African Multidisciplinary
Journal of Sciences and Artificial Intelligence

ISSN : 3434-9871

Index: Harvard, Boston, Sydney University, Dimensions, Lens, ResearchGet Scilit, Semantic, Google Scholar, Base etc

https://doi.org/10.58578/AMJSAI.v1i2.4014

Machine Learning Algorithms for Anomaly Detection in IoT Networks – A Review

Muhammad Mamman Kontagora & Bartholomew Idoko
Nasarawa State University, Keffi, Nigeria; Federal Polytechnic Ohodo, Enugu, Nigeria
bartholomew.idoko@fedpod.edu.ng; mohakontagora14@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Sep 24, 2024	Oct 7, 2024	Oct 21, 2024	Oct 26, 2024

Abstract

Internet of Things (IoT) wide applications has significantly increased the need for robust anomaly detection to safeguard against countless security breaches. This paper presents a review that examines the effectiveness of hybrid solutions incorporating supervised and unsupervised machine learning models for enhancing IoT security. The review consolidates insights from a range of studies employing models such as Random Forest (RF), Support Vector Machine (SVM), k-nearest Neighbors (k-NN), and Gaussian Mixture Models (GMM). It integrates the findings of diverse research, emphasizing improvements in terms of detection accuracy and computational demands. The study delineates challenges in the field to evaluate the efficacy of hybrid techniques and their potential for immediate IoT security applications. Moreover, future research directions encompass the exploration of new algorithms and the integration of these approaches within dynamic IoT data streams.

Keywords*:* Security*,* IoT, Detection*,* Hybrid Methods, Networks, Machine Learning

AMJSAI Journal is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

Introduction

The Internet of Things or IoT is a category of technology that is widely regarded as having disruptive potential in connecting essentially anything to the Internet. It is predicted that by the year 2025, more than thirty billion internet-enabled gadgets will be linked to the IoT Network, showing the dramatic expansion and adaptation of IoT in various sectors of life (Lee and Kim, 2017; Eddine et al., 2021). Nevertheless, the exponential growth in the number of connected devices also increases the potential for security threats, especially since many IoT gadgets have insufficient data computation and storage capacities. These limitations make IoT devices vulnerable to misuse and this creates immense security concerns as the network progresses. Leading into the description of the IoT refers to a complex chain of automated systems with the ability of collecting, storing, and analyzing data and sharing the same with different units. The adaptation of IoT technology has created massive advancements in numerous sectors including manufacturing, homes, monitoring of the climate, industries, and business activities resulting in better standards of living, and increased production among others, hence boosting the economy. Nonetheless, IoT brings several measurable benefits, and its maturity is achieved through significant security risks and attacks due to the increased number of potential targets in its infrastructures, applications, and services. The adoption of novel protocols and new ways of dealing with tasks has rapidly grown, which has by far multiplied the chances of risking and combating vulnerabilities and threats (Alsoufi et al., 2021). An example of these vulnerabilities is the Mirai botnet attack where IoT vulnerabilities were targeted and this led to high disruptions in the websites and domain name systems (Njilla et al., 2019). The use of smart mobile devices which are owned by the general public has helped shape the expansion of IoT through all fields and sectors of practice such as health, the real estate, and the construction of smart cities by Virat et al. (2018). IoT devices have Network Interface Cards and embedded microprocessors with very low power consumption capabilities multiple interface services are used in IoT devices for management and operation. The likely effects of IoT on our shared future are incumbent on technological progression as we look forward to the contemporary century. However, the rapid expansion of IoT networks has brought security to the forefront as a major challenge for these interconnected systems. Some of the risks associated with IoT device connectivity include potential attacks from hackers, viruses, and other forms of malware targeting the connected gadgets. These threats are not only a threat to data but also to the IoT networks

overall, putting individuals into possibly dangerous conditions (Alaa et al., 2017; Panagiotis et al., 2021; Maglaras et al., 2020). Therefore, there is a need for effective security measures to protect the IoT systems that are increasingly used in the modern world. In the evolving landscape of technology, the proliferation of IoT devices and the emergence of new threats necessitate the collection and analysis of data to ensure the security and optimal performance of these devices in the days ahead. These imperatives have elevated the importance of IoT security to a prominent position in ongoing industry discussions. As it becomes evident securing IoT devices is not an easy accomplishment as indicated earlier. Most of these devices are diverse and have limited resources, making traditional security models irrelevant. Additionally, IoT networks are usually distributed, so traditional perimeter security measures may not be effective. At the same time, centralized systems like cloud infrastructures can have latency issues and drawbacks related to centralization. Moreover, due to hasty development and inadequate security measures, many IoT device manufacturers prioritize market intrusion over implementing proper secure approaches and mechanisms. Owing to the lack of protocols to secure the IoT devices, the assignment becomes more challenging. It is important to design monitoring systems capable of identifying abnormalities at both the device and network levels, extending beyond organizational boundaries. In the context of IoT networks or data, outliers or outlier patterns may be defined as patterns or sequences detectably different from the mean. Analyses can be referred to in terms of different types depending on factors such as; their nature and source. Local anomalies can therefore refer to fixed anomalies that occur once only; these deviate from the normal working of an organization or go against the trend of a certain parameter. In some cases, observations may be considered outliers within one condition but abnormal in a different context (e.g., within a specific time frame). These anomalies can be influenced by factors such as time, location, and behavioral aspects related to the application domain. Collective anomalies are a set of data points where the data is familial, sequential, spatial, or data in graph forms which may be abnormally behaving as a group but the individual cases may not seem very abnormal. These anomalies have significant negative implications for businesses and government operations, despite occasionally being amazing (Cook et al., 2020). Given the security requirements of both traditional IT systems and the Internet of Things, intrusion detection systems (IDS) are made to alert users early when certain events or attacks are about to occur. Intrusion detection systems (IDSs) fall into two main categories: anomaly-based and signature-based.

These subcategories are based on different methodologies. Anomaly-based IDS are designed to detect novel or unidentified attacks, such as zero-day attacks, that diverge from the expected or standard behaviour pattern (Doshi et al., 2020). Alternatively, unless fresh signatures are created and disseminated, the signature type of IDS is less effective against emerging or evolving threats since it operates based on the attack signatures that are received (Doshi et al., 2020). This makes anomaly-based IDS well-suited to handle the dynamic nature of IoT system security threats. Regardless, because IoT devices create large amounts of data, effective algorithms are needed to identify features that indicate suspicious behavior, while existing approaches are heavily computationally intensive due to noise. Therefore, it is wise to adopt lightweight distributed IDS based on anomalies as a method of protection from cyber threats in IoT networks. Existing self-protection strategies for IoT are system security architecture and cryptographic security. Yet, IoT networks are still exposed to different types of network attacks; for instance, when there is an overload of inquiries or when other people try to access different services unlawfully, the impacts may be dreadful (Adat and Gupta, 2018; Yang et al., 2020). Hence there is a need to install Intrusion Detection Systems (IDSs) for the monitoring of IoT arenas and protection of network availability and security. While IDSs are essential for IoT networks and their security, low-power devices and restricted resources in IoT systems might pose difficulties in the efficient and effective implementation of IDSs. An IDS is designed to watch the status of a network, and the status of the traffic routinely; it notifies the administrators whenever incursions are noticed (Mbarek et al., 2015). However, the traditional IDS architectures that were designed for managing priorities of the Internet do not work well when encountered with the probabilities of volumetric and sequential variations in the form of event streams shown by the IoT networks (Fu et al., 2011). This disparity underscores the language for more specific and optimal intrusion detection services that can work within the confines of IOT devices as they meet the ever-evolving security threats in the relatively burgeoning sector. In recent years, the areas related to machine learning have demonstrated the possibility of designing IDSs for IoT systems based on the anomaly detection method. Such techniques incorporate methodologies that involve using datasets containing both normal and abnormal data for training the models to identify anomalies in real time (Alsoufi et al.,2021; Njilla et al., 2019). Despite the potential of machine learning, constructing effective anomaly detection systems remains challenging due to several inherent limitations. Typical approaches to machine learning of

classical paradigms can fail to identify the appropriate features from the data, which are subsequently incapable of providing reliable discrimination between normal behavior and anomalies. Also, the use of machine learning models in the IoT devices is a critical problem because these kinds of models need high computing power which could not be available in most resource constrained IoT devices. Moreover, anomaly detection accuracy improves with more training data for modeling normal behavior. This is where machine learning models can be limited in predicting all cyber-attack possibilities or suspicious activities to occur if the set training data is inadequate or non-inclusive of all the other alternatives, hence resulting in false positives and false negatives. Yet, several stimuli have aided the improvement of machine learning in the recent past; these include modern hardware like GPUs and the current complex architectures for neural networks including depth learning. These advancements portend a bright future for the use of MLS, particularly for anomaly detection, on cutting-edge platforms like blockchain.

Anomaly Detection Using Machine Learning Methods

Anomaly detection in the IoT context is important particularly due to the highly distributed and loosely coupled nature of things in the IoT environment and particularly due to the highly heterogeneous nature of IoT and limited resources available. Academic research has indicated that machine learning (ML) is one of the most effective and widely used techniques for identifying peculiar events in IoT ecosystems mainly because it has the capability of analyzing big data to detect possible security breaches or system failures. In this section, the present study discusses different machine learning approaches that have been used to perform anomaly detection in IoT, as well as their key features and applications. Machine learning for IoT anomaly detection involves several factors that need to be taken into account. Three categories of learning algorithm techniques may be distinguished: semi-supervised, unsupervised, and supervised. Federated learning is the process of training the learning algorithms across a large number of dispersed IoT devices. Furthermore, the dimension of the existing data may be used to understand anomaly detection, which leads to univariate and multivariate-based methods.

Supervised Learning Technique

Supervised learning is conducted on data that contains a final result or examines the instances of outliers. These are some of the most commonly used algorithms by

organizations and companies: – Support Vector Machines (SVMs) – Decision Trees – Neural Networks. Supervised algorithms, sometimes referred to as discriminative algorithms, use labeled cases to facilitate classification-based learning. These methods include neural networks (N.N.), support vector machines (SVM), Bayesian networks, K-nearest neighbor (K.N.N.), and neural networks (Hastie et al., 2009; Murphy, 2013). One of the distance-based anomaly detection techniques, K.N.N., is used when an anomalous point's distance from the bulk of the dataset is larger than a predetermined threshold. Due to the computational complexity of calculating the distances, it appears that this approach cannot be used to offer on-device anomaly detection. SVM, on the other hand, offers a hyperplane for classifying data points. Similar to K.N.N., it requires so many resources that using it for IoT anomaly detection is not feasible. Despite its low accuracy, the Bayesian network can be used for devices with limited resources since it does not always require previous knowledge about neighboring nodes for anomaly detection. Finally, many regular datasets have been used to train neural network (N.N.) algorithms to identify abnormal data by detecting deviations from the norm. Adapting N.N. algorithms to the IoT context is challenging due to their resource requirements. Supervised algorithms, which require significant resources and labeled datasets, are therefore not very suitable for use in IoT anomaly detection systems.

Support Vector Machines (SVMs): SVMs can be applied to IoT anomaly detection since high dimensional spaces can be ably processed by this model of algorithms. For instance, Thakkar and Lohiya (2021) presented the efficiency of using SVMs to perform anomaly detection in smart grid networks. They argue that since SVMs can find the hyperplane that provides the best separation of the two classes of data: normal and anomalous, they were able to assess high accuracy (Thakkar & Lohiy, 2021).

Decision Trees: As a recursive technique, Decision Trees are a very simple yet very effective method of anomaly detection through the division of the data space. Highly effective when we are looking for the interpretability of a model and they are not difficult to implement. Abdelaziz, Ahmed, and Ali Ahmed designated the Decision Trees to detect abnormal signs in both real-time healthcare IoT applications in 2020.

Neural Networks: Deep learning neural architectures, the most prominent of which is a neural network, have demonstrated notable success rates in handling intricate anomaly detection in Internet of Things systems. Because they can learn hierarchical representations

of data, they are very helpful for looking for little abnormalities in vast volumes of structured data. Because the model can identify geographical information, Al-Garadi et al. (2020), for instance, used CNN to analyze patterns of harmful behavior for IoT sensor data with high rates of detection.

Unsupervised Learning Techniques

Clustering or any other unsupervised learning approach does not involve the use of a labeled dataset and is useful for newly emerged or novel anomalies. Clustering techniques such as k-means and Principal Component Analysis (PCA) represent the conventional approaches to view this type of data. Unsupervised algorithms, sometimes referred to as generative algorithms, employ unlabeled data to acquire hierarchical characteristics. Unsupervised methods that use similarity and density features to group data points into clusters include clustering-based algorithms like K-means and density-based spatial clustering of applications with noise (D.B.S.C.A.N.) (Hastie et al., 2009; Murphy, 2013). Normal points are either within or adjacent to the clusters, whereas abnormal points are little data points that are substantially removed from the dense region. To increase the accuracy of anomaly detection, clustering methods are typically employed in conjunction with classification algorithms. The majority of clustering methods are not suitable for direct application to IoT devices for anomaly detection due to resource consumption. Utilizing dimension reduction techniques like P.C.A. and A.E. to eliminate noise and redundancy from data to decrease the original data's dimension is another unsupervised learning method (Murphy, 2013; Chadha et al., 2021). Although P.C.A. has been used widely for anomaly detection, the dynamic IoT environment does not work well with it. Reducing data volumes and reconstructing mistakes to identify anomalous points are two areas where A.E. has demonstrated promising outcomes in IoT anomaly identification. Nevertheless, feature extraction for classification algorithms has made substantial use of these approaches. IoT anomaly detection can benefit from an adaptation of unsupervised learning's dimensionality reduction methods. By using examples of typical data, semi-supervised algorithms blend the strengths of generative and discriminative algorithms, seeing deviations from the norm as aberrant behavior. Therefore, regular system monitoring is used as a baseline environment for anomaly detection in the Internet of Things, with an emphasis on unsupervised or semi-supervised algorithms (Jiang et al., 2020). k-Means Clustering: In k-Means clustering, data points are usually grouped so that anomalies are those points that do not belong to any formed cluster. Zhang et al. (2020)

used k-means clustering on the network traffic data associated with the IoT system, and the anomalies could be easily observed during the process of clustering as outliers.

Principal Component Analysis (PCA): PCA preserves data variance and transforms the data into other unrelated features, making it useful for identifying outliers. Ding et al. (2021) utilized PCA to distinguish anomalous traffic in smart city IoT. They explored a method with minimal computational burden that could detect changes in the normal operational characteristics of IoT networks.

Semi-Supervised Learning Techniques

Semi-supervised learning methods utilize a small set of labels alongside a huge number of samples not labelled. In this sense, this approach is most valuable for IoT, because labeled anomaly data may be hard to obtain.

Autoencoders: An autoencoder is a model that is trained to take in data and spit out the same data in a new form. The last statement is used for discovering anomalies – the higher the value of the reconstruction error, the higher the probability of the irregularity. Lee et al. (2020) applied autoencoders for anomaly detection in IoT systems; the model can learn from normal data and alert the system for abnormality with higher accuracy.

Gaussian Mixture Models (GMMs): GMMs is a probabilistic model within the expectation maximization framework that assigns all data points from a given dataset a probability distribution made up of a combination of several Gaussian models. They are useful when it comes to anomalies as a technique that fits the probability model and results in flagging data points with a low occurrence probability. Su and colleagues exploited GMMs for anomaly detection in IoT networks in their study (Su et al. 2019) where the model demonstrated a good ability to identify network traffic between normal behavior and abnormities.

Ensemble Learning Techniques

Ensemble learning aims to enhance the efficiency and reliability of the built models by incorporating several algorithms into a single framework for anomaly detection.

Random Forests: Random Forests combines several decision trees to improve the detection abilities as they use random vectors that subdivide the dataset into randomized subsets. For identifying the anomalous flows of IoT traffic, Nabil et al., (2020) employed a

Random Forest where the ensemble showed enhanced results in terms of both identification and lowering false positive rates.

Boosting Algorithms: This includes methods like Gradient Boosting where models are built in steps, and the emphasis is made on the mistakes made by prior models. This method has been proven to be efficient in identifying intricate patterns of turbulence. For example, Zeng et al. (2020) employed Gradient Boosting to improve IoT-based smart grid anomalous behavior detection since it can detect normal and other complicated anomalies.

Federated Learning Algorithms and Model Training

IoT devices may train machine learning models locally via federated learning, often referred to as collaborative learning. The trained models rather than the local data—are sent to the server for aggregation (Mothukuri et al., 2021; Liu et al., 2021). This training technique differs from the conventional machine learning training methods, which call for centralizing the training data on a server or data center. There are four primary phases in the federating learning process. To identify anomalies, the server first initializes a global machine-learning model. The next step is to choose which IoT devices will receive the initialized model. Each chosen IoT device will then use its local data to train the model and send the improved model back to the server. The server will combine all received models to create the global model. The server will then send the completed model to every IoT device to identify any abnormalities. It's important to note that if some devices are not available during the federated computation or drop out during each round, the server may need to repeat the process of choosing a subset of IoT devices, sending the global model, receiving the trained models, and combining them more than once. Federated learning allows for the decentralization of data inside the Internet of Things while maintaining data privacy. Federated learning also offers the benefits of reduced latency, reduced network load, reduced power consumption, and cross organizational application. Federated learning does, however, have several shortcomings, including model poisoning (Wang et al., 2021) and inference assaults (Lee et al., 2021).

Univariate IoT data is data representation from a single IoT device over time. Information from multiple IoT devices positioned in complex environments is used by anomaly detection systems. These multivariate multi-sources provide noise-tolerant temporal and geographical information, hence feeding richer contexts than a single source.

Univariate Non-Regressive Method

By establishing low and high thresholds of observations on univariate stationary data, threshold-based processes in the non-regressive scheme may be utilized to identify anomalies if a data point crosses the boundary. This min-max strategy can be replaced with more sophisticated processes, such as mean and variance thresholds generated over previous data. Using a box plot to divide the data distribution into many smaller groups and compare newly collected data points to the boxes is another comparable method. For IoT devices, these non-regressive methods are perfect for conserving resources like CPUs and memory. However, because range-based systems are spread across univariate observations and cannot capture temporal linkages, they are unable to identify contextual and collective abnormalities (Cook et al., 2020). Using univariate time series data, N.N.s like A.E.s, recurrent neural networks (R.N.N.), and long short-term memory (L.S.T.M.) can be employed as non-regressive models to address the issue of anomaly identification in the IoT ecosystem. A large reconstruction error most likely denotes abnormality. A.E. is utilized to recreate data symmetrically from the input to the output layer (Yin et al., 2020). IoT devices with limited resources can also use A.E. to save battery life and resources. R.N.N., on the other hand, gives the network memory by influencing neurons from earlier outputs via feedback loops. This makes it possible to record temporal contexts across time. RNN's vanishing gradient issue renders it inappropriate for extensive IoT networks. To overcome this error problem, L.S.T.M. can offer semi-supervised learning on normal time series data to find anomalous sequences from the reconstruction. Therefore, it appears that merging A.E. and L.S.T.M. can address the accuracy and resource-saving needs of IoT anomaly detection applications.

Univariate Regressive Method

Regressive methods, which are predictive methodologies, allow one to find abnormalities in time series data by comparing the expected value to the actual value. Despite issues with mean shift or seasonality in non-stationary datasets, parametric models like autoregressive moving averages (A.R.M.A.) remain popular methods. However, improved versions of A.R.M.A., including seasonal A.R.M.A. and autoregressive integrated moving average (A.R.I.M.A.), can be used to alleviate these issues. NN-based prediction models like M.L.P., R.N.N., L.S.T.M., and others may be used to capture the dynamics of a time series on complicated univariate data as an additional method of predictive IoT anomaly detection

(Jiang et al., 2020). To estimate the anticipated values for time sequences, for example, R.N.N., L.S.T.M., and G.R.U. models can reflect the variability in time series data. Attention-based algorithms have been used recently to detect IoT anomalies in intricate, lengthy sequential data. Sequential models have the potential to improve IoT anomaly detection accuracy in a manner akin to the non-regressive approach, provided that feature extraction can employ dimensional reduction techniques.

Multivariate Using Regressive Scheme

Techniques such as P.C.A. and A.E. can be used to reduce data size when the number of variables increases. For multivariate sources, P.C.A. can capture the interdependence of variables. It accomplishes this by breaking down multivariate data into a smaller set. The application of P.C.A. for IoT anomaly detection may be constrained by its linearity and computational complexity. Similar to P.C.A., A.E. uses reconstruction error to identify abnormalities in multivariate time series data, just as it does in univariate situations. A.E.'s non-linear feature extraction and minimal resource consumption are its most promising aspects. Anomalies in multi-source IoT systems may also be identified utilizing approaches using L.S.T.M., CNN, DBN, and other models, much like in predictive and non-predictive models on univariate data. A.E. can specifically come before CNN and L.S.T.M. algorithms to save resources and extract significant features. According to Shukla et al. (2020), these deep learning techniques are capable of learning spatiotemporal elements of multivariate IoT data. Graph networks can be used to create models for variable or sequence interactions, where an anomaly is defined as the graph nodes' weakest weight. Another method for detecting anomalies in multivariate data is through clustering processes. When analyzing anomaly detection techniques for IoT systems, it becomes apparent that machine learning techniques hold great promise, each with its advantages and limitations. Supervised learning is effective when labeled data is available, while unsupervised learning is crucial for identifying unknown abnormal cases without relying on a known classification set. Semi-supervised approaches are practical as they make use of a combination of both labeled and unlabeled data for detection, while the ensemble approach utilizes multiple models simultaneously for improved detection rates. The continuous refinement of these techniques, coupled with advancements in both hardware and computational processing power, indicates the potential to address security issues in the IoT environment.

Performance Indices & Performance Measures (Evaluation Metrics)

The assessment becomes useful when considering machine learning in the context of anomaly detection in the industry of the Internet of Things (IoT). The measures provide methodologies in gauging the outcome of the tested anomaly detection techniques, the best performing algorithms, and the applicability of such algorithms. The following is a brief review of the commonly used performance measures: This section also covers the role of each measure as well as important performance analysis techniques. To facilitate better understanding, some hypothetical examples have been as provided below along with the tables containing the metrics and their regular use.

Accuracy

Accuracy is the purest of the measures, the simplest method that shows the ratio of the correctly identified both normal and anomalous instances to the total number of instances. It is given by:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

The parameters are defined thus:

TP is the True Positives,

TN is the True Negatives,

FP is the False Positives,

FN is the False Negatives.

Strengths: It presents the unified measure of group performance or comparative measure between two or more groups.

Limitations: It may be proactively inclined in imbalanced datasets containing an evidently greater number of normal instances as compared to the anomalous ones (García-Teodoro et al., 2009).

Precision and Recall

Precision measures the proportion of correctly identified anomalies to the total number of instances classified as anomalies:

$$Precision = \frac{TP}{TP + FP}$$

Recall (or Sensitivity) measures the proportion of actual anomalies that are correctly identified:

$$Recall = \frac{TP}{TP + FN}$$

These metrics are comparatively very useful in those scenarios where the number of false positive and false negatives must be compromised.

Strengths: Precision enables the identification of the degree to which identified anomalies are relevant while, recall targets identifying all actual anomalies.

Limitations: It is still important to consider both to get the whole picture because problematic use of one may influence the other (Sokolova & Lapalme, 2009).

F1-Score

The F1-Score is the harmonic mean of Precision and Recall and is used to balance them:

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Strengths: Encapsulates Precision and Recall in one number thus making it easier to compare different models.

Limitations: It may not accurately expose the trade-off area of Precision and Recall in the cases of highly skewed datasets (Powers, 2011).

Area under Receiver Operating Characteristic Curve (AUC-ROC)

Plotting the true positive rate against the false positive rate at different probability thresholds yields the AUC-ROC, a graphical depiction of a binary classifier system's diagnostic capacity. At different threshold values, the True Positive Rate (TPR) against the False Positive Rate (FPR) could be plotted thus:

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

This index AUC has a scale or range of 0 to 1 where AUC is closer to 1 is equal to optimal model performance.

Strengths: Offers an overall measure of the model's ability of classifying patterns as belonging to one class or the other.

Limitations: It does not use real market values (Bradley, 1997).

Confusion Matrix

This offers a thorough analysis of the predicted and actual classifications, allowing for the calculation of the metrics:

Table 1: Confusion Matrix

	Predicted Normal	Predicted Anomalous
Actual Normal	TN	FP
Actual Anomalous	FN	TP

Strengths: This provides a clear and detailed description of the performance of the classification models.

Limitations: It needs further analysis and inspection and it's not measured with one specific indicator (Sokolova & Lapalme, 2009).

Performance Analysis Strategies

Cross-Validation

Cross-validation means that the observed dataset is randomly split up into the training dataset and the testing dataset in various fashion to check the efficiency of a model with different splits of the observed dataset. k-fold Cross-Validation is a standard method where every dataset is divided into K subsets and the ML algorithm is trained and validated for K times, at every iteration we use one of the K subsets as a test set.

Strengths: It reduces the probability of obtaining high scores on the training data that do not translate to higher scores on other data.

Limitations: It is statistically and computationally intensive. It can also be time-consuming in the case of large datasets (Kohavi, 1995).

Hold-Out Validation

In this scenario, the dataset is split into two separate sets: There usually is the training dataset and there is the testing set. It is equally important for the part of the data to be divided in the same ration as 70-80% for training, 20-30% for testing.

Strengths: Easier to work/implement and requires less computational power as compared to cross-validation.

Limitations: These measures may be affected by the split and that may provide more or less accurate results in certain cases (Reitermanova, 2010).

Stratified Sampling

This is advantageous in situations where there is imbalance in the construction of the classes as it preserves the construction of classes in the training and test set just like in the original population in stratified sampling.

Strengths: Makes sure that the anomalous and normal examples are distributed fairly among the splits.

Limitations: They are even more complicated to undertake in comparison to methods using random sampling (Seiffert et al., 2010).

Anomaly Scoring and Thresholding

Anomaly scoring and thresholding is the process of applying scores to anomalous data instances and setting a threshold for them.

Anomaly detection models as a rule imply the output of scores instead of binary classes. The next step in the process is thresholding, in which the analyst sets a score threshold to define what a 'normal' is and what is an 'abnormal' instance.

Strengths: Extends the ability to fine-tune the proposed model by adjusting Precision and Recall requirements.

Limitations: The problem of deciding the appropriate value for the said thresholds is not easy and the knowledge of the domain is often required (Chandola et al., 2009).

Comparative Analysis of Techniques and Case Studies

As shown in Table 2, there are several models commonly studied, and this table group's common machine learning techniques for Internet-instrumented devices, with measurement statistics from past studies.

Table 2: Performance Comparison of Anomaly Detection Techniques

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Support Vector Machine (SVM)	0.92	0.89	0.85	0.87	0.91
Decision Tree	0.88	0.84	0.81	0.82	0.87
Neural Network	0.94	0.92	0.90	0.91	0.94
k-Means Clustering	0.85	0.80	0.78	0.79	0.83
PCA	0.87	0.83	0.79	0.81	0.85
Autoencoder	0.93	0.90	0.88	0.89	0.92
Random Forest	0.91	0.87	0.86	0.86	0.90
GMM	0.86	0.82	0.77	0.79	0.84

Smart Grid Networks

For anomaly detection models in smart grid networks, they need to deal with big data and real time analysis is often required for anomaly identification. This has been applied effectively through the utilization of SVMs due to their efficiency in handling higher dimensions of data and making fast determinations regarding the outliers. According to Thakkar and Lohiya (2021) various experiments conducted proved accuracy of including SVMs in the detection of unauthorized access and alerts for different unusual energy consumption pattern (Thakkar and Lohiya, 2021).

Healthcare IoT

Indeed, it is very important to identify characteristics of anomalies that can later help intervene before the situation worsens in healthcare applications. Decision Trees have been used to analyze various health parameters in the context of human diseases and conditions and determine if they follow a passed concept. Abdelaziz et al. (2020) found that Decision Trees could provide monitoring and detection capabilities of end-point health data when combined with a wearable device.

Industrial IoT

When applied to an industrial environment, often assets and processes are characterized by IoT endpoints; therefore, the anomaly has to be detected to avoid failures. Deep learning, specifically Convolutional Neural Networks (CNNs), has been utilized for diagnosing device faults using sensor data at an early stage. Al-Garadi et al. (2020) recognized the effectiveness of CNNs in accurately predicting the probabilities of equipment failure, leading to reduced maintenance time and costs. Therefore, it is crucial to have a good understanding of the performance metrics and analysis methods when evaluating anomaly detection models in IoT platforms. Performance measures include Accuracy, Precision, Recall, F1-Score, and AUC-ROC to gauge model effectiveness. Techniques such as cross-validation, hold-out validation, stratified sampling, and anomaly scoring play a vital role in accurate performance evaluation. The comparative analysis of various machine learning techniques provides valuable insights into their potential for use in IoT applications, based on the specific requirements for such models. This approach ensures that the deployed anomaly detection models are truly capable of safeguarding IoT systems against new and emerging threats.

Conclusion

The process of protecting IoT networks for anomaly detection using machine learning is challenging but also fascinating. By analyzing current issues and exploring new directions in more detail, we can enhance the security of IoT systems against emerging threats. By collaboration and facilitating the ongoing advancement of machine learning, an enhanced secure and consistent progress can be achieved for an IoT-enabled world, which serves as the groundwork for future technologies. Witnessed in modern societies is the advancement of IoT in the world within the last decade. Nevertheless, the use of IoT devices increases the level of threat since there are numerous entry points for attacks and several drawbacks connected with the usage of IoT devices. Based on insights provided in this journal, the role and key issues related to anomaly detection in IoT networks employing a machine learning approach have been pointed out with a focus on the necessity of security measures against possible threats.

It may be beneficial to incorporate the ML- tuned anomaly detection systems with the next-generation technologies like blockchain and edge computing in managing and securing

IoT networks. Blockchain can create distributed and immutable records of the events and edge computing can help in performing the analysis in a more efficient and less bandwidth consuming nearer to the source (Conti et al., 2018).

In summary, there is a need for effective lightweight and efficient models for anomaly detection to be implemented in IoT devices that have limited computing capability. The future studies should retain the balance of computations and detection efficiency and enhance key areas with improvements, using graphics processing units, GPUs in particular (Yuan et al., 2019).

The risks faced by these IoT networks being expanded by the evolution of the IoT networks could be mitigated by adapting to evolving threats. Regular checks of the model and its update will help to have a suitable model for detection of the new and more sophisticated attacks, incorporating adaptive learning concepts. Strengthening the security of IoT requires cooperation between different industry players and academics in creating and establishing transparent controls that help to identify susceptibilities and create suitable countermeasures (Fernandes et al., 2021).

The need to emphasize on data privacy and ethics cannot be over emphasized because as the number of IoT devices continues to grow and create more data, it is crucial to protect data privacy and address any ethical issues. By creating ADS and IoAT that respect privacy laws and regulations, as well as include ethical considerations to handle data and perform analyses, trust and conformity to IoT implementations shall be supported.

References

1. J. H. Lee and H. Kim, "Security and privacy challenges in the internet of things (security and privacy matters)," IEEE Consumer Electronics Magazine, vol. 6, no. 3, pp. 134-136, 2017. doi: [10.1109/MCE.2017.2684961](https://doi.org/10.1109/MCE.2017.2684961).
2. M. S. Eddine, M. A. Ferrag, O. Friha, and L. Maglaras, "Easbf: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles," Journal of Information Security and Applications, vol. 59, pp. 102802, 2021. doi: [10.1016/j.jisa.2021.102802](https://doi.org/10.1016/j.jisa.2021.102802).
3. M. A. Alsoufi et al., "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," Applied Sciences, vol. 11, no. 18, pp. 8383, 2021. doi: [10.3390/app11188383](https://doi.org/10.3390/app11188383).
4. L. Njilla, L. Pearlstein, X. Wu, A. Lutz, and S. Ezekiel, "Internet of Things anomaly detection using machine learning," in Proceedings of the 2019 IEEE Applied Imagery

Pattern Recognition Workshop (AIPR), pp. 1-6, 2019. doi: [10.1109/AIPR47015.2019.9174572](https://doi.org/10.1109/AIPR47015.2019.9174572).

5. M. S. Virat, S. Bindu, B. Aishwarya, B. Dhanush, and M. R. Kounte, "Security and privacy challenges in internet of things," in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 454-460, 2018. doi: [10.1109/ICOEI.2018.8553825](https://doi.org/10.1109/ICOEI.2018.8553825).
6. M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on internet of things," Journal of Network and Computer Applications, vol. 97, pp. 48-65, 2017. doi: [10.1016/j.jnca.2017.08.017](https://doi.org/10.1016/j.jnca.2017.08.017).
7. P. Panagiotis, K. Taxiarxchis, K. Georgios, L. Maglaras, and M. A. Ferrag, "Intrusion detection in critical infrastructures: A literature review," Smart Cities, vol. 4, no. 3, pp. 1146-1157, 2021. doi: [10.3390/smartcities4030071](https://doi.org/10.3390/smartcities4030071).
8. L. Maglaras, T. Cruz, M. A. Ferrag, and H. Janicke, "Teaching the process of building an intrusion detection system using data from a small-scale SCADA testbed," Internet Technology Letters, vol. 3, no. 1, pp. e132, 2020. doi: [10.1002/itl2.132](https://doi.org/10.1002/itl2.132).
9. A. A. Cook, G. Mısırlı, and Z. Fan, "Anomaly detection for IoT time-series data: A survey," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6481-6494, 2020. doi: [10.1109/JIOT.2020.2992345](https://doi.org/10.1109/JIOT.2020.2992345).
10. R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35, 2018. doi: [10.1109/SPW.2018.00013](https://doi.org/10.1109/SPW.2018.00013).
11. V. Adat and B. B. Gupta, "Security in internet of things: Issues, challenges, taxonomy, and architecture," Telecommunication Systems, vol. 67, no. 3, pp. 423-441, 2018. doi: [10.1007/s11235-017-0345-9](https://doi.org/10.1007/s11235-017-0345-9).
12. X. Yang et al., "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4319-4330, 2022. doi: [10.1109/TII.2021.3138397](https://doi.org/10.1109/TII.2021.3138397).
13. B. Mbarek, A. Meddeb, W. B. Jaballah, and M. Mosbah, "A secure authentication mechanism for resource constrained devices," in 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1-7, 2015. doi: [10.1109/AICCSA.2015.7507258](https://doi.org/10.1109/AICCSA.2015.7507258).
14. R. Fu, K. Zheng, D. Zhang, and Y. Yang, "An intrusion detection scheme based on anomaly mining in Internet of Things," in IET Conference Proceedings, 2011. doi: [10.1049/cp.2011.0295](https://doi.org/10.1049/cp.2011.0295).
15. T. Hastie, R. Tibshirani, and J. Friedman, The elements of statistical learning: Data mining, inference and prediction, 2nd ed. New York, NY, USA: Springer, 2009. doi: [10.1007/978-0-387-84858-7](https://doi.org/10.1007/978-0-387-84858-7).
16. K. P. Murphy, Machine learning: A probabilistic perspective. Cambridge, MA, USA: MIT Press, 2013.

17. A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges," Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 2701-2721, 2021. doi: [10.1007/s11831-020-09408-8](https://doi.org/10.1007/s11831-020-09408-8).
18. M. A. Al-Garadi, A. Mohamed, and A. K. Al-Ali, "Deep and machine learning approaches for anomaly-based intrusion detection of IoT systems: A review," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 106-139, 2020. doi: [10.1109/COMST.2019.2958727](https://doi.org/10.1109/COMST.2019.2958727).
19. G. S. Chadha, I. Islam, A. Schwung, and S. X. Ding, "Deep convolutional clustering-based time series anomaly detection," Sensors, vol. 21, no. 16, pp. 5488, 2021. doi: [10.3390/s21165488](https://doi.org/10.3390/s21165488).
20. J. Jiang, G. Han, L. Liu, L. Shu, and M. Guizani, "Outlier detection approaches based on machine learning in the Internet-of-Things," IEEE Wireless Communications, vol. 27, no. 2, pp. 53-59, 2020. doi: [10.1109/MWC.001.1900246](https://doi.org/10.1109/MWC.001.1900246).
21. T. Zhang, J. Hu, and W. Liu, "Machine learning approaches to network anomaly detection for the Internet of Things," IoT, vol. 1, no. 2, pp. 175-191, 2020. doi: [10.3390/iot1020012](https://doi.org/10.3390/iot1020012).
22. W. Ding, L. Zheng, and T. Zhang, "Network anomaly detection based on the PCA method in smart city IoT systems," Journal of Sensors, vol. 2021, pp. 1-12, 2021. doi: [10.1155/2021/6695830](https://doi.org/10.1155/2021/6695830).
23. J. Lee, K. Park, and Y. Kim, "IoT anomaly detection using autoencoder-based models," Sensors, vol. 20, no. 22, pp. 6404, 2020. doi: [10.3390/s20226404](https://doi.org/10.3390/s20226404).
24. X. Su, H. Shen, and S. Cheng, "Anomaly detection in IoT systems using Gaussian Mixture Model," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7822-7833, 2019. doi: [10.1109/JIOT.2019.2922551](https://doi.org/10.1109/JIOT.2019.2922551).
25. A. Nabil, H. Harb, and I. F. T. Alshaikhli, "Anomaly detection in IoT networks using machine learning techniques: A comparative study," IEEE Access, vol. 8, pp. 54195-54207, 2020. doi: [10.1109/ACCESS.2020.2978363](https://doi.org/10.1109/ACCESS.2020.2978363).
26. Y. Zeng, H. Wang, and Z. Zhou, "Anomaly detection in IoT-based smart grids using boosting algorithms," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 5774-5782, 2020. doi: [10.1109/TII.2019.2955831](https://doi.org/10.1109/TII.2019.2955831).
27. V. Mothukuri et al., "Federated learning-based anomaly detection for IoT security attacks," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6348-6358, 2021. doi: [10.1109/JIOT.2021.3063856](https://doi.org/10.1109/JIOT.2021.3063856).
28. Y. Liu et al., "Deep anomaly detection for time-series data in Industrial IoT: A communication-efficient on-device federated learning approach," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6348-6358, 2021. doi: [10.1109/JIOT.2020.3043756](https://doi.org/10.1109/JIOT.2020.3043756).
29. C. Wang, J. Chen, Y. Yang, X. Ma, and J. Liu, "Poisoning attacks and countermeasures in intelligent networks: Status quo and prospects," Digital Communications and

Networks, 2021. doi: [10.1016/j.dcan.2021.10.003](https://doi.org/10.1016/j.dcan.2021.10.003).

30. H. Lee et al., "Digestive neural networks: A novel defense strategy against inference attacks in federated learning," Computers & Security, vol. 109, pp. 102378, 2021. doi: [10.1016/j.cose.2021.102378](https://doi.org/10.1016/j.cose.2021.102378).
31. C. Yin, S. Zhang, J. Wang, and N. N. Xiong, "Anomaly detection based on convolutional recurrent autoencoder for IoT time series," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 5, pp. 1719-1731, 2020. doi: [10.1109/TSMC.2020.2997340](https://doi.org/10.1109/TSMC.2020.2997340).
32. R. Shukla and S. Sengupta, "Scalable and robust outlier detector using hierarchical clustering and long short-term memory (LSTM) neural network for the Internet of Things," Internet of Things, vol. 9, pp. 100167, 2020. doi: [10.1016/j.iot.2020.100167](https://doi.org/10.1016/j.iot.2020.100167).
33. P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, no. 1-2, pp. 18-28, 2009. doi: [10.1016/j.cose.2008.08.003](https://doi.org/10.1016/j.cose.2008.08.003).
34. M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," Information Processing & Management, vol. 45, no. 4, pp. 427-437, 2009. doi: [10.1016/j.ipm.2009.03.002](https://doi.org/10.1016/j.ipm.2009.03.002).
35. D. M. Powers, "Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation," Journal of Machine Learning Technologies, vol. 2, no. 1, pp. 37-63, 2011.
36. A. P. Bradley, "The use of the area under the ROC curve in the evaluation of machine learning algorithms," Pattern Recognition, vol. 30, no. 7, pp. 1145-1159, 1997. doi: [10.1016/S0031-3203(96)00142-2](https://doi.org/10.1016/S0031-3203(96)00142-2).
37. R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in International Joint Conference on Artificial Intelligence, vol. 14, pp. 1137-1143, 1995.
38. Z. Reitermanova, "Data splitting," in WDS'10 Proceedings of Contributed Papers, Part I, vol. 10, pp. 31-36, 2010.
39. C. Seiffert, T. M. Khoshgoftaar, J. Van Hulse, and A. Napolitano, "RUSBoost: A hybrid approach to alleviating class imbalance," IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 40, no. 1, pp. 185-197, 2010. doi: [10.1109/TSMCA.2009.2029559](https://doi.org/10.1109/TSMCA.2009.2029559).
40. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1-58, 2009. doi: [10.1145/1541880.1541882](https://doi.org/10.1145/1541880.1541882).
41. A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "Hybrid machine learning model for internet of things data anomaly detection," Future Generation Computer Systems, vol. 113, pp. 99-111, 2020. doi: [10.1016/j.future.2020.06.004](https://doi.org/10.1016/j.future.2020.06.004).

42. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, vol. 78, pp. 544-546, 2018. doi: [10.1016/j.future.2017.07.060](https://doi.org/10.1016/j.future.2017.07.060).

43. Y. Yuan, F. Wang, and C. Zhang, "A lightweight anomaly detection method for data collection systems in IoT," IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2670-2679, 2019. doi: [10.1109/TII.2018.2879001](https://doi.org/10.1109/TII.2018.2879001).

44. D. A. B. Fernandes, J. J. P. C. Rodrigues, and L. F. Carvalho, "Toward a secure and efficient IoT network management," IEEE Network, vol. 35, no. 2, pp. 79-85, 2021. doi: [10.1109/MNET.001.2000402](https://doi.org/10.1109/MNET.001.2000402).