RESEARCH ARTICLE

Journal of Data Analysis and Critical Management, Volume 02, Issue 01, 2026

Recent Advances in Anomaly Identification for IoT Devices Using Machine and Deep Learning Models

Prathik Kumar Jannu[1*], Javed Ali Mohammad[2], Sri Harsha Panchali[3], Usha Mohani Kavirayani[4], Krishna Bhardwaj Mylavarapu[5], Jenitha Pilli[6]

[1]Computer Science Engineering, JNTU Hyderabad
[2]Masters in Data Science, New England College
[3]Information Systems Engineer, CrowdStrike Inc
[4]MS in Computer Science, Kent State University
[5]MS in Computer Science, University of Illinois Springfield
[6]MS in Computer Science, University of Louisiana at Lafayette

Abstract

The rapid expansion of the IoT has revolutionized data interchange in numerous industries, including smart cities, transportation, healthcare, and industry. However, it has also posed serious security problems due to the increasing number of vulnerable devices. Anomaly detection has become the primary instrument of the shield to locate abnormal behaviors in the box of the intrusion, fault, and failure of the operation. Anomaly detection in IoT systems has been the focus of recent advances in ML and DL methods. This paper assesses the efficacy, accuracy, and adaptability of supervised, unsupervised, and hybrid learning models in this context. In addition, the review emphasizes the main factors that determine detection performance, such as feature extraction, real-time detection, and multi-target learning strategies. Although ML/DL-based approaches have a strong potential, problems, for example, computational overhead, scalability limitations, and a lack of sufficient labeled data, that hinder the progress still exist. The paper provides useful information for researchers and practitioners in the choice of the most effective methods and assists in making the first steps toward future advances in IoT anomaly detection securing that it is still smart and resource-efficient

Keywords: Anomaly Detection, Internet of Things (IoT), Machine Learning (ML), Deep Learning (DL), Intrusion Detection Systems (IDS), Cyber security in IoT

Journal of Data Analysis and Critical Management (2026); DOI: 10.64235/6wy0d584

Introduction

A lot has changed in the way people communicate since the advent of the Internet. Similarly, IoT gadgets are altering how see and engage with the real world. An example of an IoT device might include a smartphone, laptop, smart device, environmental sensor, etc., all linked together through various technologies to form an interconnected network [1][2]. A number of sensors and equipment can now talk to one another directly, without any intervention from the user, thanks to the IoT. IoT devices have emerged as a major data source in recent years. Meaningful information can be extracted from these datasets using methods like machine learning techniques [3].

The aim of anomaly detection is to identify instances in data that do not conform to the norm [4][5]. Finding new and unusual things is an important part of several branches of AI, computer vision, and statistics [6][7]. Finding data cases that differ greatly from the norm is its principal objective [8]. Unprotected data could include crucial, useful, and vital information, which is why detecting anomalies is essential in many application domains.

Corresponding Author: Prathik Kumar Jannu, Computer Science Engineering, JNTU Hyderabad, e-mail: prathikjannu@gmail.com

How to cite this article: Jannu, P.K., Mohammad, J.A., Panchali, S.H., Kavirayani, U.M., Mylavarapu, K.B., Pilli, J. (2026). Recent Advances in Anomaly Identification for IoT Devices Using Machine and Deep Learning Models. Journal of Data Analysis and Critical Management, 02(1):37-47.

Source of support: Nil

Conflict of interest: None

Anomaly detection in IoT networks is enhanced with ML. techniques, including those that detect abnormalities in IoT networks and provide dependable and explicable outcomes [9]. DL is a decision-making technique that uses artificial neural networks to discover patterns and learn from them. distinct approaches, with an emphasis on their use in a variety of IoT settings. When faced with the complexity and volume of modern IoT data, conventional approaches, such as rule-based systems, provide outcomes that are easy to understand and are straightforward. ML techniques, including NNs, DTs, and SVMs, provide more accuracy and flexibility when recognizing subtle and changing anomalies. At its core, deep learning is just a ML system driven by artificial intelligence that models brain activity using neural networks. Its remarkable ability to learn from large datasets is a major reason for its meteoric rise in popularity [10][11]. It does this by utilizing supervised, semi-supervised, or unsupervised learning algorithms, as well as DL architectures, to learn on its own. Big data analysis, face recognition, customization, NLP, driverless vehicles, automated handwriting generation, news aggregation, and other applications can all benefit from deep learning methodologies.

Structure of the Paper

The structure of this article is as follows Section II discusses the process and drivers of anomaly detection in IoT systems. In Section III machine learning approches, Section IV Deep learning approches, Section V Literature of review, section VI Conclusions and future work.

Key Driver and Mechanism of Anomaly Detection In Iot System

The term "anomaly detection" refers to the steps used to spot patterns in data that don't add up. Different types of applications use different words to characterize these irregularities unusual things, pollutants, surprises, outliers, outlying observations, exceptions, aberrations [12].

Types of Anomalies

There are three main types of anomalies: point, group, and contextual. It is well-established that Deep AD (DAD) approaches are successful in detecting anomalies in all three categories. Another kind of conditional anomaly is contextual anomaly. Data that acts strangely in one setting but normally in another is what this term describes (see Figure. 1).

Figure 1: Type of Anomalies

- **Point anomaly:** Detect anomalies within network traffic data through the analysis of individual feature values, thereby identifying outliers that demonstrate substantial deviations from expected behavior. As they reveal discrete outliers unrelated to the interplay of factors, point anomalies—that is, discrepancies in a single data point—represent a basic technique in AD. If the packet loss rate were to suddenly spike, for example, it would be considered an abnormality since it deviates from the baseline.
- **Conditional anomaly:** Power consumption is one use-case that is likely to exhibit contextual anomalies due to time-related correlations [13]. For example, it is reasonable to assume that an office building's power consumption is significantly greater during the middle of the workday compared to the night and on weekends.
- **Group anomaly:** A group anomaly is an example of an anomaly that indicates atypical group distributions across a specific time period. To address the fundamental problem of recognizing group anomalies in different datasets, it may be necessary to associate certain locations and time intervals with that event or point, since this provides a larger view and help establish an overall knowledge of the event.

Anomaly Detection Approach in Iot

AD is the process of finding uncharacteristic or abnormal patterns in the network or system behavior, which might suggest security threats, attacks, or malfunction [14]. It does this by looking at the present operation against the previously recognized normal behavior, thereby letting the system find the exceptions that could be entry, cause of the performance degradation, or even track malicious user actions. Hence, the technology empowers the companies to avert the risk of penetration, to keep the system going, and to issue a swift reaction to new threats in shown in Figure 2.

Detection Method

Network Data Analysis

This approach analyze network traffic interactions through numbers and statistical patterns. It finds anomalies through the comparison of the current traffic

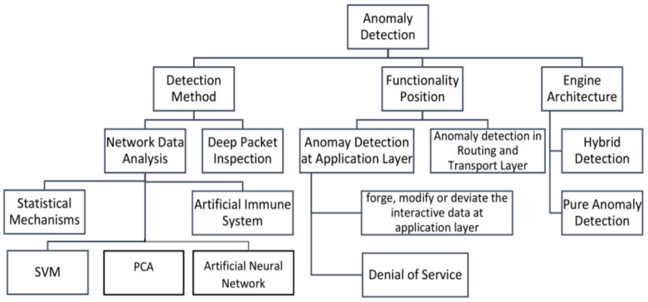

Figure 2: Anomaly Detection Approaches in IoT

with the normal traffic profile that has been learned.

- **Statistical mechanism:** Statistical models determine normal intervals for traffic features such as rate or timing. Any instance that is far outside these intervals is considered to be a suspicious one.
- **Support vector machine:** SVM identifies the edges that divide normal traffic from abnormal one. It means that if some new data goes beyond these edges, it considered an anomaly.
- **Principal component analysis:** PCA simplifies complex traffic data by extracting key components that represent the main behavior of the data. A significant deviation of the traffic from these major patterns is considered an anomaly.

Deep Packet Inspection

This method looks of packets beyond the header fields. It finds infected payloads or concealed fragments of the attacks that are the data.

- **Artificial Immune System (AIS):** AIS operates similarly to the human immune system in that it learns "self" (normal) and identifies "non-self" (abnormal). It is very good at finding brand-new or differently-shaped instances of the same type of attack.
- **Artificial Neural Network (ANN):** ANN through AI techniques learns intricate patterns from the historical traffic data. It discovers anomalies when the new traffic is different from the previously learned behavior.
- Functionality Position
- **Application Layer Detection:** The layer examines the behavior of applications and the interaction of users with them. It recognizes intrusions that change the requests or responses of an application.
- **Forge/Modify/Deviate Data**: It identifies situations in which hackers change, counterfeit, or manipulate application-layer data. One example could be a forged HTTP request or a modified user input.
- **Denial of Service (DoS):** Application layer DoS aims at overloading a service with too many or abnormal requests. The device detects sudden increases or repeated patterns that result in the unavailability of the service.
- **Routing and Transport Layer Detection:** The unit keeps an eye on the anomalies in TCP/UDP flow and routing operations. Among other things, it identifies the falsification of routing updates, excessive packet sending (flooding), or irregular packet delivery.

Engine Architecture

- **Hybrid Detection:** Hybrid engines use a combination of different methods statistical, signature-based, and ML to enhance their accuracy. They lower false positive rates and can detect both familiar and new types of attacks
- **Pure Anomaly Detection:** That system is based solely on changes in normal behavior and does not utilize any attack signatures. Such a system is very effective in the case of zero-day attacks; however, it can cause a higher number of false alarms.

Challenges in Anomaly Detection in Iot

AD method development in an IoT setting is difficult for a number of reasons. This section provides an explanation of these factors.

Scarcity of IoT Resources

Anomaly detection at the device level in the IoT might be constrained by storage, processing, communication, and power limits. Putting all of data processing, storage, and gathering needs on the cloud is one option. However, the cloud's remoteness can cause significant delay due to resource scheduling and round-trip time. For situations when IoT suspicious events must be handled in real-time, this delay might not be tolerable.

Profiling Normal Behaviours

Accumulating enough data about typical behaviors is crucial for an anomaly detection system to work, but it's not easy to define typical activities. Irregular behaviors may be grouped together with typical ones since they happen so seldom. The lack of datasets that include both typical and abnormal data from the IoT makes supervised learning even less practicable. This is especially the case when it comes to devices that are used extensively.

Dimensionality of Data

There are two types of Internets of Things data: univariate, in the form of key-value pairs, and multivariate, in the form of temporally connected univariate datasets.

The IoT anomaly detection system uses univariate series to compare real-time data with historical data. Alternatively, multivariate-based detection can offer correlations among variables as well as past stream relationships.

Context Information

The dispersed nature of IoT devices makes them ideal for gathering context data needed for detecting anomalies. Nevertheless, in big IoT deployments, whereby a portion of the devices are mobile, the difficulty is in capturing the time-related input $b1$ in relation to the location-related input bn. Anomaly detection systems benefit from adding context, but doing so might lead to increased complexity if the correct context isn't recorded.

Lack of Machine Learning Models Resiliency against Adversarial Attacks:

Since current ML models are vulnerable to adversarial attacks during training and detection and produce a large number of FP, robust algorithms and models are required.

Machine Learning Technique for Detecting Anomalies in the Iot

A lot of things need to be carefully thought out before ML can be used to find strange things in the IoT. There are primarily three types of learning algorithm approaches: supervised, unsupervised, and semi-supervised). Looking at the existing data dimension might help train learning algorithms for anomaly detection across many distributed IoT devices. This can lead to approaches that rely on univariate or multivariate analysis.

Supervised Learning Methods

Training a model to anticipate incoming data is the main objective of supervised learning. This process begins with learning a mapping from a collection of input variables to an output variable. dealing with issues related to regression and categorization.

- **Support Vector Machines (SVM):** SVMs make use of high-dimensional spaces to create the most effective border between outlier and regular data. In short, it is a perfect instrument for anomaly detection, as it can unravel complicated patterns and is still viable with a small number of samples.
- **Decision tree:** Decision Trees differentiate a given set of data by executing rules that have been drawn from sensor features thus making anomalies that have occurred easy to recognize.
- **Random forest:** Random Forest by combining multiple trees to lessen the noise and false detections enhances the accuracy.

Unsupervised Learning Methods

Data scientists use labelled data in supervised learning, such as photos of cats labeled as cats. A data scientist only needs to provide images for unsupervised learning; the system then analyze the data and make a determination. Unsupervised machine learning necessitates massive datasets, as demonstrated in (display as Figure 3).

There are four forms of unsupervised learning: clustering, association, anomaly detection, and auto encoder problems.

Types of Unsupervised Learning:

Clustering

The term "clustering" and "cluster analysis" describe the steps used to organize data into meaningful categories. One can classify clustering as either probabilistic, overlapping, hierarchical, or partitioning. Partitioning data ensures that each piece of information can only be associated with one cluster (show as Figure. 4).

The phrase "exclusive pooling" might also describe it. The partitioning process is illustrated by K-means.

Association

One unsupervised learning approach that may sift through massive datasets in search of correlations is Association Rule Learning (ARL). While other machine learning algorithms struggle with non-numerical data points, ARL can handle them with ease.

Anomaly Detection

The term "anomaly detection" refers to the procedure of identifying data signals that contain anomalies [15]. These outliers can indicate a malfunctioning

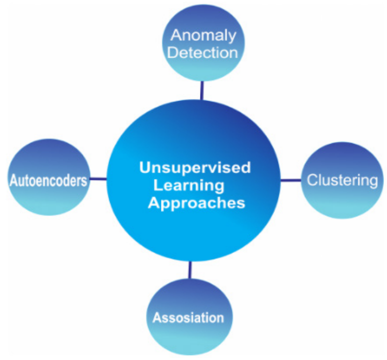

Figure 3: Types of Unsupervised Learning

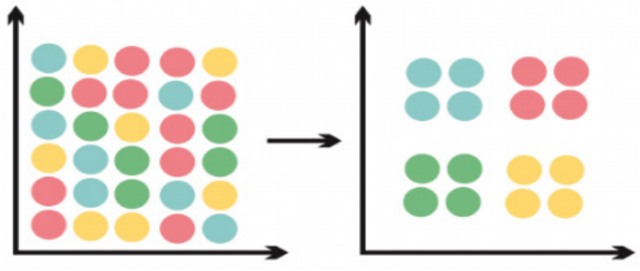

Figure 4: Example of Clustering

sensor, abnormal network activity, or data that needs cleaning before analysis. Data models are considered anomalous when they deviate significantly from the norm. Observing a peculiar pattern of network traffic.

Autoencoders

Auto encoders learn representations using neural networks, which is a type of unsupervised learning. Incorporate a limitation into the design of the neural network such that it is compelled to use a compressed form of the initial input.

Semi-Supervised Learning (SSL)

Consequently, medical image analysis tasks are well-suited to semi-supervised learning (SSL) approaches in order to decrease reliance on annotated medical picture datasets. Two main branches of the semi-supervised method exist: deep semi-supervised techniques and classic semi-supervised techniques. For classification, the classic semi-supervised algorithms combine labelled and unlabeled data. The primary objective of the traditional method is to enhance the performance of supervised models that have been trained on labeled data by incorporating insights gained via unsupervised learning on unlabeled data.

Deep Learning Approaches for IoT in anomaly detection

DL is one of several ML methods that have become de facto standards in the field. The way ML works is analogous to that of a newborn baby. When a signal is transmitted to the brain, its vast network of interconnected neurons begins processing the information. A certain cluster of neurons lights up, for example, when an infant sees a car. Just by exposing the baby to a different model of car, the identical network of neurons gets activated.

AutoEncoder

Encoder, decoder, and bottleneck layers are the standard construction of an auto-encoder.

- **Encoder:** The raw data is fed into the input layer. In order to capture important features and patterns, hidden layers progressively reduce the input's dimensionality. The encoder is made up of these layers. An extremely reduced dimensionality characterizes the last concealed layer, the bottleneck layer (latent space). The incoming data is compressed and represented by this layer.
- **Bottleneck:** It is a module that stores the compressed knowledge representations and it is the most significant component of the network.
- **Decoder:** The bottleneck layer restores the dimensions of the original input from the encoded representation. In an ideal world, the reconstructed output, which is produced by the output layer, would closely resemble the input data.

Recurrent Neural Networks (RNN):

RNNs have made a big difference in ML by making it possible to handle sequential data in Figure 5 more efficiently. The advent of DL has revolutionized AI research and is responsible for recent successes in several domains, including medical diagnostics, autonomous vehicles, and image identification and natural language processing (NLP).

Long Short-Term Memory Networks (LSTM)

The vanishing gradient problem is an issue with basic RNNs; Hochreiter and Schmidhuber proposed LSTM

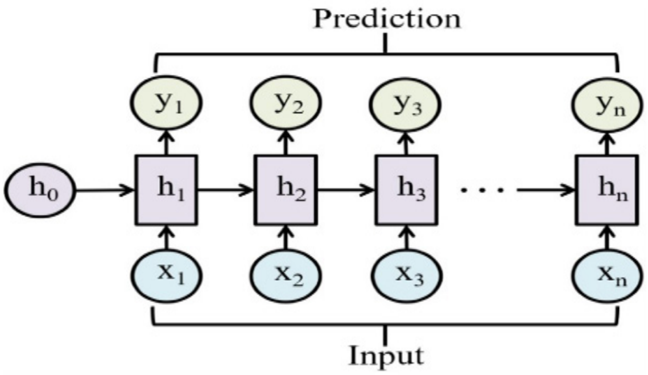

Figure 5: Basic RNN Architecture.

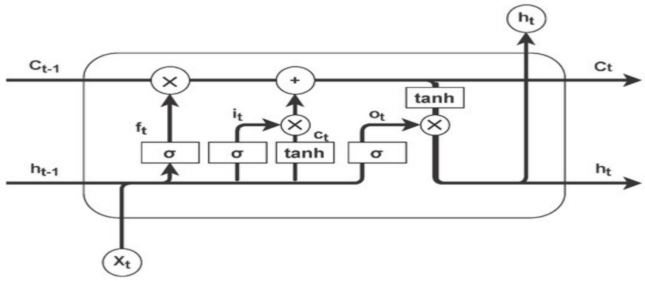

Figure 6: Architecture of the LSTM Network.

networks as an alternative. By controlling the input flow throughout the network using gating techniques, LSTM has achieved its primary goal. LSTM networks can mimic long-term dependencies very well due to their capacity to keep and update their internal state over lengthy periods of time.

The three gates that govern the cell state c*Z* (shown in Figure 6) and hidden state ht are the input gate, forget gate, and output gate, and they are present in every LSTM cell.

Gated Recurrent Units(GRU):

An alternate design that sought to streamline the long short-term memory (LSTM) structure and alleviate the vanishing gradient problem is the gated recurrent unit. By consolidating the input and forget gates into a single update gate, GRUs produce a more efficient and straightforward model by merging the cell state and hidden state (as seen in Figure 7).

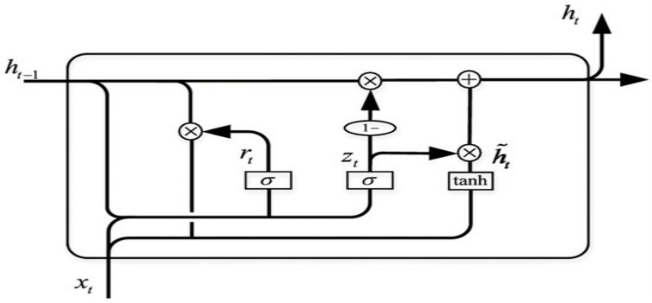

Figure 7: Architecture of the GRU Network

Networks are widely utilized in several fields such as visual identification, medical image analysis, image segmentation, NLP, and many more due to their ability to handle a variety of 2D shapes.

Convolutional Neural Networks (CNNs):

Object detection and segmentation in images, object recognition and classification, and object identification are all capabilities of CNNs, an AI system built on multi-layer neural networks. One well-liked discriminative deep learning architecture, CNNs or convolutional neural networks (ConvNets), may learn from input objects directly, eliminating the need for human feature extraction.

Generative Adversarial Networks (GANs)

GANs are state-of-the-art tools that bring together bioinformatics and artificial intelligence to generate gene expression data. Because it can produce synthetic data that resembles real-world data, the GAN paradigm offers an appealing solution to the inherent difficulties of gene expression investigations, including high dimensionality, sparse data, and sample variability.

The Machine Learning Methods in Intelligent Inhabitant Environment

The anomalies are detected using machine learning algorithms that are built and developed [16]. A widely used and highly effective technique for detecting anomalies literature review on machine learning

Table 1: The machine learning methods in intelligent inhabitant environment

Methods	*Nature of data*	*Type of anomaly*	*Availability of data*	*Type of sensor*	*Application area*
Single class support vector machine (SVM)	Binary data	Collective anomaly	Supervised learning over the pattern of normal behavior	State sensor deployed in living, kitchen and dining area	Smart home
Multi class SVM	Continous data	Collective anomaly	Supervised learning over the pattern of normal behavior	Accelerometer and gyroscope sensor	Wearable gadget
Principal component analysis (PCA) and Fuzzy rule-based system	Binary and Continous data	Collective anomaly	Supervised learning over the pattern of normal behavior	State and motion sensor	Smart home
Kernel nonlinear regression and SVM	Continous data	Contextual anomaly	Supervised learning over the pattern of normal behavior	Light, temperature, microphone, accelerometer	Human activities
Convolutional neural network (CNN) and Recurrent neural network (RNN)	Continous data with image	Collective anomaly	Supervised learning over the pattern of normal behavior	Microwave sensor and video camera	Smart home

approaches in intelligent occupant environments yielded the results shown in Table I.

Application of Deep Anomaly Detection in IoT

Deep anomaly detection has multiple uses. Across all possible use cases:

- **Intrusion Detection:** The purpose of an intrusion detection system (IDS) is to detect and prevent intrusions into computer networks and other related systems [17]. IDS can range from small, standalone systems called HIDS to massive, enterprise-level networks. There are two main types of network IDS: signature-based and anomaly-based.
- **Host-Based Intrusion Detection Systems (HIDS):** Software programs that are installed on a single host or computer that monitor system calls or events for signs of malicious activity or policy breaches are called such systems.
- **Network Intrusion Detection Systems (NIDS):** NIDS are concerned with scanning all network packets for malicious activity [18]. The data is big data in every sense: very large, very moving, very varied, and streamed in real time.
- **Fraud Detection:** The goal of fraud is to get unauthorized access to a valued resource. Fifty percent of the 7,200 businesses polled by PricewaterhouseCoopers (PwC) have fallen victim to fraud at some point. Fraud detection encompasses the identification of illegal activity in a wide range of sectors, as seen in Figure 8.

Governments and commercial companies alike face serious challenges due to fraud in the areas of telecommunications, health, vehicle, and banking (including claims for tax returns and credit card transactions). Since fraud evolves over time, it is difficult to detect and prevent.

- **Malware Detection:** The term “malware” refers to malicious software. Effective malware detection technologies based on machine learning are necessary to safeguard legitimate users from malicious digital content. There are typically two steps to malware detection in classical machine learning methods: feature extraction and classification/clustering. Previous methods of virus detection and their effectiveness.
- **Real-time Monitoring:** IoT sensors can measure things like temperature, pressure, motion, and performance indicators to keep track of the state of a system in real time. The data is sent without any delay to the analytical platforms thus, the identification of the unusual patterns or deviations becomes very fast
- **Smart security system:** Smart security systems deploy IoT-enabled cameras, motion sensors, and access devices to incessantly monitor surroundings. These systems recognize irregular activities like unauthorized entry, abnormal movement, or suspicious behavior. Instant alerts are dispatched to the users or security teams, thus, the response time is getting faster, the level of protection is being elevated and security risks are being minimized with the help of automated anomaly detection.

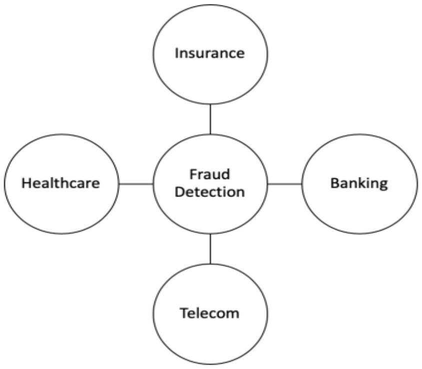

Figure 8: Fraud Detection Across Various Application Domains

Literature Review

This section reviews the research that came before concerning AI-based anomaly detection techniques in IoT systems. It explains how ML, DL, normal behavior changes of IoT. Table II summarizes the comparison of these works briefly, referring to their detection methods, applications, and Limitation faced by IoT environments

Sharma, Sharma and Lal (2019) Anomaly detection and Internet of Things security are major concerns. This survey paper provides a comprehensive overview of anomaly detection in IoT applications that utilize ML and DL algorithms. When it comes to identifying typical and non-standard actions taken by various parts of the IoT, ML and DL are potent tools. With an emphasis on research and the utilization of deep anomaly detection algorithms for low-resource devices, this paper lays out the main concerns and challenges surrounding the IoT [19].

Ayad et al. (2019) IoT ADS that is modular and hybrid. To centrally train a neural network and identify anomalies in both application and network levels, the proposed method employs cloud computing. IoT devices receive the learned neural network weights for local anomaly detection, which reduces communication detection delay [20].

Table 2: Comparative Analysis of recent studies of iot in anomaly detection using machine learning

Author / Year	*Study Focus*	*Key Technique / Approach*	*Application Area*	*Limitation*	*Future Work*
Sharma, Sharma & Lal (2019)	Survey on anomaly detection and security in IoT	Anomaly detection approaches based on Machine Learning and Deep Learning	IoT systems and devices	Resource-constrained IoT devices make deep anomaly detection difficult; high computational cost	Develop lightweight deep anomaly detection models suited for real-world IoT deployments
Ayad et al. (2019)	Modular hybrid anomaly detection system for IoT using cloud support	Cloud-based centralized training + neural network weights deployed to devices	Application and network layer anomaly detection in IoT	Dependent on cloud connectivity; still some delay in weight updating	Improve on-device learning, reduce latency further, and explore edge-based federated updates
Hoang & Nguyen (2018)	Lightweight anomaly detection for IoT using PCA	Principal Component Analysis (PCA) for complexity reduction	IoT networks with limited resources	PCA may lose accuracy with highly dynamic traffic; sensitive to noise	Enhance PCA-based detection formulas and integrate adaptive models for IoT environments
Nguyen et al. (2019)	Federated-learning–based IoT anomaly detection system (DÏoT)	Device-type-specific profiling + Federated Learning	IoT intrusion detection without labeled data	Performance depends on diversity of device types; federated models require coordination	Expand device coverage, improve robustness for unseen device types and large-scale deployments
Bhatt & Morais (2018)	ML-based IoT attack detection using a decision module	Machine Learning classifiers on a single-board computer	Smart home IoT security	Limited to tested attacks; may not cover new attack types	Extend model to wider attacks and improve generalization across heterogeneous IoT devices
Alghuried (2017)	Machine learning–based anomaly detection combining IWC and C4.5	Inverse Weight Clustering (IWC) + C4.5 decision tree	Industrial monitoring, business services, IoT data classification	Clustering quality dependent on initial parameters; scalability issues	Develop more scalable clustering models and integrate hybrid anomaly detection frameworks

Hoang and Nguyen (2018) Anomaly detection in IoT networks is an increasingly difficult task because of the limited resources and performance of these networks. Due to the ineffectiveness of comprehensive detection methods un IoT networks, it is necessary to design lightweight alternatives. One appealing strategy is to use Principal Component Analysis (PCA) methods, which simplify the process. Many prior standard research works have utilized principal component analysis (PCA) to detect anomalies; nevertheless, this work proposes an evaluation of PCA methodologies, a new universal formula for distance computation, and a novel detection approach for IoT networks [21].

Nguyen et al. (2019) The IoT relies on communication patterns that are customized to each type of device to identify unusual or harmful changes in device behavior, all without the need for human intervention or labelled data. No other system has ever used federated learning for anomaly detection-based intruder detection like this one has. Therefore, DÏoT is capable of handling threats that are both new and unknown. Demonstrated that DÏoT is both quick (257 ms) and very effective (95.6% detection rate) at detecting devices by methodically and thoroughly evaluating over 30 commercially available IoT devices over an extended period of time [22].

Bhatt and Morais (2018) A sophisticated detection system is necessary to safeguard this diverse environment from new assaults that target IoT devices in homes. an approach that employs a judgment module and machine learning techniques for the purpose of identifying assaults on IoT networks. By methodically testing it with various protocol assaults and commercially available IoT devices, the approach is demonstrated to function in a real-world context and tested on a single-board computer. The results of the experimental evaluation show that IoT devices can be protected against the assaults that are being examined with a detection accuracy ranging from 94% to 99% [23].

Alghuried (2017) A hybrid approach integrating the C4.5 decision tree algorithm with IWC is employed to identify anomalies within the IoT. An improved variant of the k-means technique, IWC is a potent instrument for effectively grouping data into clusters, which may be utilized to build decision trees for data classification.

Managing and keeping tabs on manufacturing facilities or enhancing business services or operations are two areas where it shines [24]

Conclusion And Future Work

Anomaly detection in IoT systems is a profoundly challenging problem which has attracted a lot of research attention over the last few years. The reviewed literature in this respect has been mostly representative for health care, industry, and smart cities domains. This review has covered a large number of ML and DL approaches for anomaly detection to be adopted in IoT systems, which include supervised, unsupervised, and hybrid methods. ML algorithms like DTs, SVM, and RF provide a good level of explanation and can be trained quickly, while DL networks such as CNNs, RNNs, and auto encoders are more flexible for the complex high-dimensional IoT data. Some recent works argue that moving towards multi-target anomaly detection, exploiting robust feature extraction, and real-time monitoring is crucial for further increase of accuracy and reduction of false alarms rate. Future research energy-saving anomaly detection algorithms capable of running directly on edge devices without any performance degradation developing comprehensive datasets for benchmarking and assessing models under real-world attack scenarios is of paramount importance. Besides, coupling anomaly detection with explainable AI (XAI) will be the next step to increase user confidence, system transparency, and wider deployment in critical application sectors.

References

M. binti M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*, 2016, pp. 381–385. doi: 10.1109/SEGE.2016.7589556.

L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in *Proceedings of the International Conference on Sensing Technology, ICST*, 2017. doi: 10.1109/ICSensT.2017.8304465.

M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.

P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, Feb. 2009, doi: 10.1016/j.cose.2008.08.003.

S. Garg, "Anomaly Detection And Event Correlation In Saas Operations," *Int. J. Core Eng. Manag.*, vol. 6, no. 4, 2019, doi: 10.5281/zenodo.17109813.

P. Pathak, A. Shrivastava, and S. Gupta, "A survey on various security issues in delay tolerant networks," *J Adv Shell Progr.*, vol. 2, no. 2, pp. 12–18, 2015.

M. Ahmed, A. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.

C. Noble and D. Cook, "Graph-based anomaly detection," in *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, Aug. 2003, pp. 631–636. doi: 10.1145/956750.956831.

S. Malallah, Y. Zalah, and R. Karne, "An Analysis of the Advanced Encryption Standard and Threats Associated," 2018, doi: 10.13140/RG.2.2.34873.88168.

S. Achouche, U. B. Yalamanchi, and N. Raveendran, "Method, apparatus, and computer-readable medium for performing a data exchange on a data exchange framework," 2019

V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541882.

M. A. Hayes and M. A. Capretz, "Contextual anomaly detection framework for big sensor data," *J. Big Data*, vol. 2, no. 1, p. 2, Dec. 2015, doi: 10.1186/s40537-014-0011-y.

H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology," in *2016 IEEE International Conference on Communications, ICC 2016*, 2016. doi: 10.1109/ICC.2016.7510811.

X. Xu, H. Liu, and M. Yao, "Recent Progress of Anomaly Detection," *Complexity*, vol. 2019, no. 1, Jan. 2019, doi: 10.1155/2019/2686378.

M. Fahim, "Anomaly Detection , Analysis and Prediction Techniques in IoT Environment : A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.

R. Chalapathy and S. Chawla, "Deep Learning for Anomaly Detection: A Survey," 2019, doi: 10.48550/arXiv.1901.03407.

J. Nkafu and J. Liu, "Survey of Application of Machine Learning Methods in The Development of Network Intrusion Detection and Prevention Systems," *2019*, pp. 1–15.

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. doi: 10.1109/ICCIKE47802.2019.900436.

A. Ayad, A. Zamani, A. Schmeink, and G. Dartmann, "Design and Implementation of a Hybrid Anomaly Detection System for IoT," in *2019 Sixth International*

Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2019, pp. 1–6. doi: 10.1109/IOTSMS48152.2019.8939206.

D. H. Hoang and H. D. Nguyen, "A PCA-based method for IoT network traffic anomaly detection," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, p. 1. doi: 10.23919/ICACT.2018.8323765.

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, pp. 756–767. doi: 10.1109/ICDCS.2019.00080.

P. Bhatt and A. Morais, "HADS: Hybrid Anomaly Detection System for IoT Environments," in *2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, 2018, pp. 191–196. doi: 10.1109/IINTEC.2018.8695303.

A. Alghuried, "A Model for Anomalies Detection in Internet of Things (IoT) Using Inverse Weight Clustering and Decision Tree," 2017, doi: 10.21427/D7WK7S.

Waditwar, P. (2026) De-Risking Returns: How AI Can Reinvent Big Tech's China-Tied Reverse Supply Chains. Open Journal of Business and Management, 14, 104-124. doi: 10.4236/ojbm.2026.141007

Padur, S. K. R. (2025). Automation-First Post-Merger IT Integration: From ERP Migration Challenges to AI-Driven Governance and Multi-Cloud Orchestration. *Int. J. Sci. Res. Sci. Eng. Technol*, *12*(5), 270-280.

Prajkta Waditwar. Agentic AI and sustainable procurement: Rethinking anti-corrosion strategies in oil and gas. World Journal of Advanced Research and Reviews, 2025, 27(03), 1591-1598. Article DOI: https://doi.org/10.30574/.

Zeeshan, M., Bhadauria, K., Pahal, L., Nagrath, P., & Kalla, D. (2025, June). Ensemble-Based Deep Learning for Automated Diabetic-Retinopathy Detection Using CNNs and Transfer Learning. In *International Conference on Data Analytics & Management* **(pp. 216-228).** Cham: Springer Nature Switzerland.

Prajkta Waditwar. Quantum-Enhanced Travel Procurement: Hybrid Quantum–Classical Optimization for Enterprise Travel Management. World Journal of Advanced Engineering Technology and Sciences, 2025, 17(03), 375-386. Article DOI: https://doi.org/10.30574/.

Routhu, K. K. Next-Generation Workforce Planning: AI-Enabled Forecasting and Strategic HR in Mergers and Acquisitions. *J Artif Intell Mach Learn & Data Sci 2025*, *3*(4), 2962-2967.

Prajkta Waditwar. Reimagining procurement payments: From transactional bottlenecks to strategic value creation. World Journal of Advanced Research and Reviews, 2025, 28(01), 588-598. Article DOI: https://doi.org/10.30574/.

Waditwar, P. (2024) AI for Bathsheba Syndrome: Ethical Implications and Preventative Strategies. Open Journal of Leadership, 13, 321-341. doi: 10.4236/ojl.2024.133020

NR, A. R., Rajasri, T., Praveen, R., Kalla, D., Bendale, S. P., & Venu, N. (2025, April). CAC Training-A Unified Cybersecurity Training Program for Military Staff. In *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)* **(Vol. 3, pp. 569-573).** IEEE.

Aggarwal, A., Agarwal, L., Rella, B. P. R., Nagpal, N., Kalla, D., & Sharma, M. (2025, June). A Performance Comparison of Machine Learning Models for Rain Prediction. In *International Conference on Data Analytics & Management* **(pp. 319-328).** Cham: Springer Nature Switzerland.

Padur, S. K. R. (2025). The future of enterprise ERP modernization with AI: From monolithic systems to generative, composable, and autonomous platforms. *J. Artif. Intell. Mach. Learn. & Data Sci*, *3*(1), 2958-2961.

Routhu, K. K. (2025). From Reactive to Predictive: A Strategic Framework for Attrition Analytics with Oracle 23AI. *European Journal of Advances in Engineering and Technology*, *12*(1), 29-34.

Prabakar, D., Iskandarova, N., Iskandarova, N., Kalla, D., Kulimova, K., & Parmar, D. (2025, May). Dynamic Resource Allocation in Cloud Computing Environments Using Hybrid Swarm Intelligence Algorithms. In *2025 International Conference on Networks and Cryptology (NETCRYPT)* **(pp. 882-886).** IEEE.

Nagaraju, S., Johri, P., Putta, P., Kalla, D., Polvanov, S., & Patel, N. V. (2025, May). Smart Routing in Urban Wireless Ad Hoc Networks Using Graph Attention Network-Based Decision Models. In *2025 International Conference on Networks and Cryptology (NETCRYPT)* **(pp. 212-216).** IEEE.

Vadisetty, R., Polamarasetti, A., & Kalla, D. (2025, February). Automated AI-Driven Phishing Detection and Countermeasures for Zero-Day Phishing Attacks. In *International Ethical Hacking Conference* **(pp. 285-303).** Singapore: Springer Nature Singapore.

Prajkta Waditwar. Overcoming the AI Data Eclipse: Obstacles to the Full Adoption of Artificial Intelligence in the Procurement Technology Sector. World Journal of Advanced Research and Reviews, 2025, 27(03), 1583-1590. Article DOI: https://doi.org/10.30574/.

Waditwar, P. (2025) Leading through the Synthetic Media Era: Platform Governance to Curb AI-Generated Fake News, Protect the Public, and Preserve Trust. Open Journal of Leadership, 14, 403-418. doi: 10.4236/ojl.2025.143020.

S. R. Sagili, V. K, B. Puli, P. Sundaramoorthy, M. R and K. N V, "Advancing Cervical Cancer Identification using Generative-based Adversarial Networks: An Integrative Learning Methodology," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/INCET64471.2025.11140170.

Waditwar, P. (2025) Agentic AI in Contract Analytics Harnessing Machine Learning for Risk Assessment and Compliance in Government Procurement Contracts.

Open Journal of Business and Management, 13, 3385-3395. doi: 10.4236/ojbm.2025.135179.

S. R. Sagili, S. Chidambaranathan, N. Nallametti, H. M. Bodele, L. Raja and P. G. Gayathri, "NeuroPCA: Enhancing Alzheimer's disorder Disease Detection through Optimized Feature Reduction and Machine Learning," 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 2024, pp. 1-9, doi: 10.1109/ICEEICT61591.2024.10718628.

Waditwar, P. (2025) AI-Driven Smart Negotiation Assistant for Procurement—An Intelligent Chatbot for Contract Negotiation Based on Market Data and AI Algorithms. Journal of Data Analysis and Information Processing, 13, 140-155. doi: 10.4236/jdaip.2025.132009.

Waditwar, P. (2025) Smart Procurement in the Sports Industry: A Strategic Approach for Efficiency and Performance Enhancement. Open Journal of Business and Management, 13, 1743-1761. doi: 10.4236/ojbm.2025.133090

Waditwar, P. (2025) Transforming Government Procurement through Electronic Bidding—A Case Study on the City of Somerville's Implementation of BidExpress Infotech. Open Journal of Leadership, 14, 165-175. doi: 10.4236/ojl.2025.141007

Waditwar, P. (2025) AI-Driven Procurement in Ayurveda and Ayurvedic Medicines & Treatments. Open Journal of Business and Management, 13, 1854-1879. doi: 10.4236/ojbm.2025.133096

Vanaparthi, N. R. (2025). The roadmap to mainframe modernization: Bridging legacy systems with the cloud. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(1), 125–133. https://doi.org/10.32628/

Vanaparthi, N. R. (2025). Why digital transformation in fintech requires mainframe modernization: A costbenefit analysis. International Journal of Science and Research Archive, 14(1), 1052–1062. https://doi.org/10.30574/

Vanaparthi, N. R. (2025). Intelligent finance: How AI is reshaping the future of financial services. International Journal of Computer Engineering and Technology, 16(1), 126–137. https://doi.org/10.34218/

Vanaparthi, N. R. (2025). Regulatory compliance in the digital age: How mainframe modernization can support financial institutions. International Journal of Research in Computer Applications and Information Technology, 8(1), 383–396. https://doi.org/10.34218/

Venkata, S. S. G. (2025). SECURE SOFTWARE DEVELOPMENT: INTEGRATING ENCRYPTION PROTOCOLS FROM DESIGN TO DEPLOYMENT. International Journal of Applied Mathematics, 38(2s), 1190-1213. https://doi.org/10.12732/ijam.

Venkata, S. S. G. (2025). From code to cloud: Navigating the future of software engineering and testing automation. International Journal of Basic and Applied Sciences, 14(6), 63–70. https://doi.org/10.14419/

Venkata, S. S. G. (2025). Audit: Risk Aware Software Security. QTanalytics Publication (Books), 67–75. https://doi.org/10.48001/978-

Kohli, H., Hadi, A., Mukhi, N., Miah, M. A., & Siddiqa, K. B. (2025). Energy-Aware Intelligent Computing Framework for Sustainable AI Workloads in Next-Generation Smart Systems. International Journal on Smart & Sustainable Intelligent Computing, 2(4), 34-47.

Routhu, K. K. Next-Generation Workforce Planning: AI-Enabled Forecasting and Strategic HR in Mergers and Acquisitions. *J Artif Intell Mach Learn & Data Sci 2025*, *3*(4), 2962-2967.

Kohli, H., Hadi, A., Mukhi, N., Miah, M. A., & Siddiqa, K. B. (2025). Energy-Aware Intelligent Computing Framework for Sustainable AI Workloads in Next-Generation Smart Systems. International Journal on Smart & Sustainable Intelligent Computing, 2(4), 34-47.

Jain, A., Kotha, S. S. M., Bhambri, S., & Kohli, H. (2025, March). Machine Learning Pre-trained Language Models for English-French Neural Machine Translation using Topsis. In 2025 IEEE International Conference on Contemporary Computing and Communications (InC4) (pp. 1-6). IEEE.

S. R. Sagili, C. Goswami, V. C. Bharathi, S. Ananthi, K. Rani and R. Sathya, "Identification of Diabetic Retinopathy by Transfer Learning Based Retinal Images," 2024 9th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2024, pp. 1149-1154, doi: 10.1109/ICCES63552.2024.10859381.

Agarwal, K., Bhambri, S., Sridharan, V. K., Mohammed, N., Kohli, H., & Kapoor, J. A. (2025, March). Performance Evaluation of different Machine Learning Techniques for Pothole Detection. In 2025 IEEE International Conference on Contemporary Computing and Communications (InC4) (pp. 1-8). IEEE.

Kohli, H., Mokashi, S. P., Sundaramoorthy, P., Jangid, D., & Chaganti, K. (2025, July). AI-NLP Framework for Customer Segmentation and Personalized Recommendations in Digital Marketing Environments. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 146-151). IEEE.

S. R. Sagili and T. B. Kinsman, "Drive Dash: Vehicle Crash Insights Reporting System," 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA), Pune, India, 2024, pp. 1-6, doi: 10.1109/ICISAA62385.2024.10828724.

Waditwar, P. (2024) The Intersection of Strategic Sourcing and Artificial Intelligence: A Paradigm Shift for Modern Organizations. Open Journal of Business and Management, 12, 4073-4085. doi: 10.4236/ojbm.2024.126204.