and autoencoders, do not need prior labels and can be especially useful, considering the frequently unlabeled character of IoT data. The semi-supervised models are employed based on small portions of the annotated data and large quantities of unlabeled data to increase further accuracy in detection. IoT systems enabled by the application of AI-driven machine learning processes can achieve early fault detection, predictive maintenance, and timely discovery of security threats to have continuous and reliable operation even in the most dynamic and highly heterogeneous environments.

A. *Supervised Learning Methods*

In supervised learning, learn to map a collection of input variables to an output variable and then use that mapping to forecast the behavior of unseen data on the fly. A well-known supervised learning technique for resolving problems with regression and classification is the support vector machine (SVM). Based on the idea of margin calculation, this approach divides n-dimensional space into distinct classes by determining the best decision boundary, known as the hyperplane. This is putting future data points into the appropriate categories. Among SVM's benefits is its capacity to process both structured and semi-structured data. It also reduces the likelihood of overfitting because it uses generalization. SVM, however, has several drawbacks as well. There is an increase in training time with huge datasets. Consequently, its performance starts to decline.

B. *Unsupervised Learning Methods*

In the field of ML known as "unsupervised learning," algorithms examine and interpret data without the use of labels or predetermined results. In contrast to supervised learning, it finds underlying patterns, structures, or connections in the raw data rather than depending on labelled training instances. A significant amount of data is needed for unsupervised machine learning. Four types of unsupervised learning barriers may be distinguished, as shown in Figure 5 issues with autoencoders, association, anomaly detection, and clustering. The method can be used to detect unseen attributes or clusters in models, and thus can be applied to interpret complicated data in instances when clear instructions are not provided. Unsupervised learning assists in finding insights and arranging the data in meaningful forms, and this is particularly important in cases when labelling is costly or impractical. It is used as a platform for tasks such as data exploration, anomaly detection, and feature learning.

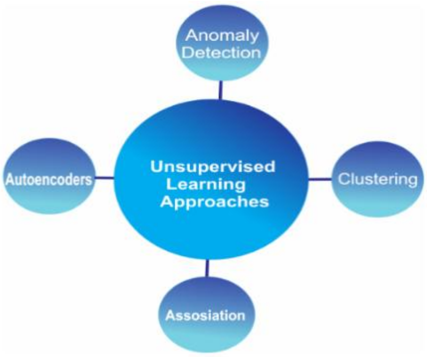

Fig. 5. Types of Unsupervised Learning

C. *Types of Unsupervised Learning:*

Unsupervised learning includes several methods that let models find hidden structures and patterns in data without depending on results that have been labelled.

1) Clustering

The practice of grouping or categorising items is called clustering or cluster analysis. There are several kinds of clustering, including partitioning, overlapping, probabilistic, and hierarchical. The splitting of the data may mean that each piece of information belongs to just one cluster. Exclusive pooling is another term for this practice. K-means is an excellent example of partitioning.

2) Association

An unsupervised learning method called Association Rule Learning (ARL) is used to identify correlations between variables in big datasets. Unlike many machine learning techniques, ARL can take non-numeric data points. To put it briefly, ARL is interested in the relationships between certain variables. A helmet is more likely to be purchased by someone who buys a motorbike, for instance. Building these sorts of relationships can lead to financial gain. Assume that consumers who purchase product X also purchase product Y, and that an internet merchant can suggest product Y to any client who buys product X.

3) Anomaly Detection

Anomaly detection is any process that finds outliers in a set of data. A malfunctioning sensor, odd network activity, or data that requires cleansing before analysis might all be the cause of these abnormalities. An anomaly occurs when data models exceed or deviate from standard models. For instance, an odd network traffic pattern suggests that the infected machine is sending private information to an unapproved destination.

4) Autoencoders

Auto encoders are an unsupervised learning technique that performs representation learning using neural networks. A bottleneck that forces It will be included in the neural network architecture to use a reduced knowledge representation of the original input [16]. If there were no relationship between the input characteristics, this compression and the reconstruction that followed would be difficult.

D. *Semi-Supervised Learning (SSL)*

In a machine learning approach known as semi-supervised learning, a significant proportion of unlabelled data is combined with a small amount of labelled data throughout the training process. When labelling data is expensive or time-consuming, this method uses the structure and patterns of the unlabelled data to improve model performance. Semi-supervised learning improves accuracy without requiring large labelled datasets by bridging the gap between supervised and unsupervised learning through the use of both labelled and unlabelled samples. It is extensively used in domains where acquiring labelled data might be difficult, but unlabelled data is plentiful, such as bioinformatics, picture recognition, and natural language processing.

IV. DEEP LEARNING APPROACHES

In several application domains, including anomaly detection in IoT systems, DL, a subset of ML, has gained popularity. ML is comparable to a newborn baby's learning process. In the human brain, billions of interconnected neurons activate in response to stimuli. For instance, a particular sequence of neurons fires when a newborn sees a car for the first time. Later, when shown a different model of the vehicle, the brain activates the original neurons along with additional ones to recognize the variation. Similarly, deep learning models in IoT systems adapt and refine their internal connections as they are exposed to diverse data patterns, enabling them to identify both known and novel anomalies. This adaptive learning process is critical for handling the complex and dynamic data generated by IoT devices, improving anomaly detection accuracy and system resilience [17].

A. *Recurrent Neural Network*

To handle sequential data, RNNs are made to remember past inputs in a hidden state. The basic design consists of three layers: input, hidden, and output. Figure 6 illustrates how recurrent connections, as opposed to feed-forward neural networks, enable information to cycle inside the networks.

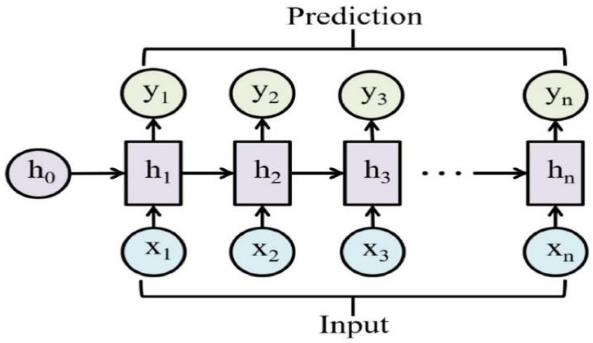

Fig. 6. Basic RNN Architecture.

B. *Long Short-Term Memory Networks (LSTM)*

To overcome the vanishing gradient problem that basic RNNs suffer, Hochreiter and Schmidhuber created LSTM networks. As the primary innovation of LSTM, gating techniques are used to control the information flow across the network [18]. LSTM networks are useful for problems involving the modelling of long-term dependencies because of their capacity to preserve and update their internal state over extended periods. Three gates are located inside each LSTM cell: input, forget, and output. These gates control the hidden state $\mathbf{h}t$ and the cell state $\mathbf{c}t$ (shown in Figure. 7).

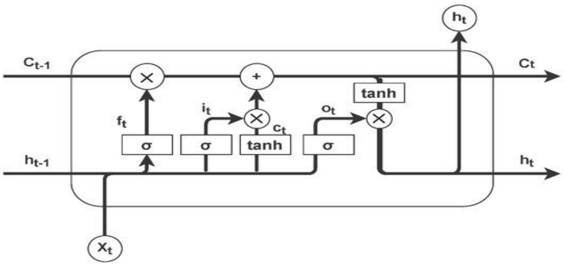

Fig. 7. Architecture of the LSTM Network.

C. *Gated Recurrent Units(GRU)*

To solve the vanishing gradient issue and simplify the LSTM architecture, gated recurrent units are an additional variation [19]. Developed by Cho et al., GRUs simplify the model and boost its computational performance by lowering the number of gates and parameters. They do this by unifying the cell state and concealed state and creating a single update gate by merging the input and forget gates. The GRU structure consists of two gates (Figure 8).

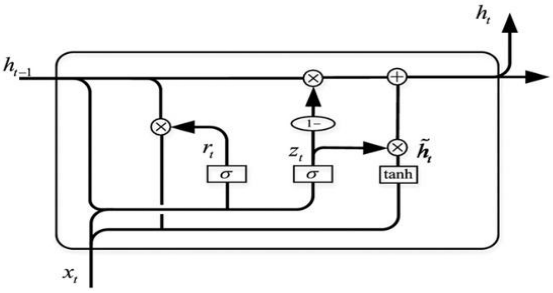

Fig. 8. Architecture of the GRU Network.

D. *Convolutional Neural Networks (CNNs)*

Multi-layer AI systems called CNNs can distinguish, identify, and categorise objects in pictures, in addition to detecting and segmenting them [20]. In reality, CNN—also known as ConvNet—is a well-liked discriminative deep learning architecture that doesn't require human feature extraction and can be trained directly from the input object. Because this network is particularly made to handle a variety of 2D forms, it is widely utilised in visual recognition, medical image analysis, image segmentation, natural language processing, and many other applications. Understanding the different CNN components and how they are used is essential to understanding the evolution of CNN architecture.

E. *Generative Adversarial Networks (GANs)*

GANs are now a state-of-the-art method for generating gene expression data. Sample variability, scarce data, and high complexity are some of the inherent issues with gene expression research that GAN can tantalizingly resolve. This algorithm can produce generated data that mimics real-life data.

This study's main objective is to increase the variety of gene expression data that is accessible by creating synthetic data, which offers an advanced alternative to traditional data augmentation or sampling techniques. GANs are helpful because they can capture and simulate the non-linear distributions seen in gene expression data and provide a more realistic and compelling synthetic dataset than these traditional methods, which may misrepresent the underlying statistical distribution of data.

V. Machine Learning And Deep Learning Techniques For Anomaly Detection In IoT Systems

The combination of machine learning (ML) and deep learning (DL) is useful in IoT anomaly detection. ML is more interpretable, suitable for smaller datasets, whereas DL is great for complex and high-dimensional data that requires automatic feature learning. The hybrid models combine the advantages of both DL and ML, where characteristics are extracted using the former and then classified using the latter to improve outcomes, reduce false positives, and utilize fewer resources. The methods have been put into practice in the practical realms of IoT, including smart homes, smart grids, and smart businesses, to detect issues and improve security. A comparative analysis reveals that hybrid models can offer an optimal mediation of performance, efficiency and adaptability to various IoT situations.

A. *Overview of Combined ML and DL Approaches*

In the context of the Internet of Things, anomaly detection engineering has shown potential using both machine learning and deep learning approaches. These techniques may reach high levels of detection efficiency and accuracy and often work in tandem. Although the traditional methods of ML are powerful in cases of limited data and interpretable models, DL is ideal for managing massive amounts of intricate, high-dimensional IoT data because of its capacity to automatically extract hierarchical features. By combining their strengths, ML and DL techniques work together to address the difficulties presented by IoT contexts. As an example, the first stage of feature selection and dimensionality reduction may use ML algorithms and make the input more manageable for subsequent DL models. On the contrary, DL models can be employed to provide rich, abstract feature representations that are fed into ML classifiers to make the final decisions on anomaly detection.

Hybrid models frequently imply stacking or cascading ML and DL models and allow detecting more potent known and unseen anomalies. It is especially useful in the context of IoT systems [21], where heterogeneity, volume, and velocity of data differ widely on different network sensors and devices. Additionally, these methods, when combined, represent the best solution to the ever-changing nature of attacks and the environment, especially in dynamic IoT networks, where anomaly detection and reaction happen instantly. This kind of collaboration enhances detection performance and aids in reducing false positive detections, a problem that arises naturally in IoT anomaly detection. Combining ML and DL is an intriguing trend towards developing anomaly detection systems that can handle the particular needs of IoT applications while being more accurate, scalable, and reliable.

B. *Hybrid Models: Leveraging Strengths of ML and DL*

Hybrid models, which integrate ML and DL approaches, are an efficient way to find anomalies in an IoT system. Such models harness the strengths of each paradigm in an integrated manner, beyond the weaknesses of either, to improve detection performance, robustness, and computational efficiency.

Traditional ML techniques, such as Random Forests and Support Vector Machines (SVM), provide great performance with less data, strong interpretability, and lower processing needs. They may find it difficult to manage the complex and high-dimensional nature of IoT data, though, and typically need manual feature engineering. As an alternative, DL models [22] represent intricate temporal and spatial connections and learn representative hierarchical features directly from raw data. Examples of these are autoencoders, long short-term memory networks (LSTMs), and convolutional neural networks (CNNs). Yet, DL methods usually need large labeled datasets and significant computing resources, which may not always be practical in many IoT environments.

Hybrid models effectively address these challenges by combining ML and DL components in complementary ways. Generally, deep learning models are first employed for automated feature extraction or representation learning from raw IoT sensor data [23]. These extracted features are then input into traditional machine learning classifiers to perform anomaly detection with improved accuracy and interpretability. Some notable hybrid models widely applied in IoT anomaly detection include:

- **Autoencoder + Support Vector Machine (SVM):** Raw IoT data is compressed into a lower-dimensional representation via an autoencoder is a type of neural network that uses input data reconstruction to learn features without supervision. The SVM classifier then uses these learned features to identify anomalies. This approach harnesses the feature extraction capability of DL with the strong classification ability of SVM, yielding high detection performance.
- **Convolutional Neural Network (CNN) + Random Forest:** Spatial feature extraction from multi-dimensional sensor data streams is a strength of CNNs. Random Forest classifiers use these acquired characteristics as inputs, which leverage ensemble decision trees to robustly classify anomalous behaviours in IoT networks.
- **Long Short-Term Memory (LSTM) + K-Nearest Neighbours (KNN):** LSTM networks are specialised recurrent neural networks that identify long-term temporal connections in sequential IoT data. The learned temporal features can then be fed to a KNN classifier, which detects anomalies by comparing new data points to known normal instances.

These hybrid designs improve anomaly detection accuracy and recall while simultaneously optimising computing resource use by partitioning activities into DL and ML modules, and are comparatively better than ML and DL hybrid, as shown in the table below. ML, DL, and hybrid models are compared in Table I based on key elements relevant to anomaly detection in IoT systems.

TABLE I. COMPARATIVE ANALYSIS OF MACHINE LEARNING, DEEP LEARNING, AND HYBRID MODELS FOR ANOMALY DETECTION IN IOT SYSTEMS

Aspect	Machine Learning	Deep Learning	Hybrid Models
Data Size	Works well with small/moderate	Needs large datasets	Flexible with data size
Feature Learning	Manual feature engineering	Automatic feature extraction	Combines both methods
Anomaly Detection	Detects known anomalies	Detects known & unknown anomalies	Improved detection accuracy
Computational Complexity	Low to moderate	High computational cost and longer training time	Moderate; balances computation between ML and DL
Model Interpretability	High; easier to understand	Low; often considered black-box models	Improved interpretability via ML components
Detection Accuracy	Good for simple patterns; limited for complex data	High accuracy on complex temporal/spatial patterns	Improved accuracy and robustness
Adaptability to Data Drift	Moderate; requires retraining	Better adaptability with continual learning setups	High adaptability when designed effectively

This comparison shows the trade-offs between the complexity of the models, accuracy, interpretability, and adaptability. It can be used to inform the choice of suitable methods depending on the scenario of IoT anomaly detection.

C. *Real-World Applications*

In many real-world industries, anomaly detection may play a crucial role in enhancing the IoT systems' dependability, security, and efficacy. The section identifies several important applications and major case studies involving the successful use of ML, DL, and hybrid models.

- **Smart Homes and Buildings:** IoT sensors can track environmental conditions, energy consumption and security [24]. Such ML algorithms as Isolation Forest and SVM identify abnormal malfunctions or invalid access to the device. Further enhancement in detection accuracy is achieved by hybrid models that incorporate autoencoders and Random Forests that recognise the subtle anomalies.
- **Industrial IoT (IIoT):** In the manufacturing context, sensors are used to monitor equipment and process variables to facilitate predictive maintenance. LSTMs and other DL models are well-suited for modeling the temporal data of sensors to provide early fault diagnosis. Hybrid schemes where DL algorithms are used to extract features in combination with ML at the classifier stage lead to an improvement in the classification of anomalies and minimization of false alarms.
- **Smart Grids and Energy:** Sensors IoT are used to monitor the performance of the grid and energy consumption. ML detects unusual use and malicious activity, whereas DL autoencoders detect new faults and cyberattacks. Hybrid solutions are those that are fast response and flexible to changing grid conditions.

VI. LITERATURE REVIEW

Recent researches point out the crucial importance of ML and DL in enhancing the accuracy and scalability of anomaly detection in IoT, along with the necessity of lightweight and privacy-preserving models to address the resource limitations and changing security issues.

Lim and Prum's (2025) article on how the number of IoT devices has been exponentially increasing in the realm of healthcare, smart cities, and industrial automation projects, complicating security concerns and making old detection methods inefficient on dynamic, heterogeneous networks. This study offers a thorough analysis of ML approaches, including federated learning, DL, and conventional methods, for anomaly identification in IoT networks. Critically assess their effectiveness, emphasizing IoT-specific challenges such as resource constraints, scalability, and concept drift. Additionally, the paper discusses recent advancements like lightweight ML models and privacy-preserving methods, including federated learning, which show potential for enhancing deployment in IoT environments. It expands the dataset review with recent, underrepresented datasets related to emerging IoT technologies and connects future research to trends such as 5G integration and privacy preservation. [25]

Shibu et al. (2025) highlight that with Many intelligent applications are appearing in this era due to the development of IoT devices. Specifically, many countries have adopted and realized smart cities. In these smart cities, vast amounts of data are generated every second, necessitating a wireless transmission medium. However, security remains a primary concern, as smart transmissions are often associated with anomalies. The accuracy of current anomaly detection systems has to be improved since feature extraction and selection procedures are inefficient. This study presents an accurate DL-based anomaly detection technique. For anomaly identification, present the Combined Deep Q-Learning (CDQL) method. Initially, the Spider Monkey Optimizer (SMO) is used to choose the best characteristics. These ideal characteristics enable CDQL to identify abnormalities with accuracy. To monitor network data, the CDQL algorithm also continually learns its surroundings. When paired with ideal characteristics, this continuous monitoring raises accuracy to 98% [26].

Rafique et al. (2024) propose that the IoT's rapid expansion has resulted in unprecedented numbers of connections and data. An essential security component is anomaly detection, which finds situations in which system behavior deviates from expected norms and enables the prompt identification and addressing of abnormalities. IoT systems' dependability, effectiveness, and integrity are improved when AI and IoT are combined to enhance anomaly detection. In IoT environments, AI-based anomaly detection systems may detect a variety of threats, including back-door vulnerabilities, replay assaults, buffer overflow, brute force, injection, DDoS attacks, and SQL injection. For IoT devices, IIDSs, or IDSs, are crucial, aiding in the detection of anomalies or intrusions within networks, especially as IoT is increasingly utilized across industries, presenting a wide attack surface with many places for attackers to enter. This study examines the research on using ML and DL to detect anomalies in IoT infrastructure [27].

Alghaithi (2024) discusses the IoT or the chain of connected devices which collect data from many sources. As the IoT networks grow, anomalies may occur due to other sources such as intrusion detection systems, data leakage and fraud detection. Such deviations may negatively impact the performance of the systems, resulting in major problems. ML is a crucial step in IoT anomaly detection since it uses advanced algorithms to find previously unidentified patterns in massive datasets. IoT sensor data may be improved by prediction and pattern recognition utilizing DL algorithms, which boost IoT system efficiency. The study examines at novel methods for IoT network anomaly detection. Using various datasets, the proposed study evaluates ML and DL approaches to determine the best ways to address certain abnormalities [28].

Atassi (2023) The paper discusses how the proliferation of IoT devices has led to technological advancements and incredibly strong connections. Fast intrusion detection systems are required, nevertheless, because this interconnected ecosystem creates new security risks. This research uses cutting-edge ML techniques to present a thorough analysis of anomaly detection on IoT networks. The Gated Recurrent Unit (GRU) architecture is carefully used to identify temporal relationships in IoT communications. In addition, are promoting scalability and privacy across dispersed IoT devices by employing hierarchical federated training. Our method uses openly accessible IoT data, which would allow for a comprehensive evaluation of the models' adaptability. These results demonstrate that our GRU-based model is capable of detecting a wide range of threats, including SQL assaults and Distributed Denial of Service (DDoS) attacks [29].

Abusitta et al. (2023) recommend an IoT system anomaly detection system based on DL that has the capability of learning and obtaining strong features that are not highly influenced by unstable environments. A denoising autoencoder was used in the development of this model to produce characteristics that are less vulnerable to the diverse IoT environment. In contrast to the most sophisticated IoT-based anomaly detection methods, the suggested framework improves the precision of identifying false data. Since data collected with IoT devices is diverse and the system is susceptible to disruptions, finding anomalous activity and compromised nodes is more challenging than in standard IT networks. The suggested model aims to make sure that malicious data is not disseminated through the IoT-driven decision support systems [30].

Table II presents a survey of the literature on ML and DL models for detecting anomalies in IoT systems, arranged by reference, topic, main conclusions, difficulties, gaps, and future research

TABLE II. LITERATURE REVIEW SUMMARY OF MACHINE LEARNING AND DEEP LEARNING MODELS FOR IOT ANOMALY DETECTION

Reference	Focus Area	Key Findings	Challenges	Limitations and Gaps	Future Work
Lim and Prum (2025)	IoT anomaly detection with ML/DL and federated learning	Comprehensive review of traditional, DL, federated learning; lightweight models and privacy important	Resource constraints, scalability, concept drift, privacy	Lack of lightweight models for IoT; underrepresented datasets; integration with 5G; trade-offs in privacy	Develop lightweight, privacy-preserving models; explore 5G impact
Shibu et al. (2025)	Anomaly detection using DL in IoT smart cities	Combined Deep Q-Learning with feature optimization improves accuracy up to 98%	Feature extraction and selection affect detection accuracy	Limited generalizability; focused on specific optimization method	Extend feature selection methods; apply to broader IoT scenarios

Rafique et al. (2024)	Examination of anomaly detection using AI	AI improves detection of wide range of attacks; real-time testing and scalability critical	Real-time deployment; scalability; dataset variety	Insufficient real-time validation and scalable systems	Develop scalable, real-time systems using diverse datasets
Alghaithi et al. (2024)	Examination of ML and DL methods for identifying irregularities in the IoT	DL can analyze sensor data to improve IoT system efficiency	Selecting appropriate ML/DL methods; dataset diversity	Lack of guidance on best models for different anomaly types	Investigate model suitability for diverse anomalies
Atassi (2023)	GRU-based DL with federated learning for IoT anomaly detection	GRU with hierarchical federated training enhances scalability and privacy	Data heterogeneity; privacy preservation	Limited federated learning research in IoT anomaly detection	Further exploration of federated learning; testing on diverse datasets
Abusitta et al. (2023)	Denoising autoencoder DL model for IoT anomaly detection	Model robust against noisy, heterogeneous IoT data; improves malicious data detection	IoT data heterogeneity; noisy environments	Validation limited to few datasets; handling extreme heterogeneity	Broaden dataset validation; enhance robustness for heterogeneous data

VII. Conclusion And Future Work

Techniques for ML and DL are becoming increasingly important for improving the security, dependability, and effectiveness of IoT systems. These methods enable the timely detection of anomalies arising from hardware faults, performance degradation, network disruptions, or malicious activities. Interpretability and adaptability to diverse IoT contexts are provided by supervised, unsupervised, and semi-supervised ML techniques, which provide flexibility in managing various data availability conditions. DL architectures such as CNNs, LSTMs, GRUs, and autoencoders can automatically extract intricate temporal and geographical patterns from high-dimensional IoT data streams. Hybrid ML–DL models combine these strengths, increasing detection precision, decreasing false positives, and enhancing flexibility in response to changing operational and cyber threats. Their proven effectiveness in industrial IoT, smart grids, and smart home applications highlights their potential to reduce downtime, prevent service interruptions, and safeguard critical infrastructure.

Future work should prioritize lightweight, energy-efficient models for resource-constrained devices and privacy-preserving approaches like federated learning. Expanding diverse datasets will improve model robustness, while integration with Scalability and real-time responsiveness may be improved by new technologies like edge computing and 5G. These steps will be key to building secure, efficient, and future-ready IoT ecosystems.

References

[1] B. Sharma, L. Sharma, and C. Lal, “Anomaly detection techniques using deep learning in IoT: a survey,” in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp. 146–149.

[2] R. Patel, “Artificial Intelligence-Powered Optimization of Industrial IoT Networks Using Python-Based Machine Learning,” ESP J. Eng. Technol. Adv., vol. 3, no. 4, pp. 138–148, 2023, doi: 10.56472/25832646/JETA-V3I8P116.

[3] D. D. Rao et al., “Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis,” J. Intell. Syst. Internet Things, vol. 24, no. 2, 2024, doi: 10.54216/JISIoT.120215.

[4] 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.

[5] N. Prajapati, “The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications,” ESP J. Eng. Technol. Adv., vol. 5, no. 2, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[6] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, “Anomaly-based intrusion detection system for IoT networks through deep learning model,” Comput. Electr. Eng., vol. 99, Apr. 2022, doi: 10.1016/j.compeleceng.2022.107810.

[7] R. Q. Majumder, “Machine Learning for Predictive Analytics : Trends and Future Directions,” Int. J. Innov. Sci. Res. Technol., vol. 10, no. 4, 2025.

[8] S. Varalakshmi, P. S P, Y. V, V. P, V. R. Kavitha, and V. G, “Design of IoT Network using Deep Learning-based Model for Anomaly Detection,” in 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Nov. 2021, pp. 216–220. doi: 10.1109/I-SMAC52330.2021.9640700.

[9] S. Kumari, C. Prabha, A. Karim, M. M. Hassan, and S. Azam, “A Comprehensive Investigation of Anomaly Detection Methods in Deep Learning and Machine Learning: 2019–2023,” IET Inf. Secur., vol. 2024, no. 1, Jan. 2024, doi: 10.1049/2024/8821891.

[10] Z. Ahmad et al., “Anomaly Detection Using Deep Neural Network for IoT Architecture,” Appl. Sci., vol. 11, no. 15, 2021, doi: 10.3390/app11157050.

[11] K. M. R. Seetharaman, “Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges,

and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, Mar. 2021, doi: 10.48175/IJARSCT-6268B.

[12] S. A. Pahune, P. Matapurkar, S. Mathur, and H. Sinha, "Generative Adversarial Networks for Improving Detection of Network Intrusions in IoT Environments," 2025 4th Int. Conf. Distrib. Comput. Electr. Circuits Electron., pp. 1–6, 2025, doi: 10.1109/ICDCECE65353.2025.

[13] P. Schummer, A. del Rio, J. Serrano, D. Jimenez, G. Sánchez, and Á. Llorente, "Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation," AI, vol. 5, no. 4, pp. 2967–2983, Dec. 2024, doi: 10.3390/ai5040143.

[14] A. Feroze, A. Daud, T. Amjad, and M. K. Hayat, "Group Anomaly Detection: Past Notions, Present Insights, and Future Prospects," SN Comput. Sci., vol. 2, no. 3, p. 219, May 2021, doi: 10.1007/s42979-021-00603-x.

[15] A. Diro, N. Chilamkurti, V.-D. Nguyen, and W. Heyne, "A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms," Sensors, vol. 21, no. 24, p. 8320, Dec. 2021, doi: 10.3390/s21248320.

[16] S. Naeem, A. Ali, S. Anam, and M. Ahmed, "An Unsupervised Machine Learning Algorithm: Comprehensive Review," Int. J. Comput. Digit. Syst., vol. 13, no. 1, pp. 911–921, Apr. 2023, doi: 10.12785/ijcds/130172.

[17] M. M. Taye, "Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions," Computers, vol. 12, no. 5, p. 91, Apr. 2023, doi: 10.3390/computers12050091.

[18] A. Gökdemir and A. Calhan, "Deep learning and machine learning based anomaly detection in Internet of Things environments," J. Fac. Eng. Archit. Gazi Univ., vol. 37, no. 4, pp. 1945–1956, 2022.

[19] I. D. Mienye, T. G. Swart, and G. Obaido, "Recurrent Neural Networks: A Comprehensive Review of Architectures, Variants, and Applications," Information, vol. 15, no. 9, p. 517, Aug. 2024, doi: 10.3390/info15090517.

[20] M. M. Taye, "Theoretical Understanding of Convolutional Neural Network: Concepts, Architectures, Applications, Future Directions," Computation, vol. 11, no. 3, p. 52, Mar. 2023, doi: 10.3390/computation11030052.

[21] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," Internet of Things, vol. 7, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[22] L. Aversano, M. L. Bernardi, M. Cimitile, R. Pecori, and L. Veltri, "Effective Anomaly Detection Using Deep Learning in IoT Systems," Wireless. Commun. Mob. Comput., vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/9054336.

[23] H. S. Chandu, "Enhancing Manufacturing Efficiency : Predictive Maintenance Models Utilizing IoT Sensor Data," IJSART, vol. 10, no. 9, pp. 58–66, 2024.

[24] H. S. Chandu, "A Review of Iot-Based Home Security Solutions : Focusing on Arduino Applications," TIJER, vol. 11, no. 10, 2024.

[25] K. Lim and S. Prum, "Machine Learning Approaches for Anomaly Detection in IoT Networks: A Survey," 2025.

[26] S. Shibu *et al.*, "Anomaly detection using deep learning approach for IoT smart city applications," *Multimed. Tools Appl.*, vol. 84, no. 17, pp. 17929–17949, 2025.

[27] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends," *Sensors*, vol. 24, no. 6, 2024, doi: 10.3390/s24061968.

[28] H. R. O. Alghaithi, M. M. A. M. Alshehhi, and T. Murugan, "IoT Network Anomaly Detection Using Machine Learning and Deep Learning Techniques - Research Study," in *2024 IEEE Students Conference on Engineering and Systems (SCES)*, 2024, pp. 1–6. doi: 10.1109/SCES61914.2024.10652305.

[29] R. Atassi, "Anomaly Detection in IoT Networks: Machine Learning Approaches for Intrusion Detection.," *Fusion Pract. \& Appl.*, vol. 13, no. 1, 2023.

[30] A. Abusitta, G. H. S. de Carvalho, O. A. Wahab, T. Halabi, B. C. M. Fung, and S. Al Mamoori, "Deep learning-enabled anomaly detection for IoT systems," *Internet of Things*, vol. 21, p. 100656, 2023, doi: https://doi.org/10.1016/j.iot.2022.100656.