Volume 12, No.10, October 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

UGC Approved Journal

RESEARCH PAPER

Available online at http://www.jgrma.info

DEEP LEARNING APPROACHES FOR REAL-TIME ANOMALY IDENTIFICATION DETECTION IN IOT SENSOR NETWORKS: A REVIEW

Dr. Nilesh Jain[1]

[1] Associate Professor, Mandsaur University, Mandsaur, Department of Computer Sciences and Applications
nileshjainmca@gmail.com

Abstract: IoT sensor networks are becoming increasingly dependent on real-time anomaly detection and predictive analytics technology to analyze continuous data streams in order to make trustworthy decisions in a timely manner. Deep learning offers advanced techniques that can handle the scale and complexity of such data more effectively than traditional methods. This paper gives a complete picture of how IoT-based predictive analytics and anomaly detection are enhanced using deep learning. The capability of extracting hierarchical information, modelling temporal-spatial relationships, and identifying subtle anomalies in real-time is displayed by models like the autoencoders, generative adversarial networks (GANs), transformers, etc. These methods enhance the accuracy of forecasting, the system's resilience, and its adaptability across many domains, such as healthcare, industrial IoT, and smart infrastructure. Despite this, and especially given scalability, computational requirements, and the limited availability of labelled data, key challenges remain. Addressing these issues is critical in ensuring strong deployment in resource constrained IoT systems. Future directions include light-weight architectures, privacy-preserving learning and explainable models to drive towards the reliability and intelligence of IoT driven applications.

Keywords: IoT sensor networks, anomaly detection, predictive analytics, deep learning, autoencoders, real-time analytics.

1 INTRODUCTION

The term "internet of things" (IoT) means a network of connected computing devices, services, and physical things that are able to collect, process, and share information. The "internet of everything" or IoT is a paradigm shift that bridge the gap between the digital and physical world through an interconnected system of computers, sensors, the internet, and the Internet of Things, the Internet of physical things, or connectivity, wireless, and RFIs, embedded systems and communication technologies [1] [2]. Any hardware, software or sensors can be a part of the system approach. Internet of Things (IoT) helps to manage security and data. The Internet of Things (IoT) is the remote connection of devices and people [3]. Acute stress, smart buildings, smart cities and vehicle-to-vehicle reaction are only a couple of examples of the numerous possible applications of the Internet of Things.

Predictive analytics has become a very important aspect in the age of big data and Internet of Things (IoT) as a technique that has the potential to radically change an organization's strategies for problem-solving, decision-making and increasing productivity [4]. The proliferation of Internet of Things (IoT) devices in numerous sectors has led to the accumulation of huge amounts of real time data generated by sensor networks, machine networks, and other interconnected systems. When properly analyzed, this massive and sometimes disorganized source of data can help firms gain insight, improve their strategy, streamline their operations and reduce their impact on the environment [5]. Every industry on the planet stands to benefit immensely from the potential of data analytics and real-time decision-making offered by the fusion of IoT and in AI. Through its huge collection of connected devices, the Internet of Things (IoT) generates copious amounts of data from an extensive range of sources, such as sensors, machines, automobiles, and even wearable gear [6] [7]. It has become apparent that machine learning models and other artificial intelligence analytics technology are necessary for businesses to mine this data for insights.

Anomalies in the Internet of Things (IoT) data are uncommon, but still occur, and can result in great insights for many different industries, including healthcare, manufacturing, banking, transportation, and energy, underlining the importance of identifying anomalies. One industry where anomaly detection is used in the internet of things is the betting and gambling industry. They use it to detect insider trading by analyzing the historical pattern of transactions. Meanwhile, industrial machinery uses a detection algorithm and ensures the security of production [8] [9]. When it comes to detecting possible problems with the functionality, security or performance, the role of anomaly detection plays a crucial role in the detection of problems before they become a bigger issue. An abundance of domains have made heavy use of traditional methods of anomaly detection such as rule based systems and statistical models [10]. Due to the inherent complexity and high dimensionality of IoT data, these approaches tend to underperform when it comes to detecting minor or evolving anomalies [11].

1.1 Structure of the paper

The structure of the paper is as follows: Section II discusses memory controller fault tolerance, Section III talks about security-aware designs, Section IV talks about integrated techniques and new trends, Section V analyzes the literature, and Section VI ends with recommendations for the future.

2 APPROACHES TO PREDICTIVE ANALYTICS IN IOT

Predictive analytics is the root method that collects real-world data from the IoT that contains practices, results or future occurrences. To deal with the huge amount of heterogeneous data generated by the Internet of Things (IoT), data processing makes use of a wide variety of models, and each which has its set of advantages. The main models of predictive analytics and their connections with processing data from IoT systems are emphasized in this section.

2.1 Traditional and Statistical Methods

Traditional methods in IoT predictive analytics include: regression models, time series forecasting (e.g. ARima), rule-based approaches. They use historical data to predict trends or detect anomalies. The simplicity and computational efficiency of these methods make them ideal for small sensor networks, but they fail miserably when faced with complicated, real-time IoT data including high dimensions. Predictive approaches of the Internet of Things are illustrated in Figure 1.

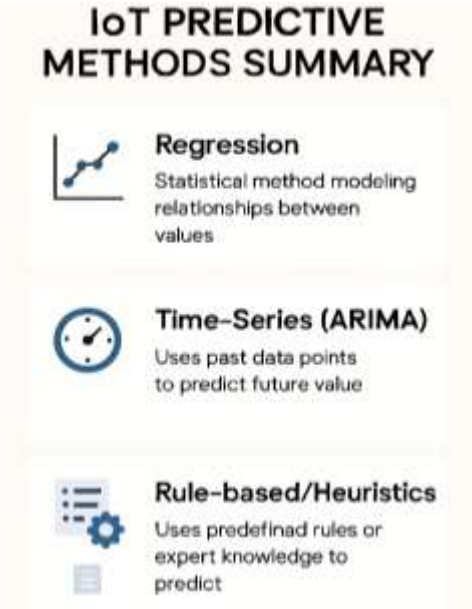

Figure 1: Methods in IoT Data

- **Regression-Based Models:** Regression models are most effectively utilized in scenarios where the dependent variable is continuous, comprising a wide range of possible values. These kinds of data might include temperature readings or any number of other continuous variables. Finding out how much of an effect the explanatory variable has on the dependent variable is the main goal of applying regression models in these environments.
- **Time-Series Forecasting:** The most distinctive feature of time series data compared to other forms of information is the passage of time. In addition to providing more information for their analysis, this attribute of theirs is a constraint and a structural component of the data gathering [12]. A collection of observations of a variable grouped into equally spaced time intervals is the basic definition of time series data, which can be any type of information shown as an ordered sequence.
- **Rule-Based and Heuristic Approaches:** One of the most important uses of predictive modelling is in the identification of fraud. While traditional rule-based systems do a good job, they can't always keep up with the changing patterns of fraud. In order to identify irregularities that could be signs of fraud, ML models, such as NN and SVM [13], can conduct real-time analyses of massive datasets.

2.2 Machine Learning-Based Predictive Analytics

An IoT monitoring system that gathers data from the environment, including temperature, humidity, and accelerometers and gyroscopes, can be created in real time and have used various machine learning models to this processed data in order to make predictions. By combining supervised and unsupervised learning methods, a hybrid machine learning algorithm outperforms its competitors. A variety of hybrid methods are employed for the purpose of prediction [14]. An assortment of ML methods for IoT anomaly detection are illustrated in Figure 2.

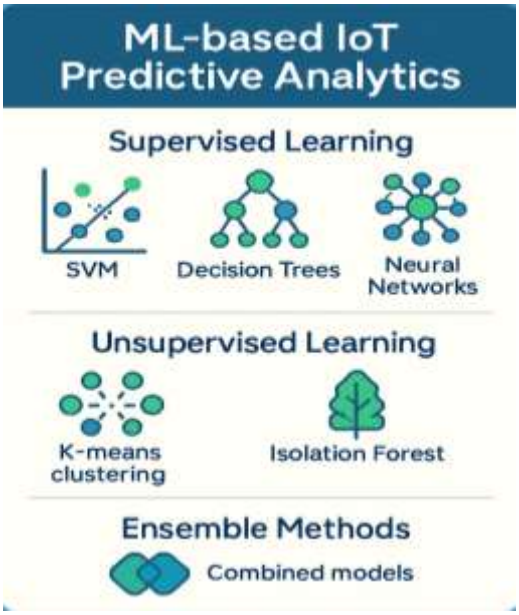

Figure 2: Different Machine Learning Methods

- **Supervised Learning Models:** Supervised learning is utilized on datasets with labeled outcomes, allowing the model to understand the relationship between inputs and final results, including the detection of outliers. It is one of the most widely used approaches in organizations and industries due to its effectiveness in classification and prediction tasks [15]. Common supervised learning algorithms include SVM, DT, NN, Bayesian Networks, and KNN. These algorithms, often referred to as discriminative models, leverage labeled instances to facilitate classification-based learning.
- **Unsupervised Learning Models:** Anomaly detection using unsupervised learning has just begun to acquire relevance. Unlabeled data pattern learning is a machine learning technique that doesn't require explicit user guidance. In order to discover hidden patterns or correlations, the algorithm investigates the data structure rather than receiving accurate outputs [16]. In this learning models like, K-means clustering, isolation forest etc.
- **Ensemble Methods:** Several models, also referred to as weak classifiers, are trained using ensemble learning, a paradigm in machine learning. In order to achieve better outcomes than any one algorithm could on its own, these models are integrated using various voting procedures and are based on features collected from multiple data projections[17].

2.3 Deep Learning Approaches for IoT Data

Deep learning uses NN to efficiently identify abnormalities, discover intricate patterns, and evaluate IoT data [18]. DNNs are just as successful in anomaly identification in the Internet of Things as they are in domains like NLP and vision. Figure 3 shows the various deep learning models used in IoT sensor networks to detect anomalies.

Figure 3: Different Deep learning Approaches

- **Recurrent Neural Networks:** The quantity and quality of training data have a significant impact on hydrological prediction using standalone RNN, LSTM, or GRU models. High-dimensional datasets with a wide range of hydrological and meteorological parameters make complex relationships easier for the model to understand [19]. The absence of easily accessible, continuous, high-quality data is a significant barrier to applying DL models for hydrological prediction.
- **Convolutional Neural Networks:** A powerful family of DL models, CNNs are utilized in many different applications, such as object detection, bioinformatics, computer vision, picture classification, and speech recognition [14]. They have also successfully completed time series prediction tasks. To extract features from data, feedforward neural networks called CNNs use convolutional layers. To automate feature extraction and enable end-to-end training with minimal preprocessing, the CNN employs a two-stage design that integrates a classifier and a feature extractor.
- **Hybrid and Advanced Architectures:** The benefits of GRU-LSTM layers for mimicking temporal relationships and CNNs for extracting spatial data are combined in the Hybrid CNN-GRU-LSTM model [20]. CNN efficiently captures spatial correlations among road segments by leveraging vehicle flow patterns in nearby areas, while the GRU and LSTM layers collaborate to learn both short-term fluctuations and long-term trends in traffic flow data.

Table 1 compares predictive analytics approaches for IoT data, focusing on traditional and statistical, ML, and DL approaches. It summarises their methods, data requirements, advantages, limitations, and use cases, offering a clear overview to help choose appropriate approaches for IoT applications and data complexity.

Table 1: Comparative Overview of Predictive Analytics Approaches in IoT Data

Aspect	Example Methods	Data Requirement	Advantages	Limitations	Use Cases
Traditional & Statistical	Regression (Linear, Multiple, Logistic), Time-Series (ARIMA, Holt-Winters), Rule-Based & Heuristic Approaches	Historical or structured sensor data; predefined variables; smaller datasets	Simple, computationally efficient, interpretable, good for basic trend prediction and threshold-based anomaly detection	Limited scalability to high-dimensional/streaming data; may not adapt to evolving or nonlinear patterns	Predicting temperature, energy usage, humidity trends, fraud detection, simple anomaly detection in IoT
Machine Learning-Based	Supervised (SVM, Decision Trees, Neural Networks), Unsupervised (K-Means, Isolation Forest), Ensemble (Bagging, Boosting)	Labeled (supervised) or unlabeled (unsupervised) IoT data	Accurate, adaptable, detects complex patterns/anomalies, works for diverse IoT applications	Resource-intensive, may overfit, complex implementation, requires data preprocessing	Predictive maintenance, fault detection, classification, anomaly detection
Deep Learning	RNN, LSTM, GRU, CNN, Hybrid (CNN-GRU-LSTM)	Large, high-dimensional datasets	Handles complex spatial-temporal patterns, automatic feature extraction, effective for multi-sensor networks	Computationally heavy, requires tuning, large labeled data needed	IoT anomaly detection, real-time time-series forecasting, multi-sensor analytics, complex pattern recognition

3 ANOMALY DETECTION IN IOT

A major concern in the Internet of Things (IoT) ecosystem is ensuring the reliability, efficacy and safety for all the connected devices. Anomaly detection is becoming increasingly important as there is a huge amount of data coming from IoT devices. Businesses can gain important insights and improve their efficiency with operations if they use anomaly detection correctly [21]. It helps identify possible issues before they worsen. When a data point does not match the expected behavior of a modeled system, it is considered an anomaly. As seen in Figure 4, anomalies are occurrences that are highly unusual and do not conform to the norms or patterns seen in the dataset as a whole, in a particular context, or over a shorter period of time (such as a quarter or season) [22].

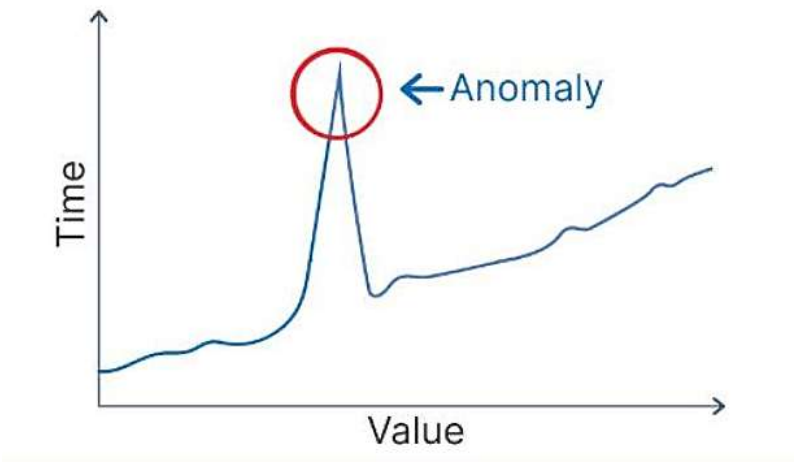

Figure 4: Anomaly in Dataset

3.1 Types of Anomalies

The type of anomaly that is sought after is a crucial component of anomaly detection techniques. The following three groups of anomalies can be identified, as illustrated in Figure 5:

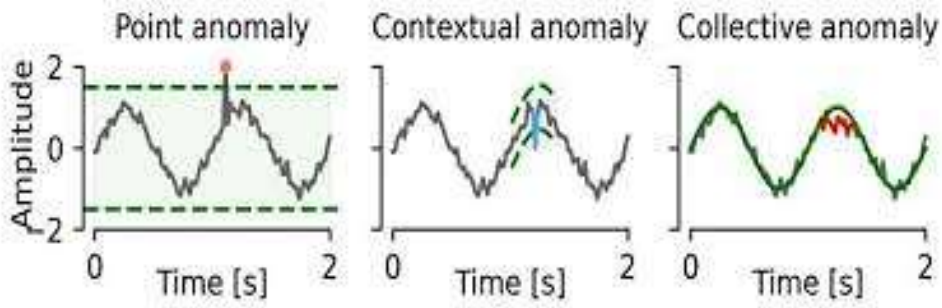

Figure 5: Different Types of Anomalies

- **Point Anomalies:** Data may reveal point anomalies, sometimes called global anomalies. Although point anomalies are the easiest to spot, a big challenge in this area is determining an appropriate measurement of the object's divergence from other objects. In a typical network, each hub needs at least two neighbors that are connected to it [23]. Group V2's hubs form this type of network, which is typical behavior; group V1, on the other hand, has isolated nodes.
- **Contextual Anomalies:** This kind of strange behavior happens when something that would be considered unusual in one setting isn't in another. There are two categories of characteristics associated with contextual anomalies: contextual and behavioural. Location datasets that include longitude, spatial, and latitude all have unique contextual features [24]. The contextual feature of time in time-series data also shows the arrangement's position for each instance. The second trait is seen as a trait of behavior.
- **Collective Anomalies:** These happen when a large number of continuous data points exhibit, in unison, aberrant behavior that contradicts the behavior of other points. Collective anomalies in database systems are a series of seemingly legitimate database operations that, when executed concurrently, reveal a system breakdown or an attack [25]. Common methods for spotting group outliers include clustering and sequence analysis, such DBSCAN and sequence-based neural networks.

3.2 Anomaly Detection using Deep Learning

Deep learning models like autoencoders, GANs, and transformers can automatically learn patterns in IoT data and detect deviations in real time. They handle complex, high-dimensional sensor streams better than traditional methods. These are some of the approaches that help in improving the scalability, accuracy and adaptability for detecting anomalies in IoT networks.

- **Autoencoder-Based Anomaly Detection:** One type of neural network that mimics input from output is called an autoencoder. The autoencoder uses the thump rule to compress the input into latent space and reconstruct the output [26]. One type of unsupervised machine learning is the auto encoder, sometimes referred to as a feature extraction algorithm. Text, voice, images and videos are just some of the many types of input that autoencoder can handle.
- **Transformer-Based Anomaly Detection:** Anomaly detection and some other time series related tasks have witnessed growth in the use of transformers due to efficiency in handling big data and complex dependencies. There are a number

of models that are based on Transformers; these models vary in their strengths in the case of anomaly detection, important contributions and some others [27]. When it comes to time series data for example, Anomaly Transformer is all about gathering temporal relationships and distinguishing between the normal and the unusual. By comparing the expected and actual patterns within the data sequences, it combines attention techniques in order to efficiently reveal the abnormalities in IoT log data.

- **GAN-Based Anomaly Detection:** A common deep anomaly detection approach is GAN-based anomaly detection, which is gaining popularity rapidly [28]. In general, the goal of this method is to train a generative network's latent feature space G such that it accurately represents the data's inherent normalcy. The anomaly score is a residual that exists between the actual occurrence and the created one.

4 CHALLENGES OF IOT ANOMALY DETECTION

The machine learning model may need to be retrained or updated on a frequent basis due to potential changes in data patterns and relationships brought about by the ever-changing nature of the IoT. The scarcity of labelled training data is another obstacle to anomaly detection on the IoT. There are several challenges in deep learning to find anomalies:

- **High dimensionality:** There are usually a lot of sensors, devices, and data sources that contribute to the high dimensionality of IoT data. Because algorithms must deal with a huge number of features and capture intricate correlations between them, anomaly detection becomes more challenging due to this high dimensionality. To overcome this obstacle, dimensionality reduction techniques might be necessary.
- **Scalability:** The IoT creates real-time huge data sets. Anomaly detection systems need to be scalable in order to deal with the rapid and massive amounts of data [29]. Fast, efficient algorithms and storage-and processing-capable infrastructure are necessities for real-time processing of data sets of this magnitude.
- **Context Information:** The dispersed nature of IoT devices makes them ideal for gathering context data needed for detecting anomalies. On the other hand, in large IoT deployments, where some IoT devices are mobile, it is sometimes unnecessarily hard to capture the time-related input b1 in relation to spatial contexts and input bn [30]. In other words, the advantage of anomaly detection systems is that they are in a position to add information, but getting the right context right can make them more complex.
- **Profiling Normal Behaviours:** Defining typical actions is tough, but having enough data about them is essential for an anomaly detection system to work. Since they don't occur very frequently, sometimes the abnormal behaviors would be lumped in with normal behaviors. For widely dispersed IoT devices in particular, supervised learning is not an option due to a dearth of datasets capturing both typical and out-of-the-ordinary data from the IoT.

5 LITERATURE REVIEW

This review summarises the progress in IoT anomaly detection in terms of accuracy, robustness, and scalability. Approaches like self-attention mechanism, GAN-based model, edge-enabled framework and hybrid approaches reflect the advancement towards more reliable and adaptive IoT systems.

Yan *et al.* (2025) presented an IoT sensor data correlation and anomaly detection model based on a self-attention mechanism, which is innovative on the basis of existing time series analysis and deep learning models. The model combines a multi-layer self-attention-based architecture and a hybrid encoder-decoder architecture, which can extract temporal and spatial correlations in sensor data in parallel. They proposed a new type of attention scoring function which can handle irregularities in sensor data, improving on the traditional attention mechanism to better deal with missing values and sensor noise. The model further improves this aspect by including a dynamic attention mechanism, which helps to focus on the most relevant sensor data sequences to correlate data and separate out the anomalous patterns more effectively [31].

Gutierrez-Rojas *et al.* (2025) presented a model for detecting anomalies in IoT-enabled CPSs via WSNs. The model consists of three main blocks of data in the cyber layer: sensor-based data acquisition, data fusion to transform raw data into information, and analytics for decision-making. The logic behind these blocks shows the importance of anomaly detection and is illustrated by three use cases, i.e. the selection of faults in power grids, the detection of anomalies in an industrial chemical process and the prediction of the carbon dioxide level in a room [32].

Li *et al.* (2024) introduced UatGAN, a GAN-based technique for detecting anomalies in time-series signals from IoT devices without manual supervision. The method combines autoencoders (AEs) and GANs, using the encoderdecoder structure of AE to learn compressed representations of input data, and enhances sensitivity to anomalous inputs through adversarial training of GANs. Given time correlation, the dynamic time warping (DTW) algorithm is used to compute reconstruction errors, and a new anomaly diagnosis strategy is proposed. Experiments conducted on public datasets demonstrate that their method detects anomalies more accurately than baseline methods [33].

Shahnejat Bushehri *et al.* (2024) developed a system to analyse data transmissions to identify IoT nodes experiencing energy anomalies. They make use of a publicly available dataset comprising data on energy and link quality in peer-to-peer IoT communication. To begin, their system examines data transfer for IoT transceivers using linear regression to determine the most

important characteristics. At a later stage, the gradient flow is adjusted using a deep neural network in order to highlight the most important properties. This adjustment reduces the corresponding reconstruction error, thereby increasing the accuracy of anomaly identification. The last piece of information that nodes can use to improve their transmission configuration for future communication is the energy stabilization feedback [34].

Zerkouk, Mihoubi and Chikhaoui (2023) introduced DGM-IF, an innovative unsupervised approach of anomaly detection for IoT and wireless sensor networks. Anomaly detection and resilient normal data representation are attained by the combination of deep generative models and Isolation Forest technique in DGM-IF. Using the learnt distribution as a basis, the model generates synthetic data and the Isolation Forest is used to isolate the outliers. The proposed approach is evaluated on real-world datasets and compared with state-of-the-art methods to demonstrate its effectiveness in detecting outliers. The DGM-IF method can detect possible threats and attacks, which might greatly improve the security and dependability of IoT systems and wireless sensor networks [35].

Li et al., (2022) introduced ADRIoT, a framework for detecting anomalies in IoT networks that makes use of edge computing to reveal possible dangers. Anomaly detectors, a traffic preprocessor, and a traffic capturer are the components of an anomaly detection module that an edge can employ. These modules are further customized to each device type. An LSTM autoencoder builds each detector unsupervised, so it can handle new zero-day attacks as they emerge and doesn't require labelled attack data. The edge retrieve the matching detector from the cloud and run it locally whenever a device connects to it. Another issue is that deploying such a detection module is hindered by the resource constraint of a single edge device, such as a home router [36].

Qiao, Zhang and Zhang (2022) suggested a GAN-based model for Internet of Things anomaly detection that can effectively learn data patterns unsupervisedly, even when faced with contaminated training data. To facilitate effective representation mapping, the new model incorporates the Bidirectional GAN (BiGAN) architecture, and to eliminate training-set noise, it uses the Robust Principal Component Analysis (RPCA) method. The training approach incorporates a proximal method and Alternating Direction Method of Multiplier (ADMM), and a new objective function and score function are meticulously constructed to enhance its performance [37].

The recent IoT anomaly detection studies are summarized in Table 2 and they have shown improvements in accuracy, robustness and adaptability. The main issues are scalability, efficiency, and generalization, and one of the directions of future work should be lightweight models and deploying at the moment.

Table 2: Summary of Previous Study on IoT Anomaly Detection Approaches

Reference	Study On	Approach	Key Findings	Challenges / Limitations	Future Directions
Yan et al., 2025	IoT sensor data correlation & anomaly detection	Self-attention mechanism with hybrid encoder-decoder	Captures temporal & spatial correlations, handles missing values & sensor noise using dynamic attention	High computational cost for multi-layer self-attention; scalability issues for large IoT systems	Optimize lightweight attention mechanisms; extend to real-time IoT monitoring
Gutierrez-Rojas et al., 2025	IoT-enabled industrial CPS anomaly detection	Cyber-layer model with data acquisition, fusion, and analytics	Demonstrated effectiveness in power grids, chemical processes, CO_2 prediction	Dependency on wireless sensor reliability; domain-specific model tuning	Apply to broader CPS domains; enhance adaptability for heterogeneous IoT systems
Li et al., 2024	IoT time series anomaly detection	UatGAN (AE + GAN + DTW)	Improved anomaly detection accuracy over baselines; novel diagnosis strategy	GAN training instability; computationally heavy DTW calculations	Develop more stable GAN architectures; apply to diverse IoT datasets
Shahnejat Bushehri et al., 2024	Energy anomaly detection in IoT nodes	Linear regression + deep neural network with gradient modification	Identifies dominant features; improves anomaly detection by reducing reconstruction error	Limited to energy & link quality datasets; model generalizability not proven	Extend framework to multiple IoT domains; real-world deployment testing
Zerkouk, Mihoubi & Chikhaoui, 2023	WSN & IoT anomaly detection	Deep Generative Model + Isolation Forest (DGM-IF)	Learns robust normal data representation; effective anomaly detection in real datasets	Synthetic data quality affects performance; limited evaluation scope	Broader benchmarking; improve synthetic data generation quality
Li et al., 2022	IoT edge-based anomaly detection	ADRIoT framework with LSTM autoencoder detectors	Detects zero-day attacks without labeled data; edge-cloud integration	Resource constraints of edge devices; scalability challenges	Optimize lightweight detectors; explore federated learning for distributed IoT

Qiao, Zhang & Zhang, 2022	IoT anomaly detection with noisy data	BiGAN + RPCA + ADMM	Handles noisy data; robust unsupervised anomaly detection	Training complexity due to multiple integrated components	Simplify training pipeline; expand robustness to different IoT noise patterns

6 CONCLUSION AND FUTURE WORK

The heterogeneity, large scale, and limited resources of the IoT ecosystem have hindered cyberattack detection and prevention, as this review demonstrates, and have also highlighted how deep learning can support real-time anomaly detection and predictive analytics in IoT sensor networks. DL models are more effective than traditional statistical and ML models when processing large-scale, high-dimensional, and heterogeneous IoT data. Autoencoders, GANs and transformers are some of the techniques that offer adaptive and scalable methods to detect subtle anomalies or predict system behavior in a variety of fields, including healthcare, smart infrastructure, industrial internet of things, and environmental systems. Deep models can vastly improve system durability, efficiency, and decision-making accuracy by automatically extracting hierarchical features. Nevertheless, there are various limitations, including the imbalance of the data, high computational and the lack of interpretability, and which are limiting the scaling of this technology in resource-constrained IoT settings. In general, deep learning-based solutions can be viewed as a viable direction of creating strong and intelligent IoT systems, leading to predictive, proactive, and secure IoT systems.

Future studies should focus on developing light and energy-efficient deep learning models capable of running on edge and fog computing frameworks to eliminate reliance on cloud systems. Federated and distributed learning advances are potentially useful to assure privacy and provide collaborative anomaly detection across the IoT devices. Also, predictive analytics and anomaly detection in next-generation IoT networks will be further enhanced by adaptive models capable of adapting to changing IoT data patterns, as well as integration of reinforcement learning to make decisions in real-time.

REFERENCES

[1] S. Nourildean, M. Hassib, and Y. Mohammed, “Internet of things based wireless sensor network: a review,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, pp. 246–261, 2022, doi: 10.11591/ijeecs.v27.i1.pp246-261.

[2] Honie kali, “The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday,” *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[3] A. H. Bagdadee, M. Z. Hoque, and L. Zhang, “IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid,” *Procedia Comput. Sci.*, vol. 167, pp. 1148–1160, 2020, doi: https://doi.org/10.1016/j.procs.2020.03.417.

[4] Nirav Kumar Prajapati, “Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[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, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[6] G. Vani, R. N. Raman, R. Singha, R. Sharkar, and N. Kumar, “Advancing Predictive Data Analytics in IoT,” *Nanotechnol. Perceptions*, vol. 20, pp. 568–582, 2024, doi: 10.62441/nano-ntp.vi.3968.

[7] Dhruv Patel, “Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices,” *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 454–464, Jan. 2024, doi: 10.48175/IJARSCT-11900D.

[8] A. Chatterjee and B. S. Ahmed, “IoT anomaly detection methods and applications: A survey,” *Internet of Things*, vol. 19, p. 100568, 2022, doi: https://doi.org/10.1016/j.iot.2022.100568.

[9] V. Thangaraju, “Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques,” *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, pp. 1–8, 2025.

[10] S. Narang and A. Gogineni, “Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment,” *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[11] A. Singh, S. Singh, M. Nazmul Alam, and G. Singh, “Deep Learning for Anomaly Detection in IoT Systems: Techniques, Applications, and Future Directions,” vol. 6, p. 9, 2024.

[12] V. Shah, “Managing Security and Privacy in Cloud Frameworks : A Risk with Compliance Perspective for Enterprises,” *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 606–618, 2022.

[13] A. Abdulkareem, “Applying Predictive Modelling Techniques to Complex Data: Enabling Proactive Solutions in Evolving Market Scenarios,” *Int. J. Res. Publ. Rev.*, vol. 6, no. 1, pp. 3125–3140, 2025, doi: 10.55248/gengpi.6.0125.0510.

[14] A. R. Bilipelli, “AI-Driven Intrusion Detection Systems for LargeScale Cybersecurity Networks Data Analysis: A Comparative Study,” *TIJER – Int. Res. J.*, vol. 11, no. 12, 2024.

[15] M. Kontagora and B. Idoko, “Machine Learning Algorithms for Anomaly Detection in IoT Networks – A Review,” *African Multidiscip. J. Sci. Artif. Intell.*, vol. 1, pp. 802–823, 2024, doi: 10.58578/amjsai.v1i2.4014.

[16] V. Shah, “Analyzing Traffic Behavior in IoT-Cloud Systems : A Review of Analytical Frameworks,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 9, no. 3, pp. 877–885, 2023, doi: 10.32628/IJSRCSEIT.

[17] B. Naderalvojoud and T. Hernandez-Boussard, “Improving machine learning with ensemble learning on observational healthcare data,” *AMIA ... Annu. Symp. proceedings. AMIA Symp.*, vol. 2023, pp. 521–529, 2023.

[18] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, “Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations,” *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, 2023,

doi: 10.63282/3050-9262.ijaidsml-v4i3p103.
[19] M. Waqas and U. W. Humphries, "A critical review of RNN and LSTM variants in hydrological time series predictions," *MethodsX*, vol. 13, no. September, p. 102946, 2024, doi: 10.1016/j.mex.2024.102946.
[20] V. Singh, S. K. Sahana, and V. Bhattacharjee, "A novel CNN-GRU-LSTM based deep learning model for accurate traffic prediction," *Discov. Comput.*, vol. 28, no. 1, 2025, doi: 10.1007/s10791-025-09526-0.
[21] S. Narang and V. G. Kolla, "Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, pp. 1–7, 2025, doi: 10.56975/ijrar.v12i3.319048.
[22] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet of Things (Netherlands)*, vol. 19, no. June, p. 100568, 2022, doi: 10.1016/j.iot.2022.100568.
[23] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, Dec. 2023, doi: 10.14741/ijcet/v.13.6.11.
[24] S. Natha, "A Systematic Review of Anomaly detection using Machine and Deep Learning Techniques," *Quaid-e-Awam Univ. Res. J. Eng. Sci. Technol.*, vol. 20, pp. 83–94, 2022, doi: 10.52584/QRJ.2001.11.
[25] H. J. Veeravenkata Maruthi Lakshmi Ganesh Nerella, Kapil Kumar Sharma, Sarat Mahavratayajula, "A Machine Learning Framework for Cyber Risk Assessment in Cloud-Hosted Critical Data Infrastructure," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 4, pp. 2409–2421, 2025.
[26] M. R. Ahasan, M. S. Haque, M. R. Akram, M. F. Momen, and M. G. R. Alam, "Deep Learning Autoencoder based Anomaly Detection Model on 4G Network Performance Data," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 232–237. doi: 10.1109/AIIoT54504.2022.9817338.
[27] N. Sánchez *et al.*, "Towards Enhanced IoT Security: Advanced Anomaly Detection using Transformer Models," pp. 1–5, 2024.
[28] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep Learning for Anomaly Detection: A Review," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–36, 2022, doi: 10.1145/3439950.
[29] M. Yang and J. Zhang, "Data Anomaly Detection in the Internet of Things : A Review of Current Trends and Research Challenges," vol. 14, no. 9, pp. 1–10, 2023.
[30] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 04, pp. 3557–3564, 2025.
[31] X. Yan, H. Zhang, Y. Di, and L. Xie, "Research on IoT Sensor Data Correlation and Anomaly Detection Based on Self-Attention Mechanisms," in *2025 5th International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, 2025, pp. 802–805. doi: 10.1109/ICCECE65250.2025.10985672.
[32] D. Gutierrez-Rojas *et al.*, "Detection and Classification of Anomalies in WSN-Enabled Cyber-Physical Systems," *IEEE Sens. J.*, vol. 25, no. 4, pp. 7193–7204, 2025, doi: 10.1109/JSEN.2024.3520507.
[33] Y. Li, X. Li, S. Lv, Y. Chen, W. Zhang, and Y. Ding, "Unsupervised Anomaly Detection for IoT Time Series Signals with GANs," in *2024 IEEE International Conference on Signal, Information and Data Processing (ICSIDP)*, 2024, pp. 1–6. doi: 10.1109/ICSIDP62679.2024.10869232.
[34] A. Shahnejat Bushehri, A. Amirnia, A. Belkhiri, S. Keivanpour, F. G. de Magalhães, and G. Nicolescu, "Deep Learning-Driven Anomaly Detection for Green IoT Edge Networks," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 1, pp. 498–513, 2024, doi: 10.1109/TGCN.2023.3335342.
[35] M. Zerkouk, M. Mihoubi, and B. Chikhaoui, "Deep Generative Model with Isolation Forest (DGM-IF) for Unsupervised Anomaly Detection in Wireless Sensor Network and Internet of Things," in *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2023, pp. 2275–2280. doi: 10.1109/CoDIT58514.2023.10284184.
[36] R. Li, Q. Li, J. Zhou, and Y. Jiang, "ADRIoT: An Edge-Assisted Anomaly Detection Framework Against IoT-Based Network Attacks," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10576–10587, 2022, doi: 10.1109/JIOT.2021.3122148.
[37] Y. Qiao, B. Zhang, and Z. Zhang, "Unsupervised Anomaly Detection for IoT Data based on Robust Adversarial Learning," in *2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, 2022, pp. 2324–2330. doi: 10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00343.

