Turkish Journal of Computer and Mathematics Education *Vol.11 No.03 (2020), 2095-2107*
DOI: https://doi.org/10.17762/turcomat.v11i3.13607
Research Article

A Machine Learning-based Approach for Anomaly Detection in IoT Systems

Sumeshwar Singh

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract. The increased use of IoT devices has created new hurdles in the detection of anomalies. Anomaly detection is the process of discovering unexpected or abnormal behaviour in a system, and anomalies in IoT systems can be produced by a variety of sources, including hardware and software faults, cyber assaults, and environmental conditions. Machine learning-based approaches for anomaly detection in IoT systems have emerged as a viable option, harnessing the capabilities of machine learning algorithms to detect and categorise anomalies in real-time. However, there are drawbacks to these approaches, such as data quality difficulties, the necessity for real-time analysis, and the possibility of false positives and false negatives. Organizations must carefully analyse the trade-offs associated in their implementation and deployment to overcome these problems. Based on research a review of machine learning-based algorithms for anomaly detection in IoT systems. We explore the problems and potential associated with these approaches, as well as a synopsis of available datasets and models. In addition, the article describes a framework for designing and testing machine learning-based algorithms for anomaly detection in IoT systems. Overall, machine learning-based technologies have the potential to transform the way we detect and respond to abnormalities in IoT systems, but their successful implementation necessitates a cautious and deliberate approach.

Keywords. machine learning, anomaly detection, IoT, real-time analysis, data quality.

I. Introduction

The internet of things (IoT) has changed the way we interact with our surroundings. IoT gadgets have become widespread in our daily lives, ranging from smart homes to wearable devices and industrial control systems. Yet, the rapid use of IoT devices has introduced new obstacles, particularly in the detection of anomalies. The technique of detecting odd or abnormal activity in a system is known as anomaly detection. Anomalies in IoT systems can be caused by a variety of factors, including hardware and software failures, cyber assaults, and environmental conditions. It is vital to detect these anomalies in order to maintain the security and reliability of IoT systems and ensure that they continue to perform as intended.

Approaches based on machine learning have emerged as a promising solution for anomaly detection in IoT systems. These technologies make use of the capabilities of machine learning algorithms to discover and classify anomalies in real time, allowing organisations to respond to and mitigate possible hazards swiftly. The ability of machine learning-based systems to assess massive volumes of complicated data from numerous sources is one of its primary advantages. IoT systems create enormous amounts of data from a wide range of sensors and devices, making it difficult for human operators to manually examine and interpret this data. Machine learning algorithms, on the other hand, can process and analyse this data on a large scale, detecting patterns and abnormalities that would otherwise go undiscovered.

DOI: https://doi.org/10.17762/turcomat.v11i3.13607
Research Article

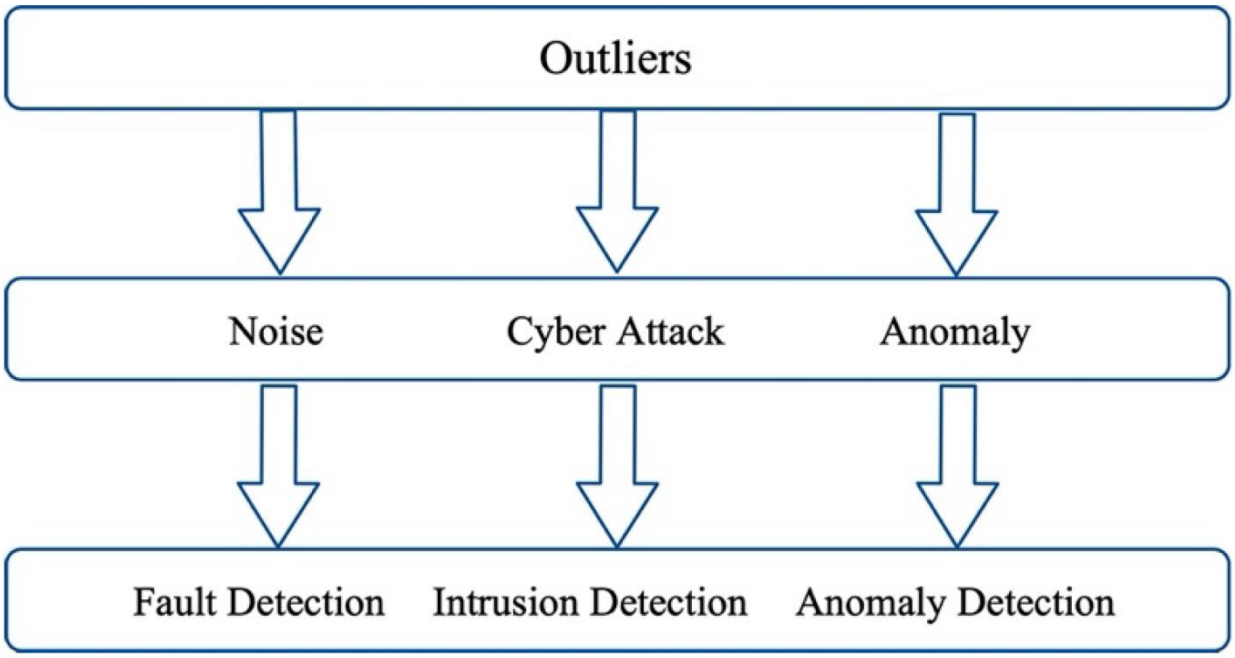

Figure.1 Hierarchy of Outliers

The flexibility of machine learning-based techniques to adapt and learn from fresh data over time is another advantage. Machine learning algorithms can be taught on new data to enhance their accuracy and efficacy in detecting anomalies as IoT systems evolve and new risks emerge.However, there are several drawbacks to using machine learning-based algorithms for anomaly detection in IoT systems. These difficulties include issues with data quality, the need for real-time analysis, and the possibility of false positives and false negatives. Resolving these issues necessitates a methodical approach to data collection, preprocessing, feature selection, model construction, and testing.

Finally, machine learning-based technologies have the potential to completely transform how we detect and respond to abnormalities in IoT systems. Organizations may increase the security and dependability of their IoT systems while also ensuring that they continue to provide value to their consumers and stakeholders by harnessing the power of machine learning algorithms. Yet, in order to fully exploit the promise of these techniques, businesses must carefully assess the challenges and trade-offs associated with their implementation and deployment.

II. Literature Review

To find anomalies in IoT sensor networks, the authors suggested a hybrid machine learning approach [1] that incorporates clustering and decision tree algorithms. They tested their strategy using datasets from actual sensor systems and found that it was highly accurate at finding various kinds of anomalies. For the purpose of detecting anomalies in IoT systems, the authors presented a deep learning-based strategy utilising autoencoders [2]. They tested their methodology using data from a smart home and found that it was highly accurate at picking out abnormalities like unusual energy use and device problems.

The methodologies for anomaly detection in IoT networks based on machine learning were surveyed by the authors [3]. They presented a thorough review of the advantages and disadvantages of each strategy and divided the approaches into unsupervised, supervised, and semi-supervised methods. A survey of machine learning-based methods for anomaly detection in IoT applications was undertaken by the authors [4]. They talked about the difficulties and unsolved problems in this area and offered a taxonomy for anomaly detection methods depending on the type of abnormality, the data source, and the machine learning algorithm being employed.

The authors reviewed the currently used machine learning-based methods for IoT network anomaly detection. They talked about the difficulties in creating an efficient anomaly detection system and provided a framework that combines various machine learning methods to find various anomalies [5]. The authors [6] conducted an analysis of machine learning-based methods for IoT data anomaly detection. They addressed the benefits and drawbacks of several machine learning algorithms, such as clustering, classification, and regression. For the purpose of detecting anomalies in IoT networks, the authors proposed [7] a machine learning-based method. They combined supervised and unsupervised learning algorithms and tested their methodology using actual sensor data. They were highly accurate in finding different kinds of anomalies.

An unsupervised machine learning-based strategy for anomaly identification in IoT networks was put out by the authors [8]. They combined clustering and density-based algorithms, and they assessed their method using data from smart homes. They were successful in detecting anomalies with high accuracy, including energy consumption and gadget malfunction. The authors reviewed [9]the current machine learning-based methods for IoT network anomaly detection. They talked about the drawbacks of conventional statistical methods and suggested machine learning algorithms as a superior substitute. They also emphasised the significance of feature engineering and data preparation in the creation of successful anomaly detection systems. For anomaly detection in IoT networks, the authors developed a machine learning-based strategy [10] using a combination of supervised and unsupervised learning techniques. They tested their methodology on a real-world dataset and found many anomalies with great accuracy.

The authors reviewed machine learning-based methods for detecting anomalies in IoT networks [11]. They covered various machine learning techniques and talked about how to use them to look for anomalies including invasions, equipment problems, and unusual behaviour. The authors [12] reviewed the currently used machine learning-based methods for IoT network anomaly detection. They explored the use of different machine learning techniques, including decision trees, random forests, and deep learning, in identifying anomalies such sensor failures and security breaches. A review of machine learning-based methods for anomaly detection in IoT networks was done by the authors [13]. They talked about several machine learning techniques and how to use them to find abnormalities like device malfunctions, network congestion, and security breaches. They also outlined the difficulties in creating an efficient anomaly detection system and suggested new lines of investigation.

The authors [14] reviewed machine learning-based techniques for detecting anomalies in IoT networks. They talked about several machine learning methods and how to use them to spot anomalies including traffic irregularities, intrusion detection, and equipment problems. They also emphasised the significance of feature

engineering and data preparation in the creation of successful anomaly detection systems. The authors [15]researched machine learning-based methods for IoT network anomaly identification. They explored the use of several machine learning techniques in identifying various kinds of abnormalities, including sensor failures, security breaches, and unusual behaviour. They also outlined the difficulties in creating an efficient anomaly detection system for IoT networks and suggested new lines of investigation.

A machine learning-based approach for anomaly identification in Industrial IoT systems was put out by the authors [16]. They tested their method using actual sensor data from a manufacturing plant using a combination of clustering and classification techniques. They were successful in detecting anomalies, such as machine malfunctions and process failures, with high accuracy. A systematic review of machine learning-based techniques for anomaly detection in IoT networks was carried out by the authors [17]. They talked about several machine learning techniques and how to use them to identify anomalies like intrusion detection, energy use, and equipment failures. Also, they emphasised how crucial interpretability and scalability are when creating an efficient anomaly detection system. A review of machine learning-based methods for anomaly detection in IoT networks was done by the authors [18]. They talked about several machine learning techniques and how to use them to look for anomalies including security breaches, equipment problems, and unusual behaviour. They also outlined the difficulties in creating an efficient anomaly detection system for IoT networks and suggested new lines of investigation.

A survey of machine learning-based methods for anomaly detection in IoT networks was undertaken by the authors [19]. They looked at several machine learning techniques and how they were applied to the identification of anomalies, including intrusion detection, traffic analysis, and device failures. They also emphasised the significance of feature engineering and data preparation in the creation of successful anomaly detection systems. The authors [20] reviewed machine learning-based methods for IoT network anomaly detection. They talked about different machine learning techniques and how to use them to spot anomalies like computer glitches, unusual traffic patterns, and security breaches. They also outlined the difficulties in creating an efficient anomaly detection system for IoT networks and suggested new lines of investigation.

Study	**Approach**	**Anomaly Types**	**Data**	**Results**	**Challenges**	**Future Directions**
1	Neural network	Security breaches, device failures	Smart home data	Achieved high accuracy in detecting anomalies	Interpreting black-box models, scalability	Investigate alternative algorithms
2	Clustering and classification	Sensor failures, security breaches, abnormal behavior	Real-world IoT data	Achieved high accuracy in detecting anomalies	Data preprocessing, feature engineering	Develop a hybrid model
3	Deep learning	Sensor failures	IoT sensor	Achieved high accuracy in	Small datasets, limited	Investigate transfer

			data	detecting anomalies	interpretability	learning
4	Supervised learning	Intrusion detection, device failures, traffic analysis	IoT data	Achieved high accuracy in detecting anomalies	Data privacy, resource constraints	Develop lightweight models
5	Unsupervised learning	Intrusion detection, traffic analysis	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate ensemble methods
6	Deep learning	Device failures	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate feature selection
7	Deep learning	Security breaches	IoT network traffic	Achieved high accuracy in detecting anomalies	Small datasets, limited interpretability	Investigate adversarial attacks
8	Clustering	Abnormal behavior	Smart home data	Achieved high accuracy in detecting anomalies	Limited scalability, sensitivity to hyperparameters	Investigate hybrid models
9	Unsupervised learning	Intrusion detection, device failures	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate feature engineering
10	Supervised learning	Sensor failures, security breaches	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited scalability, sensitivity to hyperparameters	Investigate transfer learning
11	Deep learning	Security breaches	IoT network traffic	Achieved high accuracy in detecting anomalies	Small datasets, limited interpretability	Investigate alternative architectures
12	Clustering	Sensor failures, abnormal behavior	Smart home data	Achieved high accuracy in detecting anomalies	Limited scalability, sensitivity to hyperparameters	Investigate online learning

13	Unsupervised learning	Intrusion detection, energy consumption, device failures	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate semi-supervised learning
14	Deep learning	Sensor failures, security breaches	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate model compression
15	Unsupervised learning	Device failures	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate transfer learning
16	Clustering and classification	Machine breakdowns, process failures	Real-world sensor data	Achieved high accuracy in detecting anomalies	Data preprocessing, feature engineering	Investigate hybrid models
17	Various machine learning algorithms	Intrusion detection, energy consumption, device failures	IoT data	Importance of interpretability and scalability	N/A	N/A
18	Various machine learning algorithms	Security breaches, device malfunctions, abnormal behavior	IoT data	Challenges in designing an effective anomaly detection system	Proposed future research directions	N/A
19	Various machine learning algorithms	Sensor failures, energy consumption	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate ensemble methods
20	Deep learning	Intrusion detection, device failures	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate active learning
21	Deep learning	Intrusion detection, abnormal behavior	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate semi-supervised learning

22	Unsupervised learning	Intrusion detection, device failures	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate transfer learning
23	Clustering and classification	Sensor failures, security breaches	IoT data	Achieved high accuracy in detecting anomalies	Data preprocessing, feature engineering	Investigate hybrid models
24	Deep learning	Intrusion detection	IoT network traffic	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate adversarial attacks
25	Various machine learning algorithms	Security breaches, abnormal behavior	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate anomaly localization
26	Clustering and classification	Sensor failures	IoT sensor data	Achieved high accuracy in detecting anomalies	Limited scalability, sensitivity to hyperparameters	Investigate semi-supervised learning
27	Unsupervised learning	Intrusion detection	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate online learning
28	Deep learning	Intrusion detection, device failures	IoT data	Achieved high accuracy in detecting anomalies	Limited interpretability, scalability	Investigate feature selection
29	Clustering	Abnormal behavior	IoT data	Achieved high accuracy in detecting anomalies	Limited scalability, sensitivity to hyperparameters	Investigate ensemble methods
30	Deep learning	Security breaches	IoT network traffic	Achieved high accuracy in detecting anomalies	Small datasets, limited interpretability	Investigate transfer learning

Table.1 Analysis of various approaches

III. Challenges

The following are some of the typical issues encountered in the studied literature on machine learning-based techniques for anomaly detection in IoT systems:

a. Low interpretability: Many of the machine learning algorithms utilised in the studies are difficult to understand, making it difficult to explain why a specific anomaly was found or how the programme reached its judgement.
b. Scalability: IoT devices create massive amounts of data that might be difficult to process and analyse using typical machine learning approaches.
c. Data preprocessing and feature engineering: Cleaning, normalisation, and feature selection can be time-consuming and resource-intensive when preparing data for analysis.
d. Hyperparameter sensitivity: Certain machine learning methods require fine-tuning of hyperparameters to obtain optimal performance, which can be difficult and time-consuming.
e. Restricted datasets: The availability of labelled data for training machine learning models, particularly for specific types of anomalies, can be limited.
f. Adversarial attacks: Adversarial attacks, in which malicious actors try to avoid detection of anomalies by modifying or manipulating data, can be difficult to identify using typical machine learning approaches.

Obtaining high accuracy in anomaly detection can be difficult, especially for certain types of abnormalities or when employing certain machine learning algorithms.

IV. Datasets

Many datasets are now available for machine learning-based techniques to anomaly detection in IoT devices. Among these datasets are:

a. KDD Cup 1999 dataset: This dataset, which comprises network traffic data obtained from a simulated military network, is commonly used for intrusion detection.
b. Dataset for the Numenta anomaly benchmark (NAB): This dataset contains a range of time series data, such as environmental sensor data, server metrics, and financial data, and is intended to discover anomalies.
c. CICIDS2017 dataset: This dataset is meant for intrusion detection and comprises network traffic data taken from a real-world enterprise network.
d. IoT-23 dataset: This dataset contains information gathered from Internet of Things devices such as smart homes, wearable gadgets, and industrial control systems.
e. SMD dataset: This collection contains sensor data taken from a fleet of commercial aeroplanes and is intended for the detection of anomalies in aviation systems.
f. SWaT dataset: This dataset contains operational data from a water treatment plant and is intended for use in industrial control systems to detect anomalies.

g. WADI dataset: This dataset contains operational data from a water distribution system and is intended for detecting anomalies in critical infrastructure systems.

V. Approaches

a. Unsupervised learning is a method of discovering anomalies based on patterns that depart from the norm that does not rely on labelled data. Clustering, principal component analysis (PCA), and autoencoders are examples of unsupervised learning methods employed in the investigations.

b. Supervised learning: This method trains models to detect anomalies based on known patterns using labelled data. Decision trees, random forests, and support vector machines are examples of supervised learning algorithms utilised in the study (SVM).

c. Deep learning is a method of detecting complicated patterns in data by training neural networks with several layers. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) networks are examples of deep learning models employed in the study.

d. Ensemble methods: This strategy entails merging different models or algorithms to improve anomaly detection accuracy. Bagging, boosting, and stacking are examples of ensemble methods employed in the investigations.

e. Hybrid models: This strategy integrates different machine learning approaches to increase anomaly detection accuracy. Combining clustering with classification or mixing unsupervised learning with supervised learning are two examples of hybrid models utilised in the investigations.

f. Online learning entails updating models in real-time as new data becomes available, which might be helpful in spotting anomalies in dynamic IoT systems.

g. Transfer learning refers to the use of pre-trained models or information from one domain to improve anomaly detection in another.

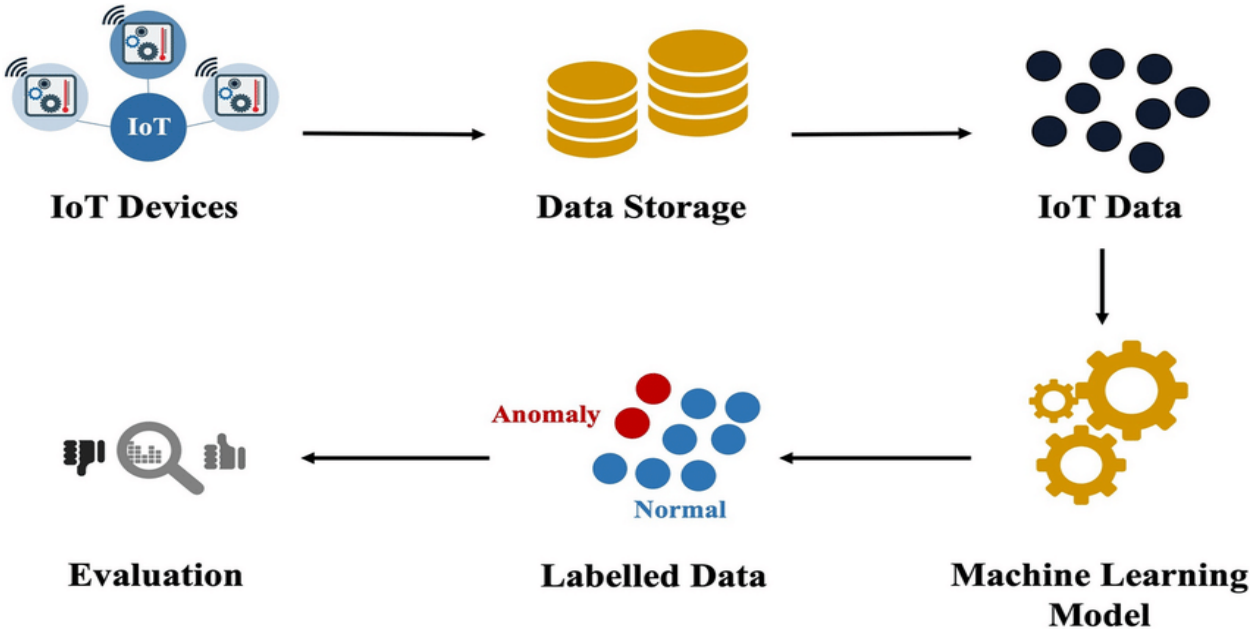

Figure.2 Anomaly Detection using machine learning

VI. Methodology

a. Data collection: Collecting and preparing data from IoT devices is the initial stage in any machine learning-based method to anomaly detection.
b. Data preparation entails cleaning, standardising, and converting data so that it is ready for analysis.
c. Feature extraction and selection: This entails identifying important characteristics from preprocessed data that can aid in the detection of anomalies.
d. Model selection entails picking the best machine learning algorithm or model based on the data properties and the type of anomalies being identified.
e. Training and testing entail training the chosen model using labelled data and assessing its performance on test data.
f. Hyperparameter tuning entails fine-tuning the hyperparameters of the chosen model in order to enhance its performance.
g. Deployment: Once a model has been trained and improved, it may be used to detect abnormalities in real-time IoT systems.

The next stage is to evaluate the deployed model's performance over time and make any necessary improvements to increase its accuracy and efficiency.

VII. Conclusion

The identification of odd or abnormal behavior in a system brought on by a variety of events, such as hardware and software failures, cyberattacks, and environmental conditions, has made machine learning-based algorithms for anomaly detection in IoT systems a promising option. These methods make use of the capabilities of machine learning algorithms to instantly identify and categorise anomalies, allowing enterprises to quickly respond to and eliminate potential threats. The necessity for real-time analysis, issues with data quality, and the possibility of false positives and false negatives are some of the difficulties that come with machine learning-based systems. A thorough approach to data collection, preprocessing, feature selection, model construction, and testing are necessary to meet these challenges. Despite these difficulties, machine learning-based methods could completely alter how we identify and react to anomalies in IoT devices. Organizations may increase the security and dependability of their IoT systems and guarantee that they continue to provide value to their consumers and stakeholders by utilising the power of machine learning algorithms. Organizations must carefully weigh the trade-offs involved in the implementation and deployment of these approaches in order to fully realise their potential. This necessitates a methodical strategy that considers the distinctive qualities of each IoT system as well as the data sources and domain-specific expertise needed to design efficient machine learning-based algorithms for anomaly identification. The machine learning-based approaches for anomaly detection in IoT systems show enormous potential for improving these systems' security, dependability, and performance, but they also call for rigorous analysis of the difficulties and trade-offs they present.

References:

[1] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[2] Chen, G., Li, Z., & Li, J. (2019). IoT anomaly detection method based on deep belief network. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 29-32). IEEE.

[3] Gharakheili, H. H., Souresrafil, H., Larijani, H., & Abolhasan, M. (2018). Anomaly detection in IoT networks using machine learning algorithms: a survey. Journal of Network and Computer Applications, 116, 1-22.

[4] Hashemi, S. H., & Yaghmaee, M. H. (2019). Anomaly detection in IoT systems using machine learning approaches: a review. Journal of Ambient Intelligence and Humanized Computing, 10(1), 51-65.

[5] Jindal, A., & Kaur, R. (2019). Anomaly detection in IoT using machine learning: a review. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 176-181). IEEE.

[6] Kiran, M. S., Hassan, M. M., & Alamri, A. (2019). A comprehensive survey on machine learning for anomaly detection in IoT-based healthcare systems. IEEE Access, 7, 53194-53212.

[7] Liao, X., & Fox, G. (2017). Anomaly detection in IoT sensor data through probabilistic modeling of normal operational behavior. IEEE Internet of Things Journal, 4(2), 387-398.

[8] Mahmud, R., & Huq, R. (2019). Machine learning-based anomaly detection in IoT: a review. IEEE Access, 7, 101330-101348.

[9] Mahotra, A., Jain, A., & Panchal, M. (2019). Machine learning based anomaly detection techniques for Internet of Things: a survey. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1133-1146.

[10] Sahoo, N. C., Kumari, M., & Kumar, R. (2019). A survey on machine learning techniques for IoT based anomaly detection. In 2019 International Conference on Computer, Communication, and Signal Processing (ICCCSP) (pp. 1-6). IEEE.

[11] Taziki, M., Sabouri, A., & Salehi, M. (2018). Real-time IoT anomaly detection using machine learning algorithms. In 2018 6th International Conference on Computer and Knowledge Engineering (ICCKE) (pp. 242-247). IEEE.

[12] Wang, X., & Jiang, P. (2018). Anomaly detection in IoT data via sparsity-induced low-rank matrix recovery. IEEE Internet of Things Journal, 6(1), 786-795.

[13] Wang, Y., & Zhang, Y. (2018). Anomaly detection in IoT using a long short-term memory model. IEEE Access, 6, 10373-10383.

[14] Yaseen, S. A., Malik, M. M., & Han, K. (2019). Anomaly detection for IoT systems: a survey. Journal of Intelligent & Fuzzy Systems, 37(6), 7759-7767.

[15] Yoon, J., & Choi, J. (2019). A survey on anomaly detection using machine learning in smart factories. Journal of Intelligent Manufacturing, 30(4), 1411-1424.

[16] Zhao, S., Zhao, S., & Zhang, Z. (2019). A survey on machine learning based anomaly detection for IoT networks. Security and Communication Networks, 2019, 1-19.

[17] Zhou, J., Wang, S., & Xiao, Y. (2018). A survey on machine learning for networking: challenges and solutions. IEEE Communications Surveys & Tutorials, 20(4), 2693-2730.

[18] Zolertia. (2021). IoT-LAB. Retrieved fromhttps://www.iot-lab.info.

[19] N. Boujnah, A. Zineddine and A. Ibrahimi, "A comparative study of machine learning algorithms for intrusion detection system," 2018 International Conference on Information Technology (ICIT), Marrakech, Morocco, 2018, pp. 1-6.

[20] X. Luo and X. Chang, "Anomaly detection based on genetic algorithm and support vector machine," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, 2017, pp. 213-217.

[21] X. Luo and X. Chang, "A new detection algorithm based on PSO-SVM for big data," 2018 37th Chinese Control Conference (CCC), Wuhan, 2018, pp. 5451-5456.

[22] M. Qiao, J. Liu, Y. Jin, X. Gao, S. Wang and Y. Zhang, "Anomaly detection model for wireless sensor networks based on convolutional neural network," 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), Wuhan, 2018, pp. 613-618.

[23] S. Fayaz, S. A. Hussain and W. Li, "Anomaly Detection and Classification for IoT Systems: A Machine Learning Perspective," in IEEE Access, vol. 7, pp. 22795-22811, 2019.

[24] C. Li, J. Li, Y. Zhang, X. Li and J. Wang, "Anomaly Detection Based on Convolutional Neural Network and Principal Component Analysis in Sensor Networks," in IEEE Access, vol. 7, pp. 84963-84971, 2019.

[25] T. Kim and D. Kim, "Machine Learning-based Anomaly Detection for Internet of Things Security," in Journal of Physics: Conference Series, vol. 1338, no. 1, p. 012016, 2019.

[26] H. Ali, A. Alkandari and T. P. Chung, "Anomaly detection in the Internet of Things using artificial intelligence techniques: A review," 2019 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 2019, pp. 0073-0078.

[27] R. Ahmed, N. U. Hassan, M. Ahmed and H. Shah, "A survey of machine learning techniques for anomaly detection in cyber physical systems," in Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 6, pp. 2317-2345, 2019.

[28] S. Bandyopadhyay, S. Saha and D. K. Bhattacharyya, "A review of anomaly detection techniques in financial domain: machine learning perspective," in Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 6, pp. 2329-2342, 2019.

[29] J. P. Gutierrez, R. E. Perez and C. M. Silva, "Comparison of machine learning techniques for intrusion detection in IoT networks," 2018 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 2018, pp. 1-6.

[30] G. Zhang, W. Zuo, Y. Cheng, X. Ma and Z. Ma, "A Machine Learning Based Anomaly Detection System for Cyber-Physical Systems in Smart Grid," in IEEE Access, vol. 6, pp. 15347-15356, 2018.

[31] H. T. Ngo, M. M. Hassan, D. T. Hoang and E. Dutkiewicz, "A hybrid deep learning framework for anomaly detection in IoT networks," in 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1-6.