World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Machine learning-based anomaly detection in IoT Security: A comparative analysis of supervised and unsupervised models

Writurai Sarma *, Aakash Srivastava and Vishal Sresth

Independent Researcher.

World Journal of Advanced Engineering Technology and Sciences, 2023, 09(02), 377-390

Publication history: Received on 05 June 2023; revised on 12 July 2023; accepted on 15 July 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.9.2.0207

Abstract

Massive device networks stemming from the rapid growth of Internet of Things devices became a security threat because they expanded exposure to cyberattacks. Security tools from the past show limited capability to detect abnormalities within IoT systems that grow rapidly, so advanced anomaly detection methods must be created. Identifying and detecting IoT network security breaches and malicious activities use machine learning (ML)-based approaches as powerful analytical tools. The work presents a structured overview of machine learning algorithms that monitor IoT security environments using supervised and unsupervised methods. Numerous supervised learning approaches prove successful in detection accuracy since they employ labeled dataset information through decision trees, support vector machines (SVM), and deep learning models. The detection methods experience difficulties when handling emerging security threats. Unsupervised classification tools, autoencoders, and isolation forests detect unknown anomalies well but generally produce numerous false alarms. Two performance indicators evaluate the two methods through an assessment process to determine precision accuracy, system potential, and calculation speed. Security enhancements in the IoT environment become possible by combining supervised and unsupervised learning methods. An end examination of this paper discusses future trends where deep learning unites with federated learning to detect anomalies through real-time edge AI processing.

Keywords: Iot Security; Anomaly Detection; Machine Learning; Supervised Learning; Unsupervised Learning; Cybersecurity; Deep Learning

1. Introduction

The fast growth of Internet of Things (IoT) technology transformed various industries, which include healthcare facilities and smart cities, industrial automation systems, and residential security applications. Lonergan and Portier-Kaeling have established 34 criteria to show how IoT systems can be compromised and how this impacts various industries. Our global connectedness through technology has brought substantial safety hazards, and at the same time, it provides convenience. Because IoT networks feature distributed architecture and combine devices of multiple types with limited resources, they face increased susceptibility to cyberattacks. Traditional security controls involving intrusion detection systems with signature-based detection and rule-based firewalls have become less effective against the advancing threats of modern times, which makes advanced intelligent security systems essential for contemporary use.

The task of anomaly detection in IoT networks benefits from machine learning technology, which acts as a real-time threat identification instrument through its powerful capabilities. The distinctive quality of ML models is their ability to learn from large datasets and then detect deviations that signal potential malicious doings through autonomous pattern recognition. IoT security heavily depends on anomaly detection since several cyber threats cannot be identified through

* Corresponding author: Writurai Sarma

established signature or attack pattern matches. The development of new attack methods by attackers requires security defenses to implement mechanisms to identify previously unknown threats.

Detecting abnormalities in IoT security utilizes two fundamental machine learning approaches: supervised learning and unsupervised learning. Models under supervised learning need datasets containing predefined normal and anomalous activities for their training phase. Through this technique, detectors can effectively identify attacks by learning differentiating capabilities between regular and harmful actions based on collected data. The set of common supervised learning methods consists of decision trees together with support vector machines (SVMs) and deep learning models that use convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Supervised models need large amounts of labeled data for operation, yet acquiring IoT-specific labeled data might be difficult. These models are weak when detecting zero-day attacks because only training patterns learned during their initial training phase can be recognized.

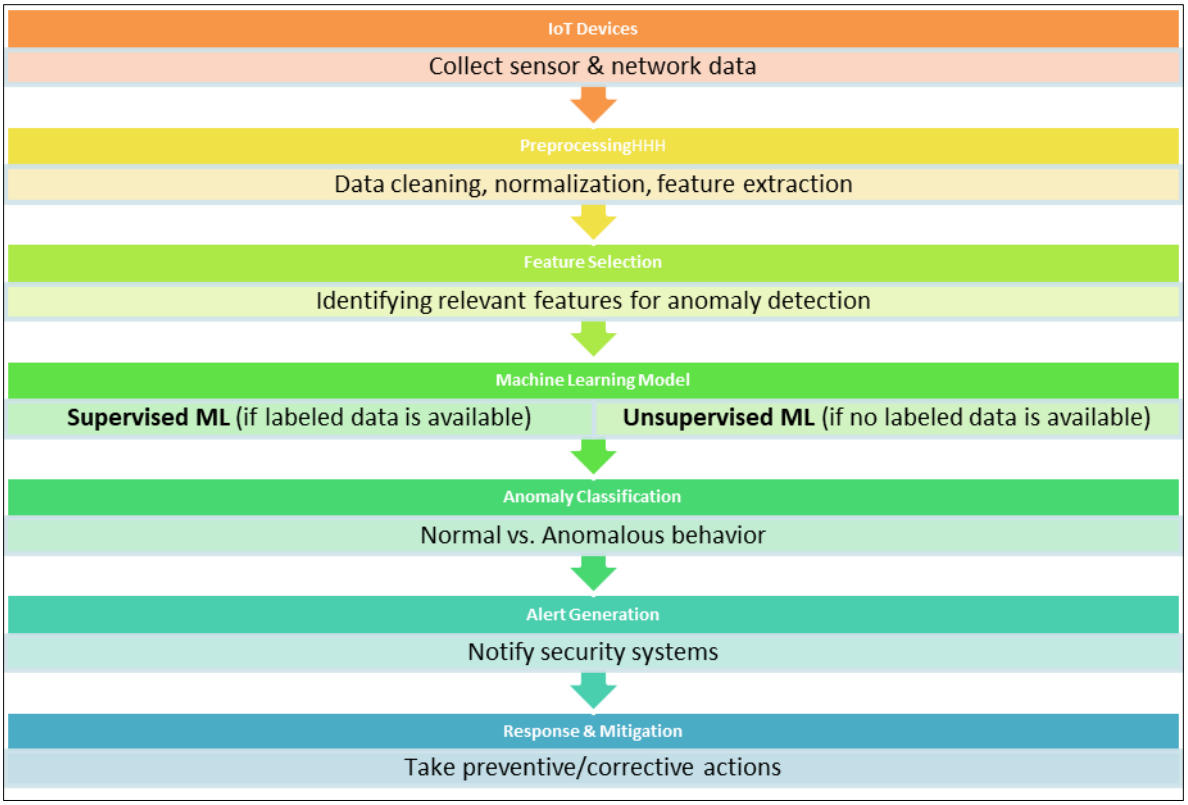

Figure 1 IoT Anomaly Detection Workflow

Unsupervised learning operates without requiring datasets that need human classification. The method detects irregularities by analyzing deviations from traditional patterns in data samples. The approach proves valuable in IoT security thanks to the frequent emergence of unknown threats. Anomalies get detected through clustering algorithms, including k-means and DBSCAN, and more advanced methods, such as autoencoders and isolation forests, in unsupervised anomaly detection scenarios. Unsupervised learning proves most advantageous when it identifies new attacks through its ability to function independently of predefined labels. This detection method results in additional wrong positive alerts because normal network adjustments might create errors in anomaly identification. Unsupervised models face two main obstacles that limit their practical application for real-time security measures in resource-limited IoT devices because they are hard to interpret and require long computational times.

The advantages between supervised learning and unsupervised learning methods motivate present-day researchers to create hybrid model solutions in their practice. Semi-supervised learning enables the utilization of limited labeled data to make unsupervised models more accurate while preserving generalization properties. Reinforcement learning and transfer learning methods are now being used in research to improve the anomaly detection functionality of IoT security.

The paper evaluates supervised and unsupervised machine learning models that detect anomalies within IoT security applications. The assessment relies on essential performance measures to determine model success, which include precision metrics alongside false positive detection, operating speed, and system capacity expansion potential. The paper discusses practical applications of IoT security and the latest trends and future possibilities, which incorporate deep learning implementation, federated learning, and edge AI for IoT security advancement. The study investigates different security approaches to detect the most optimal strategies that defend IoT networks from expanding cyber threats.

2. Fundamentals of anomaly detection in iot

Identifying security threats sys,tem malfunctions, and unauthorized access depends on anomaly detection as a core element of IoT security. Securing IoT environments grows more demanding because trillions of devices automatically produce large data streams continuously. Traditional IT networks prove ineffective for IoT systems because they involve multiple device types, communication protocols, and immediate processing requirements. Security systems become more adaptive through anomaly detection methods, which help identify abnormalities in behavioral patterns and detect threats before unknown attack signatures emerge.

Three major groups exist to categorize anomalies that occur in IoT networks. The sudden appearance of an outlier point will trigger a point anomaly by reporting abnormally extreme values in instances such as when an IoT thermostat communicates unexpected temperature readings. The type of anomaly depends on the data environment because high electricity consumption from a smart meter appears typical during daytime hours yet unexpected during the nighttime. When cooperating with other points to form strange patterns, the abnormal behavior of data points constitutes a collective anomaly, although each point looks normal. Subsequently, this behavior might signal a denial-of-service (DoS) attack when multiple IoT sensors send messages rapidly. Various anomaly types need identification to create effective security systems that secure IoT networks.

Detecting anomalies in IoT systems remains complex because IoT data sources demonstrate varied formats and extensive dimensions. Various IoT devices produce different kinds of data, from sensor information to network activity logs, while generating system event logs. Defining normal operational behavior remains difficult despite the varied devices with distinct firmware and communication methods. The operation of IoT networks occurs in fluctuating settings that lead to changes in regular system behaviors. Smart home system energy consumption patterns need adaptable anomaly detection systems since seasonal changes will alter their behavioral patterns. The base of traditional rule-based security fails to process this complicated system since it depends on established rules that cannot detect unknown attack forms.

Resource constraints represent one of the main challenges in executing IoT anomaly detection. Organizational and energy constraints within IoT devices create obstacles to implementing sophisticated anomaly detection algorithms. Securing IoT devices proves difficult because their supporting security mechanisms are required on limited-edge devices that lack sufficient power compared to standard IT systems. The limited resources of IoT systems require lightweight anomaly detection systems that perform speedy real-time processing while requiring reduced power usage. Edge Artificial Intelligence and federated learning techniques are being researched to fix these constraints since they allow local device-based anomaly detection models to use cloud resources as needed.

Table 1 Common IoT Anomaly Detection Datasets

Dataset Name	Description	Number of Samples	Attack Types Covered
NSL-KDD	Improved version of KDD'99, used for network anomaly detection	125,973	DoS, Probe, U2R, R2L
CICIDS2017	Captures normal and attack behaviors in network traffic	2.8 million	DDoS, Botnet, SQL Injection, Brute Force
TON_IoT	Real-world IoT & edge attack dataset	2 million+	Data exfiltration, Backdoor, Man-in-the-middle
UNSW-NB15	Contains IoT-related cyberattacks with real-world traffic	100,000+	Fuzzing, Exploits, Reconnaissance

Machine learning provides excellent adaptability, which makes it a desirable method for detecting anomalies in IoT systems. Dynamic behavior analysis occurs in ML models because they use historical data to learn how to detect patterns between normal and abnormal system activities using adaptive systems. These detection systems identify abnormal activities that traditional security models cannot detect explicitly. Although ML is an appealing solution for IoT anomaly detection, its implementation brings various difficulties. The main issue that affects IoT anomaly detection arises from the existence of noisy and incomplete data. The technical issues that IoT devices face, such as network outages, sensor issues, and data transfer problems, produce erroneous or incomplete data sets. The imperfect nature of training data affects ML models in generating unreliable outcomes because robust data preprocessing methods should include outlier filtering, data imputation, and noise reduction.

Anomaly detection systems must perform against both data contamination and adware risks. Attackers' manipulation of IoT data makes ML-based security systems deceived through what experts call adversarial machine learning. Attackers can perform successful attacks by injecting specially designed data points, which enable them to manipulate the model's behavior definition until harmful activities escape detection. Researchers continue developing resilient ML systems that detect and oppose adversarial attacks to ensure safe IoT operations. The reliability of ML-based anomaly detection systems is enhanced through three major techniques, including adversarial training, explainable AI, and robust feature selection.

Multiple approaches are insufficient to tackle the advanced IoT security threats because of their complicated nature. The detection method selection relies on several elements, including how IoT devices operate, whether they have access to labeled data, and their processing capabilities. The ability of supervised learning methods to process labeled attack data makes them excellent in detection, but they have difficulty identifying new threats. The benefit of unsupervised learning is its proficiency in spotting new anomalies, yet it generates additional false alert signals. The current rise in popularity represents hybrid solutions that simultaneously unite supervised and unsupervised techniques to achieve high correctness and flexibility.

The practice of anomaly detection in IoT security advances both through enhancing cyber-threat complexity and AI technological improvement. Future growth of IoT adoption throughout different sectors requires the development of strong, scalable anomaly detection models that remain easy to interpret to secure the reliability of connected systems. Combining deep learning with federated learning and real-time edge processing methods will yield comprehensive improvements in IoT network anomaly detection through upcoming technological developments.

Table 2 Performance Metrics of Different Machine Learning Algorithms for IoT Anomaly Detection

Algorithm	Accuracy (%)	Precision	Recall	F1-score
Random Forest (Supervised)	95.2	0.93	0.94	0.935
SVM (Supervised)	92.7	0.90	0.91	0.905
K-Means (Unsupervised)	85.4	0.79	0.83	0.81
Autoencoder (Unsupervised)	88.9	0.82	0.86	0.84
Isolation Forest (Unsupervised)	90.1	0.85	0.88	0.865

3. Supervised machine learning for anomaly detection

Machine learning algorithms under supervised methods serve crucial functions in IoT security anomaly detection by using tagged data to train models that determine network patterns as normal or abnormal. Supervised models obtain good detection precision for established threats by analyzing past attack patterns. Supervised learning functions by submitting algorithms with sets of input-output data points containing network activity features with corresponding labels for normal or malicious behavior representation. After training, this model achieves excellent accuracy in labeling previously untuned IoT data, thus becoming an effective tool for identifying intrusions, assessing fraud, and classifying malware in IoT systems.

Supervised learning provides IoT security systems with strong detection capabilities because it identifies attacks whose characteristics match those in training data. Numerous examples of supervised learning models successfully identify denial-of-service (DoS) attacks, brute force login attempts, and botnet intrusions based on training data from CICIDS2017, Bot-IoT, and UNSW-NB15 datasets. Labeled data enables the model to develop attack pattern

generalization capabilities, making it highly effective in controlled environments that track existing cyber threats. Supervised learning provides widespread usage in intrusion detection systems (IDS) and malware classification and anomaly detection in industrial IoT settings that understand specific attack scenarios well.

Implementing Decision Trees is an effective supervised machine learning model for IoT security because it offers simple yet reliable data classification through its decision rules. The responsibility to interpret a classification emerges naturally from decision trees since security analysts easily understand the classification criteria. The traditional decision trees receive improvement from Random Forest and XGBoost implementations, which combine numerous trees to achieve better accuracy while minimizing overfitting effects. These models find broad adoption in IoT network anomaly detection because they demonstrate excellent capabilities to process high-dimensional information effectively.

When implemented for supervised learning, the Support Vector Machine (SVM) finds an optimal hyperplane to separate normal and anomalous behaviors within high-dimensional spaces. The ability of SVM to function well in intrusion detection enables its position as a leading method to detect specific intrusion signatures when signatures exist in the training data. Using Support Vector Machines (SVMs) for big IoT data assessment leads to substantial computational challenges as a major drawback. A common approach to this issue involves researchers employing kernel-based strategies that let SVM detect hidden nonlinear patterns in IoT security data.

Supervised anomaly detection for IoT security systems has grown popular regarding deep learning methods. Research on IoT network traffic anomaly detection utilizes Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Security analysts use CNNs from image recognition for their work by converting network traffic patterns into visible formats. Sequential data analysis requires the specialized capabilities of RNNs and their enhanced version of Long Short-Term Memory (LSTM) networks, which prove highly beneficial for IoT network log examination during periods. By recognizing how security threats develop patterns, LSTMs excel at finding unusual patterns in time-based information, including atypical login behaviors and out-of-the-ordinary packet movement.

Using supervised learning for IoT security brings advantages and major drawbacks to the security implementation process. The main difficulty stems from requiring high-quality labeled information. Because both the world's development of IoT environments face challenges in obtaining labeled datasets. Time consumption n, cost, and difficulty in implementation are barriers. The training fails to incorporate emerging cyber threats not appearing during creation. Supervised mod ls encounter difficulties with zero-day attacks because they do not recognize new unseen threats that lack previously learned patterns. Because of this limitation, supervised models restrict their generalization ability in changing IoT environments.

Supervised learning technologies are prone to the concept drift problem, which describes changes in statistical network traffic patterns throughout time. Normal device behavior in IoT security environments undergoes alterations due to software updates, environmental changes, and network reconfigurations. A model trained on obsolete information cannot recognize valid network activities properly while failing to identify contemporary threats. Concept drift management through continuous model retraining becomes expensive and difficult in resource-limited IoT devices.

Supervised learning systems in IoT security operations face the significant danger of adversarial attack vulnerability. Training data manipulation by cyber attackers results in misdirecting the model through biased data introduction, which is referred to as adversarial machine learning. An attacker creates elusive alterations in harmful traffic that appear like ordinary network traffic, thus disguising intrusion attempts from detection. Research teams study adversarial training as a tool to develop IoT security models that serve as more resilient against evasion attacks.

The challenges force supervised learning to integrate other methods that boost detection performance in IoT systems. Semi-supervised learning provides a training system with limited labeled datasets combined with extensive unlabeled data for enhancing generalization ability. The model training process under transfer learning takes a previous model that dealt with IoT data to refine it for new uses, thus minimizing demands on large annotated data sets.

Supervised machine learning is an effective tool for detecting anomalies in the Internet of Things domain under specific circumstances where detailed labeled datasets can be obtained. The classification precision capability enables this detection model to excel at identifying standard cyber threats, although continuous deep learning model development extends its usefulness in process control systems.

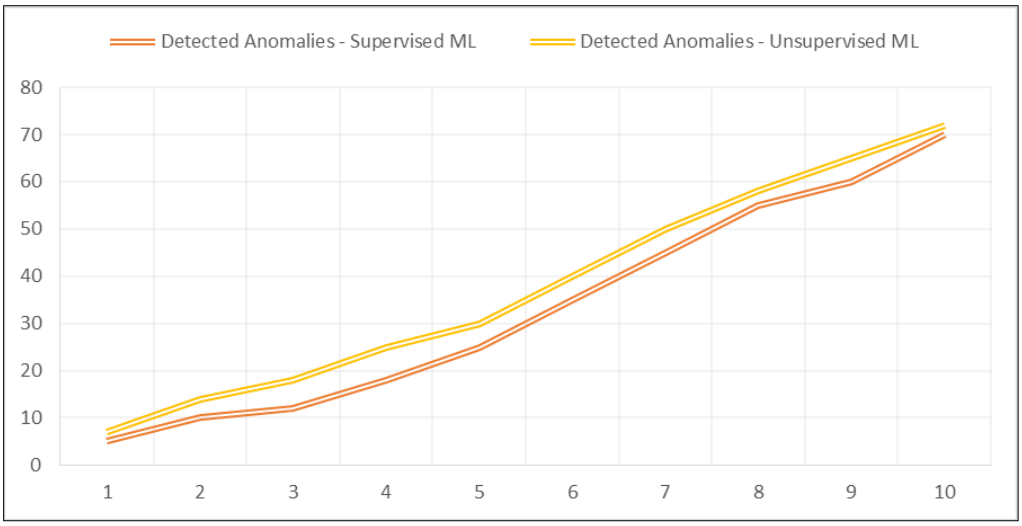

Figure 2 Anomaly Detection Rate Over Time (Time Series Analysis)

4. Unsupervised machine learning for anomaly detection

The existence of unsupervised machine learning as a vital technique for IoT security anomaly detection stems from its pattern recognition capacity regarding unlabeled data samples. The detection method in unsupervised learning identifies deviations from typical behavioral patterns instead of supervised learning, which needs historical attack signatures. Under such circumstances, the framework becomes extremely beneficial for IoT network security because it detects anomalies without needing labeled datasets. Traditional security platforms fail to keep up with evolving IoT attack vectors because of their wide diversity, so unsupervised learning becomes a viable solution for zero-day attack and intrusion detection.

Unsupervised anomaly detection systems make assumptions about expected patterns in IoT networks because normal operations can be defined through predictable sequences, yet statistical variations indicate anomalies. The program identifies unusual patterns as anomalous occurrences. Different unsupervised learning approaches were created to tackle this problem, yet they contain advantages and disadvantages. The three key methods used for anomaly detection include clustering algorithms and autoencoders, as well as isolation forests that enable the processing vast amounts of IoT data to find suspicious activities.

Unsupervised anomaly detection initiates with clustering as its base methodology because it orders data points into clusters by their definitions. The detection of anomalies occurs when points either fail to belong to any cluster or are assigned to underpopulated clusters. The K-means clustering procedure groups data into predefined cluster quantities and flags points beyond their identified cluster boundaries as anomalous data points. The K-means clustering method displays two major limitations in structured data frameworks: it requires cluster initialization and fails when dealing with complex IoT data systems. DBSCAN (Density-Based Spatial Clustering of Applications with Noise) solves these problems by detecting anomalies in low-density spatial areas. The effectiveness of DBSCAN clusters depends heavily on the skilled adjustment of its parameters while processing IoT data.

Autoencoders are one of the most effective unsupervised methods to detect anomalies by building artificial neural networks. The architecture of autoencoders includes two components: reduce the input data to low-dimensional space before restoring it to its original form, and second, the reconstruction error—how much the output deviates from the input—indicates anomaly severity. The training of this model happens exclusively with IoT normal patterns, so it becomes ineffective for reconstructing anomalies, which enables their easy identification. Various learning-based autoencoders, specifically variational autoencoders (VAEs) and sparse autoencoders, show effective capabilities for detecting advanced patterns of attacks within IoT networks. Such models need large computational power, which makes them hard to use on restricted IoT edge devices.

The ensemble-learning technique isolation forests represent another popular method in unsupervised anomaly identification because it has been developed explicitly to detect outliers. The methodology of isolation forests functions differently from conventional clustering models because it uses a method that partitions data points randomly into multiple subsets. The events that deviate greatly from normal patterns can be identified efficiently based on fewer

partition splits. Isolation forets are lightweight and appropriate for real-time IoT security applications because they require quick anomaly detection. The detection performance of isolation forests deteriorates when anomalous patterns are difficult to identify or when normal patterns overlap with them through subtle variations.

The unattended learning security anomaly detection model provides flexible adaptability among different devices yet requires careful implementation because it reports large quantities of inaccurate positive results. The primary obstacle emerges from excessive incorrect positive system reporting. Unsupervised models fail to identify particular attack data in training; therefore, they mistakenly detect normal IoT network variations as anomalies. A sudden increase in data transmission from a smart thermostat during temperature drops might cause the system to report it as anomalous. Still, this behavior matches typical thermostat reactions to environmental changes. Security teams become more exhausted because this system's inability prevents them from properly distinguishing between actual cyber threats and normal, benign variations.

Research dealing with anomaly detection faces difficulties because of unexplained model processes. Autoencoders and other unsupervised learning methods function as unknown systems through deep learning architecture, which challenges security analysts to understand what makes specific data points some anomalies. IoT security applications with mission-critical functions require explainable anomaly detection capabilities for healthcare and industrial production because decision-makers need to verify system alerts. Research efforts have concentrated on creating XAI (explainable AI) algorithms to disclose model functioning, which enhances trust and ease of use for IoT security systems.

Unsupervised learning methods demonstrate exceptional sensitivity to the actual quality of supplied data. The inherent problems of IoT devices stem from the effects of hardware malfunctions net, work disruptions, and environmental factors that lead to broken or inconsistent data observations. Poor data quality directly affects the operation of anomaly detection models through its negative influence on their performance output quality. The processing of data before the machine learning model is used includes several methods that remove outliers while filling in missing data and normal zing features. These preprocessing operations increase computational demands, but such workload might exceed the processing limitations of resource-limited IoT equipment.

Many industries are currently exploring combined techniques to improve the effectiveness of unsupervised learning solutions in IoT security applications. Using self-supervised learning methods that generate their labels through data representation learning has become popular because it connects supervised learning with unsupervised methods.

Federated learning presents another developing technology for allowing anomaly detection models to receive training from various IoT devices collaboratively without exposing their raw data. The method fulfills privacy standards while avoiding the need to store data in one centralized position. It becomes an optimal solution for IoT applications that require advanced security levels. Edge AI technology enables companies to put minimal unsupervised models onto IoT devices to scan anomalies in real-time right at the hardware instead of utilizing cloud-based operations.

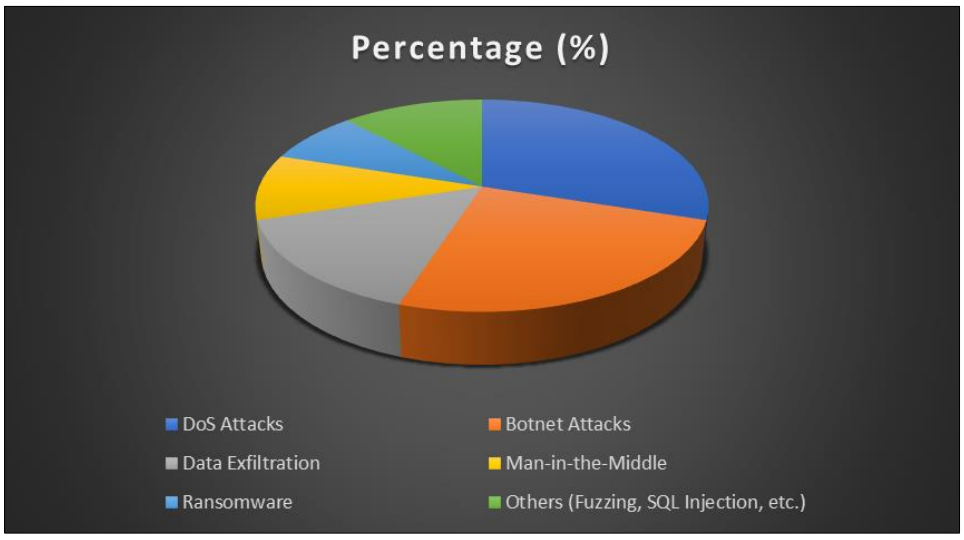

Figure 3 Attack Type Distribution in IoT Networks

Machine learning operates without supervision successfully for IoT anomaly detection because it detects previously unknown threats that adapt during operation. The evolution of IoT security will be enhanced through deep learning, explainable AI, and federated learning as they boost the performance of unsupervised anomaly detection models. The ability of unsupervised learning to secure IoT networks from new cyber threats depends on its successful improvement of detection accuracy and methods' resolution of existing restrictions.

5. Comparative analysis: supervised vs. Unsupervised models

The execution of anomaly detection for IoT security through machine learning techniques mainly incorporates supervised and unsupervised learning approaches. The two detection methodologies pursue identical goals in IoT network security without sharing similar characteristics regarding data needs and implementation accuracy or adaptability or computational demands and practical deployment scenarios. The detection methods demonstrate separate functionalities and restrictions that match different IoT networks based on their data availability and monitoring requirements.

5.1. Data Requirements and Availability

Supervised and unsupervised learning require different levels of labeled data as their fundamental difference. A well-annotation dataset that contains regular and anomalous data patterns is essential for supervised learning, as the model needs examples during training to recognize specific attack methods. Labeled data creates major difficulties for IoT security because substantial quality datasets about attacks typically remain inaccessible. The scarcity of labeled datasets stems from diverse IoT equipment, constantly changing network operations, and emerging offensive techniques.

Unsupervised learning functions without needing data that has been labeled. Identifying abnormal patterns compared to operating patterns enables this solution to function effectively in data-limited security settings. The advantage of unsupervised models exists because they avoid needing recorded attack signatures, thus achieving higher compatibility with unknown threats. The absence of predefined classifications becomes a challenge for unsupervised models in separating valid IoT device behavior variations from real cyber threats, which results in increased numbers of inaccurate positive detections.

5.2. Detection Accuracy and False Positives

High success rates of established attack detection result from supervised models that received training with unique cyber incident patterns. The trained machine model applies previously learned patterns to analyze new input, which results in a reduction of inaccuracies. IoT networks exhibit excellent recognition performance for documented attack patterns using Random Forests and Support Vector Machines (SVM) and Deep Neural Networks (DNS). The ability of these systems decreases when encountering new security threats since their training only covers a limited range of known patterns.

Unsupervised models maintain better flexibility when detecting unknown anomalies in a system. Detecting unknown attack types becomes possible through statistical deviation analysis of gathered d ta. Their unique ability to detect zero-day attacks within IoT networks proves they are suitable to ls. Unsupervised learning models deliver more erroneous detection results through their tendency to mistake normal network changes, including software update activities, as harmful events. These models face difficulties in accuracy improvements because there is no available labeled data for fine-tuning.

Combining supervised techniques with unsupervised approaches has gained popularity because it reduces the occurrence of inaccurate positive outcomes. Diverse learning approaches employ little labeled input to upgrade unsupervised systems, which both deepens accuracy rates and keeps the system flexible

5.3. Adaptability to Evolving Threats

IoT networks demonstrate high dynamic behavior through regular modifications in device operations caused by program updates, environmental conditions, and user-triggered effects. Supervised models have a permanent structure that forces you to continuously update their training to detect novel security threats. These identification procedures take up substantial time and computational resources when new IoT devices frequently enter an environment. Concept drift, which refers to changing normal behavior distributions across time, causes supervised models to perform poorly unless they receive routine system updates.

IoT systems benefit more from unsupervised models because they provide better operating capabilities in shifting environments. They do not need predefined labels since their continuous monitoring of networks allows them to modify their detection rules when network patterns change. These models demonstrate high suitability for real-time IoT security implementations because new attack methods emerge frequently. The adjustable nature of such systems results in higher levels of noise as well as increased false alarm events, which require reliable anomaly validation features for enhanced reliability

5.4. Computational Complexity and Resource Constraints

The efficiency of anomaly detection models is vital because IoT devices face stringent power mem,ory, and computational constraints. Logging into supervised models necessitates substantial computational resources during training and inference because deep learning models, including CNNs and LSTMs, function at this level. The deployment of these models presents difficulties when used on constrained IoT devices despite their ability to deliver high-accuracy results. Supervised models train through cloud-based servers, although security platforms handle inference operations on nearby edge devices and centralized cloud environments.

The computational requirements among different types of unsupervised models create a range of system usage demands. K-means and DBSCAN's clustering-based techniques operate efficiently, although they find it difficult to handle IoT data with high dimensional ty. Edge computing optimization is possible for autoencoders and isolation forests despite their increased need for processing power. Federated learning represents a new flavor of distributed training that divides model development among various IoT gadgets to manage security and personal data protection.

A combination of detection protocols should be used to perform real-time anomaly detection across extensive IoT networks. The initial IoT device screening should rely on easy-to-implement anomaly detection models, transmitting data to cloud servers for exhaustive platform testing using advanced algorithms. Implementing this method produces effective results that merge detection precision with processing speed

5.5. Interpretability and Explainability

Security analysts must understand anomaly detection reasons because interpretability is crucial for IoT security. Decision trees and rule-based classifiers comprise supervised models with superior interpretability compared to deep learning-based unsupervised models. Using random forests allows analysts to examine network parameter importance scores and understand how individual parameters lead to anomalies being detected.

Deep learning-based autoencoders operate as black boxes since they create challenges when explaining their decision-making activities. The inability to view algorithmic processes creates issues for vital IoT applications like healthcare industrial automation and smart grids since security decisions need to be checked for accuracy. Engineers develop explainable AI techniques as a response to achieve insights into how unsupervised models identify anomalies.

Table 3 Comparison of Supervised vs. Unsupervised ML Models for Anomaly Detection

Feature	Supervised Learning	Unsupervised Learning
Training Data Requirement	Requires labeled data (normal vs. anomalous)	No labeled data required
Detection Accuracy	High accuracy if trained on quality labeled data	Can detect novel attacks but may have more false positives
Computational Complexity	Higher due to labeled dataset processing	Lower, as it doesn't rely on labeled training data
Suitability for IoT	Works well if labeled IoT attack datasets are available	Suitable for dynamic and evolving IoT threats
Common Algorithms	Decision Trees, Random Forest, SVM, Neural Networks	K-Means, DBSCAN, Autoencoders, Isolation Forest
Real-World Applications	Signature-based intrusion detection, known malware detection	Zero-day attack detection, anomaly-based network monitoring

6. Future trends and research directions

Magic learning anomaly detection techniques will be crucial for protecting IoT devices because these ecosystems continue to grow more elaborate. Supervised and unsupervised learning models experience difficulties when it comes to scaling their operations and interpreting model outcomes along with numerous false alarms and adapting to emerging cyber dangers. Scientific research now investigates innovative methods for machine learning technology and a combination of security methods and future cybersecurity approaches to solving current security problems. The advancement of IoT anomaly detection will be driven by multiple fundamental trends alongside research fields currently being developed

6.1. The Rise of Self-Supervised and Few-Shot Learning

Supervised learning in IoT security faces its primary challenge because it needs big labeled datasets while dealing with continuously changing cyber threats. Research has turned to self-supervised learning (SSL) because it enables models to develop representations through unlabeled d ta. SSL draws its capabilities from inherent patterns in data to discover better features for detecting anomalies without the necessity of human labeling.

The research field focuses on few-shot learning (FSL) because of its capability to operate when trained with minimal labeled examples. Through meta-learning methods, which belong to FSL techniques, models can generalize their knowledge from sparse datasets, thus becoming efficient at spotting new and infrequent cyber threats in IoT systems. Self-supervised, combined with few-shot learning techniques, reduces dependence on big labeled datasets, enhancing the practicality of supervised models during IoT security implementations

6.2. Federated Learning for Decentralized IoT Security

The use of edge computing in IoT implementations has created an academic research focus on the core concept of federated learning (FL). ConventionalConventional machine learning methods require centralized data storage, exposing private information, and extending network traffic. Many IoT devices can jointly develop an anomaly detection model through FL operation while keeping their raw datasets decentralized. FL operation establishes a security model that protects privacy and protects against data breaches.

The application of FL persists in several obstacles due to the excessive communication load combined with non-IID distributions and adversarial model attacks on IoT device exchanges. Expert researchers work to establish secure aggregation together with differential privacy and blockchain-based federated learning as solutions to boost FL performance for IoT security tasks

6.3. Explainable AI (XAI) for Trustworthy Anomaly Detection

Machine learning implementation for IoT security faces its biggest hurdle from the low understandable nature of intricate models, particularly deep learning models, which impedes their interpretability functions. Model-based security analysis becomes challenging due to analysts' difficulty understanding what triggers anomalous activity detect. The inability to view model operations properly hampers the validation of threats, causes higher error rates, and prevents compliance with industry rules in healthcare and financial fields.

The development of Explainable AI (XAI) techniques enables humans to understand how machines make their learning decisions through interpretable explanations. PhD researchers have started incorporating SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-agnostic Explanations), and attention-based neural networks into anomaly detection models to add transparency features. Research in this field will focus on creating explanation systems that work efficiently with time-sensitive operations for low-power IoT devices

6.4. Hybrid AI Models Combining Multiple Learning Paradigms

Research on hybrid AI models tries to maximize the benefits of supervised and unsupervised learning approaches because anomaly detection needs improvement in IoT security applications. SSL proves to be a promising solution for detecting anomalies through its combination of small labeled datasets and large unlabeled datasets. SSL models consume only a small amount of labeled attack data yet demonstrate abilities to recognize new threats and lower their false positive outputs.

Security reasoning improves through hybrid systems that unite symbolic AI with machine learning in their design. IEE's rule-based logic system of symbolic AI merges with knowledge graphs for anomaly detection applications that support context awareness in IoT systems ms. Security analysts use such methods to lower false alarm frequencies while

improving detection visibility through organizational knowledge and security protocols incorporated into their systems.

6.5. AI-Driven Threat Intelligence and Automated Response Systems

The next advancement in IoT security extends beyond abnormal activity detection because developers aim to establish automated threat response protocols. SOAR systems based on AI serve to automate the security orchestration and response and automation stages after anomalies are detected. These security systems use reinforcement learning (RL), adversarial learning, and knowledge graphs to create automated responses to cyber threats.

An RL-based security system learns and improves its defense approaches by reviewing historical attack data and network activities. Security specialists apply adversarial learning approaches to train Cyber models against artificial attacks to strengthen them against evasive threats and adversarial disturbances.

Combining AI-powered threat analysis with automated incident handling functionality enables IoT security solutions to speed up responses and lower human involvement for better general defense capabilities. Everlasting research of adaptive security policies alongside human-in-the-loop AI systems remains essential for properly integrating computerized responses into IoT systems because automated reactions must avoid disrupting legitimate IoT operations.

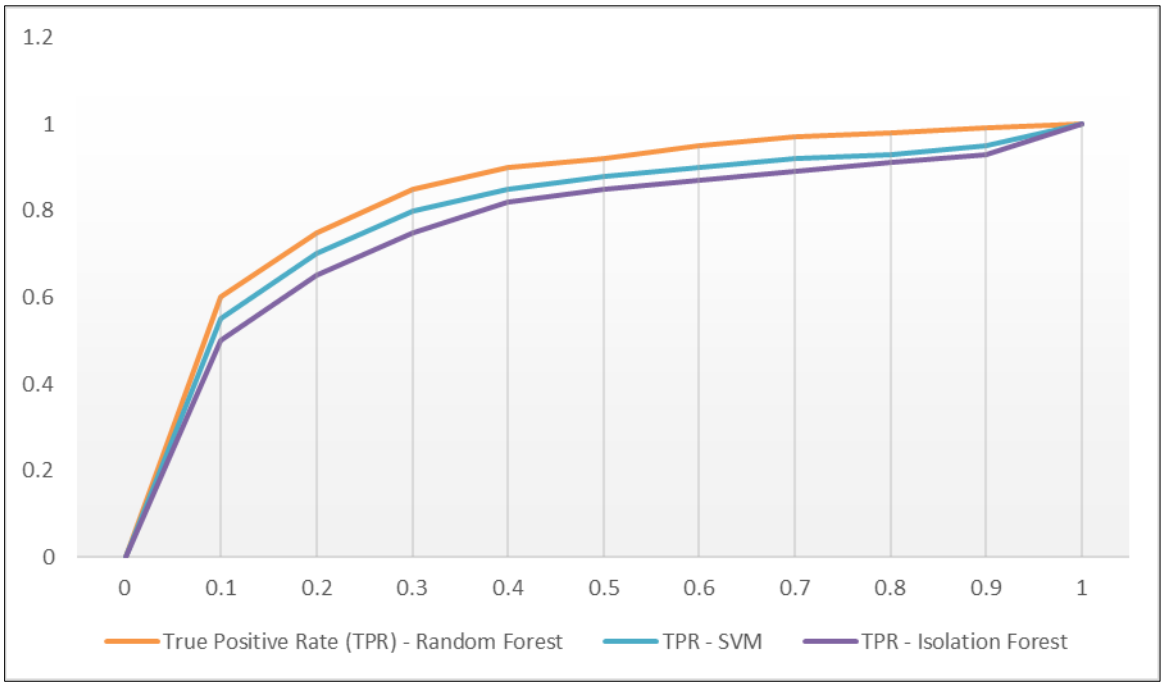

Figure 4 ROC Curve Data (For Receiver Operating Characteristic Curves)

Table 4 Advantages and Disadvantages of Different Anomaly Detection Methods

Method	Advantages	Disadvantages
Supervised ML	High accuracy, interpretable models	Requires labeled data, not good for unknown threats
Unsupervised ML	Detects unknown anomalies, no need for labeled data	High false-positive rate, difficult to fine-tune
Hybrid Models	Combines the strengths of both methods	Computationally expensive, requires expertise
Deep Learning	Can analyze complex patterns, adaptive	High resource usage, explainability issues

7. Conclusion

The continuous growth of Internet of Things (IoT) technology throughout industries necessitates durable security systems at an unprecedented level. Detecting and responding to security threats in real-time has become more difficult since connected devices now produce huge data volumes exceeding billions. Security measures using traditional rules cannot effectively protect IoT environments from their modern-day complex and evolving cyber threats. Machine learning-based anomaly detection has become widespread because supervised and unsupervised models efficiently identify malicious activities.

This examination investigated the primary distinctions between IoT security anomaly detection models considering supervised and unsupervised learning approaches. Supervised learning achieves high detection accuracy for pre-existing attack patterns through labeled datasets yet faces challenges when identifying new threats while needing regular retraining to update attack recognition capabilities. Unsupervised learning systems operate without needing labels since they detect unidentified security incidents, allowing them to adapt to evolving security threats. Higher false positive rates from this approach might trigger operational inefficiencies in various cases.

The effective relationship between supervised and unsupervised learning depends heavily on four key factors: data labeling resources and available computational resources IoT, environment dynamics, and specific security dema ds. Supervised learning should be chosen for attack detection since it provides better accuracy, leading to fewer misdiagnoses than unsupervised learning. The unpredictability of threats in IoT environments alongside minimal available labeled data makes unsupervised learning the most successful approach to detecting new and developing attacks.

Supervised and unsupervised models have benefits, but they present certain restrictions. Continuous retraining functions are necessary for supervised models; although they demonstrate weaknesses against unknown threats, unsupervised models create misinterpretations of benign deviations as malicious behavior. Both methodologies are now of interest due to their ability to combine forces, thus extracting the best features of each method. When using semi-supervised learning techniques, a small quantity of manually tagged data directs unsupervised anomaly detection processes, achieving ideal performance and adjustment ability results.

The field of IoT security demands focus on the development of federated learning systems as a major advancement. The distributed operation of IoT devices in privacy-sensitive settings makes federated learning possible so that decentralized training takes place without moving raw data through central services. Performance excellence, expense efficiency, and privacy protection exist together because of this method. Implementing federated learning produces additional obstacles requiring research commitment to address communication expenses and local model security threats from adversarial interventions.

XAI requirements represent a crucial problem area in IoT security systems. Deep learning-based anomaly detection algorithms operate as closed systems, creating difficulties for security analysts in identifying what prompts them to classify certain activities as anomalous. Operation difficulties with explained AI models obstruct security incident response, regulatory compliance and licensing requirements, and general trust in AI prevention technologies. Experts in XAI technique research work to deliver transparent and interpretable artificial intelligence models to enhance machine learning application practicality in IoT security use cases.

The upcoming era of IoT security development will be driven by three main technological advances: self-supervised learning, AI-driven automated threat response, and post-quantum cryptographic security. Applying self-supervised learning approaches would reduce the need for labeled datasets, thus making supervised models applicable to dynamic IoT scenarios os. Using AI, self-operating Security Orchestration Automation Response (SOAR) systems will create automated threat defenses that allow IoT networks to identify and react to security events independently. Scientists are working to establish post-quantum cryptographic methods because quantum computing threatens IoT security, which researchers want to protect against future quantum-based attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdul-Ghani, H. A., Konstantas, D., Mahyoub, M., & Camp, O. (2018). A comprehensive IoT attacks survey based on a building-blocked reference model. International Journal of Advanced Computer Science and Applications, 9(3), 355–373. https://doi.org/10.14569/IJACSA.2018.090348

[2] Abdel-Basset, M., Manogaran, G., & Gamal, A. (2019). A comprehensive review of federated learning in the Internet of Things: Challenges and future research directions. IEEE Access, 7, 173747–173764. https://doi.org/10.1109/ACCESS.2019.2955640

[3] Aggarwal, C. C. (2016). Outlier analysis (2nd ed.). Springer. https://doi.org/10.1007/978-3-319-47578-3

[4] Cherukuri, B. R. (2020). Microservices and containerization: Accelerating web development cycles.

[5] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[6] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122. https://doi.org/10.3390/info10040122

[7] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

[8] Carlini, N., & Wagner, D. (2017). Towards evaluating the robustness of neural networks. IEEE Symposium on Security and Privacy (SP), 39–57. https://doi.org/10.1109/SP.2017.49

[9] Jain, A. M. (2023). AI-Powered Business Intelligence Dashboards: A Cross-Sector Analysis of Transformative Impact and Future Directions.

[10] Cherukuri, B. R. (2019). Future of cloud computing: Innovations in multi-cloud and hybrid architectures.

[11] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[12] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Cyber threat intelligence: Challenges and opportunities. Computers & Security, 72, 140–166. https://doi.org/10.1016/j.cose.2017.09.001

[13] Doshi, R., Yilmaz, E., & Reddi, V. J. (2018). Adversarial machine learning in network intrusion detection: Current trends, challenges and research directions. Proceedings of the 2018 Workshop on Machine Learning for Cybersecurity, 1–8. https://doi.org/10.1145/3268876.3268889

[14] Patel, A., & Patel, R. (2023). Analytical Method Development for Biologics: Overcoming Stability, Purity, And Quantification Challenges. Journal of Applied Optics, 44(1S), 1-29.

[15] Gómez, J., & Moens, M. (2019). Hybrid deep learning-based anomaly detection in IoT: A multi-model approach. Future Generation Computer Systems, 98, 653–668. https://doi.org/10.1016/j.future.2019.03.011

[16] Malhotra, S., Saqib, M., Mehta, D., & Tariq, H. (2023). Efficient Algorithms for Parallel Dynamic Graph Processing: A Study of Techniques and Applications. International Journal of Communication Networks and Information Security (IJCNIS), 15(2), 519-534.

[17] Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making machine learning robust against adversarial inputs. Communications of the ACM, 61(7), 56–66. https://doi.org/10.1145/3134599

[18] Masurkar, P. P., Chatterjee, S., Sherer, J. T., Chen, H., Johnson, M. L., & Aparasu, R. R. (2022). Risk of serious adverse events associated with individual cholinesterase inhibitors use in older adults with dementia: A population-based cohort study. Drugs & Aging, 39(6), 453-465.

[19] Goyal, P., Mahajan, D., Gupta, A., & Misra, I. (2021). Self-supervised learning for domain adaptation and generalization in IoT networks. IEEE Transactions on Neural Networks and Learning Systems, 32(4), 1426–1439. https://doi.org/10.1109/TNNLS.2021.3052634

[20] Hady, M. F. M. A., & Schwenker, F. (2017). Semi-supervised learning: A brief review. Proceedings of the 2017 International Conference on Machine Learning and Cybernetics, 1–6. https://doi.org/10.1109/ICMLC.2017.8107631

[21] Cherukuri, B. R. Developing Intelligent Chatbots for Real-Time Customer Support in E-Commerce.

[22] Patel, R., & Patel, A. (2023). Overcoming Challenges in Vaccine Development: Immunogenicity, Safety, and Large-Scale Manufacturing. Well Testing Journal, 32(1), 54-75.

[23] He, K., Fan, H., Wu, Y., Xie, S., & Girshick, R. (2020). Momentum contrast for unsupervised visual representation learning. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 9729–9738. https://doi.org/10.1109/CVPR42600.2020.00975

[24] Huang, C., Zhang, G., Sun, Y., & Yu, H. (2020). Federated learning for intrusion detection in industrial cyber-physical systems. IEEE Transactions on Industrial Informatics, 16(6), 4290–4299. https://doi.org/10.1109/TII.2020.2973176

[25] Talati, D. V. (2023). Artificial intelligence and information governance: Enhancing global security through compliance frameworks and data protection. International Journal of Innovative Research in Computer and Communication Engineering, 12(6), 8418–8427. https://doi.org/10.15680/IJIRCCE.2023.1206003

[26] Jangid, J. (2020). Efficient Training Data Caching for Deep Learning in Edge Computing Networks.

[27] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., & Zhao, S. (2021). Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[28] Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. A., Dang, T. N., & Hong, C. S. (2020). Edge computing-enabled smart cities: A comprehensive survey. IEEE Internet of Things Journal, 7(10), 10200–10232. https://doi.org/10.1109/JIOT.2020.2997474

[29] Kim, D., Kim, J., Lee, H., Im, E. G., & Eom, J. (2018). Anomaly detection based on one-class SVM in IoT networks. Sensors, 18(7), 2174. https://doi.org/10.3390/s18072174