The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4735

# Machine Learning Techniques for Enhancing Internet of Things (IoT) Performance : A Review

**Diana Hayder Hussein[1], Rebwar Abdulmajeed Abdullah[2], Shavan Askar[3], Media Ali Ibrahim[4]**
diana.hussein@epu.edu.iq[1], rebwar.abdullah@epu.edu.iq[2], shavan.askar@epu.edu.iq[3], media.ibrahim@epu.edu.iq[4]
[1,2,3,4] Information System Engineering Department, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq

**Article Information**

Received : 12 Feb 2025
Revised : 23 Feb 2025
Accepted : 26 Feb 2025

**Keywords**

Machine Learning (ML), Internet of Things (IoT), smart city, supervised learning, unsupervised learning.

**Abstract**

The Internet of Things (IoT) is basically billions of interconnected smart devices that can communicate with little interference from humans, thus making life easier. The IoT is a fast-moving area of research, and the challenges are growing, thus requiring continuous improvement. As IoT systems become more challenging to improve, machine learning (ML) is increasingly incorporated into IoT systems to develop better capabilities. This article review explores several machine learning techniques aimed at enhancing the performance of IoT systems. It highlights the growing importance of integrating machine learning with IoT to address challenges such as data management, security, and real-time processing. The techniques discussed include supervised learning, unsupervised learning, reinforcement learning, deep learning, ensemble methods, anomaly detection, and federated learning. Each method is evaluated for its effectiveness in optimizing IoT applications, such as predictive maintenance, energy efficiency, and smart city solutions. The review emphasizes the potential of these techniques to improve decision-making processes, automate operations, and enhance user experiences. Additionally, it addresses the limitations and challenges associated with implementing machine learning in IoT environments, including data privacy concerns and the need for robust algorithms capable of handling diverse datasets. Overall, the article underscores the transformative role of machine learning in advancing IoT capabilities and suggests future research directions to further leverage these technologies for improved system performance and reliability.

## A. Introduction

The Internet of Things (IoT) and machine learning (ML) are developing a new vision of the world of data innovation to build a strong global structure by fusing real and virtual objects with recently created extensions and sensors[1].The Internet of Things (IoT) has changed the way devices communicate, enabling a wide range of applications from smart homes and healthcare to industrial and agricultural automation [1]. However, IoT systems face significant challenges related to performance, scalability, security, and energy efficiency [2]. To address these challenges, researchers have turned to machine learning (ML) techniques, which offer the potential to optimize IoT operations, improve decision-making processes, and improve overall system performance [3]. This review combines findings from seven key papers that focus on the application of machine learning techniques to enhance IoT performance [4]. These papers examine various ML methods, including supervised learning, reinforcement Machine learning, unsupervised learning, and deep learning are applied across a wide range of IoT contexts [5]. They demonstrate how ML can help improve the efficiency, scalability, security, and energy management of IoT systems, enabling smarter, more adaptive, and more resilient networks [6]. By facilitating intelligent data analysis, predictive maintenance, anomaly detection, and real-time decision-making, machine learning (ML) has become a potent tool for improving IoT efficiency. Machine learning (ML) may enhance network efficiency, optimize resource allocation, and fortify IoT security by utilizing supervised, unsupervised, and reinforcement learning models. Furthermore, ML's integration with cloud and edge computing improves computational efficiency and scalability [7]. The many machine learning approaches used in IoT to improve system performance are examined in this review. It talks about important machine learning models, how they are used in various IoT areas, and the difficulties in putting them into practice. The report also outlines new developments and potential lines of inquiry for enhancing IoT effectiveness with AI-powered solutions [8].

## B. Research Method

This section present the integration of ML techniques into the IoT ecosystem has become a key research area aimed at improving the performance, efficiency, and scalability of IoT systems [20]. This topic illustrates the wide range of methods and approaches used to apply ML to IoT challenges [22]. Below, the methods used in these studies are analyzed, highlighting common techniques and distinctive strategies employed to enhance IoT performance . The Integrating machine learning into IoT systems promises significant advances in key areas, such as real-time data analysis, resource optimization, and anomaly detection [7]. However, as the reviewed articles also point out, there are several challenges in applying these ML techniques in resource-restricted environments, including limited computing power, data privacy concerns, and the need for a large volume of tagged data [8]. This introduction provides a brief overview of the importance of machine learning to enhance the performance of the IoT and provides the basis for a deeper exploration of the various ML techniques examined in the selected articles. Through this combination, our goal is to identify key trends, benefits, challenges, and future research orientations at the intersection of ML and IoT technologies, IoT refers to the use of the internet to link physical devices in order to enable seamless information sharing. The IoT's technical assistance is essential to realizing the dream of a smart city and would not be achievable without it. A vast amount of data is generated by "things" in the context of urban IoT. One important issue that machine learning can address is extracting important insights from this data. Urban IoT ML differs slightly from other domains because of its diverse range of devices, data, and applications as also illustrated in figure 1 [9].

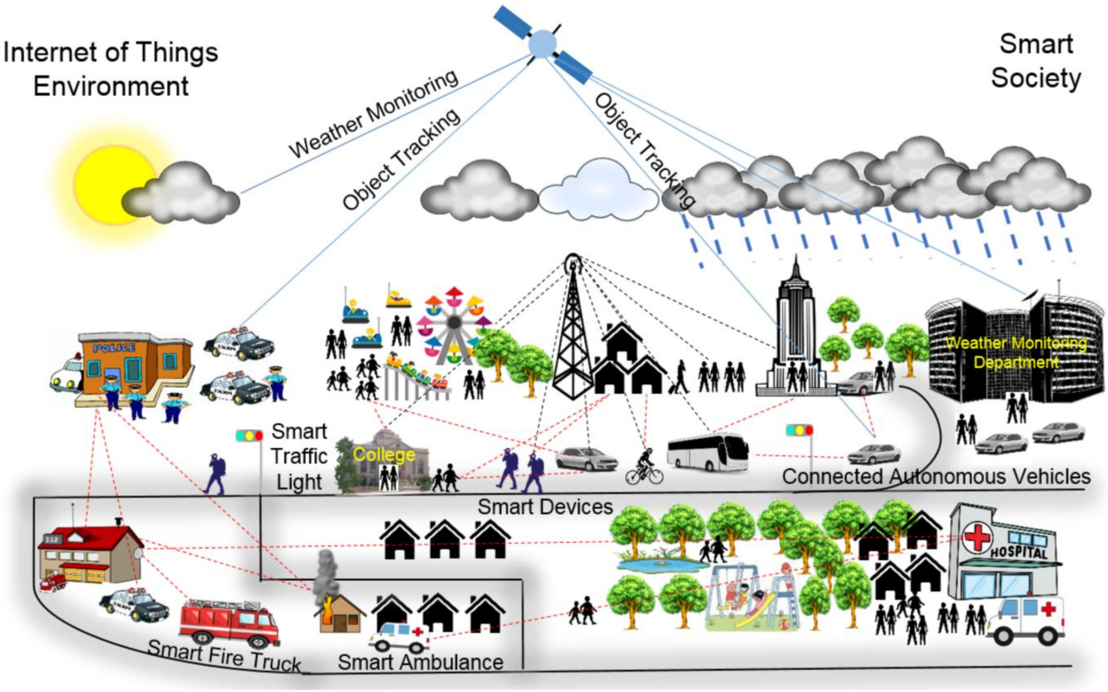


**Figure 1**. Machine Learning-Enabled Internet of Things (loT)

## Data production of ML enabled (IoT)

The ability to sense various activities and events occurring in our surroundings through technical infrastructure is one of the important roles of the Internet of Things. A large amount of data is anticipated to be produced via IoT. These data would be produced by several suppliers, resulting in data as a service. Data and information exchange and collaboration will be essential to delivering sustainable and pervasive applications and services that will enable smart cities and societies to reach their full potential [10]. In ubiquitous environments, combining several data types and forms to improve data quality and decision-making will be crucial. "The theory, techniques, and tools used to combine sensors' data, or data derived from sensory data, into a common representational format" is what data fusion represents [10]. The Internet of Things (IoT) refers to a network of interconnected devices and sensors that collect, exchange, and analyze data to deliver smarter services and solutions in a variety of domains, including smart homes, healthcare, transportation, and industrial automation, as shown in figure 2 [10]. As IoT systems grow in complexity and scale, optimizing their performance is becoming increasingly important. ML techniques are being integrated into IoT frameworks to address challenges such as data overload, resource constraints, energy efficiency, real-time decision-making, and security [11]. ML, which involves the use of algorithms that enable systems to learn from data and make predictions or decisions, plays a significant role in enhancing the performance of the Internet of Things [12].


**Figure 2.** Machine Learning and loT-Based Solutions in Industrial

**Machine learning techniques applied in IoT systems**

**Supervised Learning:** Supervised learning is one of the most common ML techniques used in IoT applications [13]. On this approach, models are trained on labelled datasets to predict outcomes or classify data [14]. For example, supervised learning can be used for anomaly detection; IoT systems can use supervised learning models to detect unusual behaviour or failures in devices or networks [15]. For example, in predictive maintenance, sensors on industrial equipment can be monitored for irregular patterns [16]. Helping to identify potential failures before they occur. Energy consumption prediction in smart homes or buildings, supervised learning can predict energy consumption based on historical data, leading to more efficient resource allocation and energy savings [17].

**Unsupervised Learning:** Unlike supervised learning, unsupervised learning does not require labeled data [18]. Instead, it identifies hidden patterns or structures in the data [19]. Unsupervised learning techniques, such as clustering and dimensionality reduction, are useful in several IoT applications.

**Machine Learning Techniques to Enhance IoT Performance**

The main approach in the reviewed papers focuses on the use of various machine learning techniques to enhance the performance of IoT systems [29]. Below is an analysis of the main ML techniques used:

**Supervised Learning:** Regression and Classification Models Many studies use supervised learning models such as decision trees, support vector machines (SVMs), and random forests to predict specific outcomes or classify IoT data into predefined categories [30]. For example, in predictive maintenance, supervised learning is applied to predict the failure of industrial machines based on sensor data [31]. Training data Supervised learning models rely heavily on large, labelled datasets that are collected from historical data from IoT devices [32].

**Unsupervised Learning:** Clustering Algorithms K-means, DBSCAN, and hierarchical clustering are commonly used in peer-reviewed literature to identify hidden patterns in data [33]. These techniques can help group similar devices, predict device behaviour, or identify clusters of devices prone to anomalies [34].

**Dimensionality reduction:** Techniques such as principal component analysis (PCA) are used to reduce the dimensions of large datasets from IoT sensors, making it easier to process and analyse [1].

**Policy optimization:** Methods such as Q-learning and deep Q-networks (DQN) are used to train models that can dynamically adjust parameters in real-time IoT systems, such as bandwidth allocation in communication networks [4].

**Deep Learning:** Convolutional Neural Networks (CNN): In IoT applications involving image or video data, CNNs are used for tasks such as image recognition, object detection, and anomaly detection. For example, IoT-enabled cameras in smart cities or smart homes use CNNs to identify objects or monitor surveillance data [5].

**Recurrent Neural Networks (RNN):** For sequential IoT data (e.g., time series data from sensors), RNNs, especially long-term memory networks (LSTM), are used to model temporal dependencies and predict future trends or system states [6].

## Data Collection and Preprocessing

Most of the reviewed papers emphasize the importance of data collection and preprocessing as a fundamental step in implementing ML for IoT systems [23]. Given that IoT devices generate large amounts of data in real time, many studies follow similar approaches in this regard to IoT sensors and device networks. Data is typically collected from various IoT devices such as sensors, smart meters, wearables, cameras, or industrial machinery [24]. These devices continuously produce raw data, which is often needed filtered; it is cleaned and pre-processed before being fed into ML models [25]. Data Preprocessing techniques, Common preprocessing techniques include noise reduction, Filtering out irrelevant data or noise from sensor readings [26]. Data normalization, ensuring standardization or scaling of data to facilitate model training [27]. Missing Data Imputation Handling missing or incomplete data through interpolation or using models to predict missing values [28].

## Model Training and Evaluation

Training machine learning models on IoT data involves several key steps that are common in studies. Data Splitting in most methodologies, data is split into training, validation, and test datasets [7]. This approach ensures that the models generalize well to unseen data [8]. Cross-validation is used to avoid overfitting and ensure robust performance; many papers use k-fold cross-validation, especially in supervised learning scenarios [9]. This technique divides the training data into k subsets and trains the model k times, using each subset for testing once [10]. Performance metrics, evaluation of machine learning models, usually include metrics such as accuracy, precision and recall used for classification tasks to measure the performance of the model [11]. Root Mean Square Error (RMSE), Mean Absolute Error (MAE). These are common metrics for regression tasks, especially in predictive maintenance or energy consumption forecasting [12]. F1 score is often used in cases of imbalance in classes, especially in anomaly detection [13].

### Literature Review

The integration of machine learning (ML) into Internet of Things (IoT) systems has become a major research focus due to its potential to significantly improve performance in various IoT domains [18]. Through a review of several articles, This section presents key findings, applications, challenges, and opportunities related to using ML techniques to enhance IoT performance [19].

### Integration of Machine Learning (ML) Techniques into IoT systems

[1] provide a comprehensive review of the integration of machine learning (ML) techniques into IoT systems [20]. It examines various ML models and their applications in IoT, focusing on their impact on system performance and efficiency. This survey categorizes ML algorithms into supervised and unsupervised. The authors identified key ML techniques driving the advancement of IoT systems, with supervised learning dominating in classification and regression [22]. Unsupervised learning in anomaly detection and applications of reinforcement learning on network optimization and dynamic resource allocation.

[3] survey explores the intersection of IoT and machine learning and details how various ML techniques can improve IoT applications [30]. The article categorizes ML methods in the Internet of Things into data-driven and model-driven approaches, providing examples of their application in healthcare, smart cities, and smart homes [28]. The authors found that ML in IoT leads to improved system adaptability, resource efficiency, and decision-making [29]. Specifically, supervised learning was It is often used in healthcare to predict disease, while reinforcement learning has been effective in optimizing energy consumption in smart homes [30].

[7] focuses on the integration of machine learning techniques with IoT to develop smart city solutions. While [7] discuss applications in areas such as traffic management, waste management, and energy consumption optimization. [8] also covers the challenges and future directions for deploying IoT and ML technologies in urban environments [9]. The authors concluded that ML-based solutions have significantly enhanced smart city systems, especially in optimizing traffic flow through [10]. Analyze and reduce energy consumption through demand forecasting. [11]) They also noted that scalability and real-time data processing remain key challenges for the widespread implementation of IoT and ML in smart cities [12].

**Security and Privacy Challenges in IoT systems**

[2] examine the security and privacy challenges in IoT systems. [23] focuses on machine learning techniques used to enhance IoT security and discusses their effectiveness in intrusion detection, authentication, and secure communication; it also addresses privacy concerns, showing how ML can be used to mitigate risks while ensuring data confidentiality [24]. This study showed that machine learning models, especially anomaly detection models (such as clustering and neural networks), can significantly improve security [25]. IoT systems are increasingly being used to detect malicious activity. However, challenges such as data privacy and the scalability of these models in large networks remain critical obstacles [26].

**Application of data mining and machine learning techniques in IoT**

[4] discussed and described the application of data mining and machine learning techniques in cybersecurity for intrusion detection with a focus on the Internet of Things. Networks compare various ML methods, including decision trees, SVMs, and neural networks, to detect network anomalies and malicious behaviors [31]. The study showed that machine learning models, especially decision trees and support vector machines (SVMs), showed strong performance in detecting Infiltration of IoT networks [31]. However, the authors noted the need for continuous retraining of the model to adapt to evolving attack patterns and increase the model's accuracy [32].

**Machine learning approaches for securing IoT systems**

[5] provides an overview of machine learning approaches for securing IoT systems [33] It covers a wide range of ML models. Learn deep learning and its application in securing IoT devices and communication protocols against attacks such as data breaches, denial of service (DoS), and eavesdropping [34]. The authors highlight the effectiveness of deep learning methods in detecting complex attacks such as DoS while SVM and random forests are for easier attack detection. They also noted that hybrid models combining multiple ML techniques can improve overall security in IoT networks by addressing different types of threats [1].

**Reinforcement Learning for IoT-Enabled Wireless Networks**

[6] survey explores the application of reinforcement learning (RL) in optimizing wireless networks equipped with IoT. [36] This paper discusses different RL algorithms and their potential to address challenges such as resource allocation, energy management, and dynamic spectrum access in wireless IoT networks. [3] This study showed that RL models, especially Q-learning and deep Q-networks (DQN), were very effective in optimizing resource allocation in IoT networks [4]. These models were dynamic [5]. Adjusting to network conditions, improving throughput, and reducing latency. However, the authors noted that the computational complexity of RL algorithms needs to be reduced for practical deployment in IoT networks [6].

## C. Result and Discussion

The integration of ML techniques into IoT systems has led to significant improvements in performance optimization, security, and scalability [19]. The following discussion synthesizes key insights from these papers, focusing on how to enhance IoT systems, challenges ahead, and emerging directions for future research [21].

**Enhancing IoT Performance with Machine Learning**

Machine learning techniques have become essential for improving various aspects of IoT systems, especially in data analysis, optimization, and decision-making [1],[3]. Focus on how supervised learning models (e.g., decision trees, SVM) can be used for tasks such as predictive maintenance, energy optimization, and resource allocation in IoT environments [22]. By training algorithms on sensor data, IoT systems can predict failures or optimize energy consumption in real time, thereby improving system efficiency and reducing costs [24]. Furthermore, unsupervised learning, especially clustering techniques, is widely used for anomaly detection in large-scale IoT networks [1]. This approach helps to identify abnormal behaviour patterns such as security system breaches or failures, which can compromise the performance of the IoT system [25]. The ability of unsupervised learning to detect anomalies without labelled data is especially useful in rapidly changing environments where data patterns evolve over time [26].

**Security and privacy concerns**

A significant focus of several papers [2],[5] is on IoT security, where machine learning techniques play a significant role in defending against cyber threats [27]. The vulnerabilities of IoT networks due to their open nature and massive scale have led to the use of ML for intrusion detection systems (IDS) [28]. in [4] discuss how to supervise learning models, such as SVM And decision trees are widely used to detect malicious activity, while deep learning models are better equipped to detect more complex attacks, such as denial of service (DoS) attacks or man-in-the-middle attacks [29]. However, integrating ML for security also presents challenges. For example, the trade-off between security and privacy in IoT systems is complex. As [5] point out, using ML to enhance security often requires access to large volumes of sensitive data, which can raise concerns about data privacy. In [27] using federated learning, in which ML models are trained on devices without the need to transmit raw data to central servers, is one promising solution to address privacy issues while still using ML to enhance security [31].

**Machine Learning for Smart City Applications**

As discussed by [7] smart cities are one of the most promising areas for the application of IoT and machine learning [2]. A combination of IoT devices and ML It enables the collection and analysis of large volumes of data from urban environments, leading to improved traffic management and optimization of energy consumption and waste [3]. For example, ML algorithms can predict traffic patterns, reduce congestion, and optimize traffic light timing in real time [4]. Similarly, energy consumption can be dynamically adjusted based on demand forecasts, reducing waste and increasing efficiency [5]. Despite the potential [7] also highlight significant challenges in scaling these solutions to large urban environments [6]. Data privacy, system interoperability, and real-time data processing are critical barriers to this system [7]. Deploying ML-based solutions in smart cities These challenges emphasize the importance of developing more efficient, scalable, and privacy-preserving algorithms for smart city applications [8].

**Data Quality Challenges and Computational Limitations**

One of the recurring challenges in the literature is data quality and availability [9]. IoT systems generate large amounts of data, often in real time, but this data can be noisy and incomplete [10]. Several authors, including [2],[4] point out that the effectiveness of ML algorithms strongly depends on the quality of the data [11]. Data preprocessing, feature extraction, and noise reduction techniques are essential to improve the performance of ML models. In many cases, unsupervised learning algorithms are used in IoT systems to identify patterns in noisy or incomplete data without the need for extensive preprocessing [12]. Furthermore, the computational limitations of IoT devices, many of which are low-power and resource-constrained, pose significant challenges for deploying complex ML models, especially deep learning algorithms. In [6] discuss the limitations of RL algorithms in IoT environments due to high computational requirements. Strategies such as edge computing, where data processing occurs close to the source at the edge of the network [13]. It is increasingly being explored to address these limitations [15]. Edge computing reduces the need to transfer large data sets to centralized cloud servers, reduces network congestion, and improves response times [14].

**Future Research Directions**

The reviewed articles suggest several promising directions for future research in integrating ML with the Internet of Things [16]. These include:

**Hybrid ML models**: Combining different ML techniques, such as combining supervised learning with reinforcement learning or deep learning with unsupervised [17]. Learning can provide more robust and adaptive solutions for IoT systems. Hybrid models can be particularly useful in addressing complex tasks such as security, anomaly detection, and optimization in dynamic environments [18].

**Federated Learning for Privacy:** Given the concerns about privacy, especially in IoT systems that handle sensitive data, federated learning as discussed by [52] is gaining traction. [53] enable training of ML models on local devices without the need to share raw data, thus preserving user privacy while still benefiting from ML advances [54]. Explainability and interpretability of ML models as ML models become more integrated with IoT applications, ensuring that these models are interpretable and transparent, is essential for user trust and regulatory compliance [55]. Future research It should focus on developing methods to explain decisions made by ML models, especially in security and healthcare applications, where decisions can have significant consequences [56].

## D. Conclusion

Exploring machine learning techniques to enhance the performance of the IoT emphasizes the transformative impact that these technologies can have on various applications and industries. The reviewed literature highlights Several key insights, performance optimization, and machine learning algorithms significantly improve the performance of IoT systems by enabling smarter data processing, predictive analytics, and efficient resources. Managing these developments leads to increased responsiveness and reliability in IoT applications. Increased security and integrating machine learning into IoT frameworks play a significant role in strengthening security. Techniques such as anomaly detection and intrusion detection systems help identify and mitigate potential threats, thus protecting sensitive data and devices. Data Management, With the exponential growth of data generated by IoT devices, machine learning offers effective ways to analyse and interpret data. This capability helps extract valuable insights, facilitate better decision-making, and drive operational efficiency. Scalability and compatibility, machine learning models can adapt to changing and scaling environments by increasing the number of connected devices. This flexibility is essential to maintain optimal performance in dynamic IoT ecosystems**.** Energy efficiency by optimizing energy consumption through predictive maintenance and intelligent resource allocation, machine learning helps to make IoT systems more sustainable and energy efficient.

## E. References

[1] Z. Zhou, T. Zhang, and Y. Liu, “A survey on machine learning techniques in Internet of Things (IoT) systems,” *IEEE Access*, vol. 7, pp. 126189–126212, 2019. doi: 10.1109/ACCESS.2019.2933039.
[2] J. Li, F. Liu, and X. Zhang, “A comprehensive survey on IoT security and privacy issues,” *IEEE Access*, vol. 6, pp. 7278–7288, 2018. doi: 10.1109/ACCESS.2018.2802210.
[3] A. Sharma and R. Sharma, “Machine learning in IoT: A survey,” *IEEE Access*, vol. 5, pp. 10399–10413, 2017. doi: 10.1109/ACCESS.2017.2674282.
[4] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” *IEEE Commun. Surv. Tutor., vol. 18, no. 2, pp. 1153–1176, 2016. doi: 10.1109/COMST.2015.2494181.
[5] M. A. Ganaie and H. Kim, “An overview of machine learning approaches for Internet of Things (IoT) security,” *Wirel. Commun. Mob. Comput.*, vol. 2020, 2020. doi: 10.1155/2020/1854389.
[6] Z. Liu and Z. Xu, “Reinforcement learning for IoT-enabled wireless networks: A survey,” *IEEE Access*, vol. 8, pp. 21220–21235, 2020. doi: 10.1109/ACCESS.2020.2961781.
[7] S. Rani and S. Singh, “IoT and machine learning-based smart city solutions: A comprehensive review,” *IEEE Access*, vol. 7, pp. 157238–157258, 2019. doi: 10.1109/ACCESS.2019.2947057.
[8] S. Chatterjee and N. Dey, “A review of machine learning techniques in Internet of Things (IoT) applications,” *J. King Saud Univ. - Comput. Inf. Sci.*, 2020. doi: 10.1016/j.jksuci.2018.06.022.
[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Ayyash, and M. Al-Rakhami, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2347–2376, 2015. doi: 10.1109/COMST.2015.2444095.

[10] V. Vasilenko and V. Prokopenko, “Machine learning in the Internet of Things: Challenges and approaches,” *Adv. Intell. Syst. Comput.*, vol. 1016, pp. 215–221, 2020.
[11] S. Jiang and Z. Xu, “Machine learning for Internet of Things data analysis,” *J. Comput. Sci.*, vol. 25, pp. 96–102, 2018. doi: 10.1016/j.jocs.2018.07.014.
[12] S. Singh and B. Dahiya, “Optimization techniques for smart IoT systems using machine learning algorithms,” *Elsevier J. Comput. Netw., vol. 151, pp. 121–137, 2019.
[13] I. A. T. Hashem, I. Yaqoob, and M. Anwar, “The role of big data in Internet of Things,” *Comput. Netw.*, vol. 101, pp. 1–18, 2016. doi: 10.1016/j.comnet.2016.02.024.
[14] S. Ghosh and G. Manogaran, “Deep learning approaches in the Internet of Things,” *Comput. Mater. Continua*, vol. 63, no. 3, pp. 1299–1316, 2020.
[15] P. R. Suresh and S. Siva, “IoT and Machine Learning for Smart Cities: Trends and Challenges,” *J. Comput. Sci.*, vol. 28, pp. 50–58, 2018. doi: 10.1016/j.jocs.2018.12.015.
[16] M. Jain and P. Pande, “Internet of Things: A review of machine learning techniques in IoT systems,” *Int. J. Comput. Appl.*, vol. 178, no. 3, pp. 1–8, 2019.
[17] I. Pustokhina and S. Smirnov, “Machine learning methods for Internet of Things: A review,” in *Proc. IEEE 15th Int. Symp. Auton. Decentralized Syst. (ISADS)*, 2017, pp. 1–8.
[18] Y. Ren and W. Li, “Data-driven machine learning techniques for Internet of Things applications,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–6.
[19] K. Rohit and M. Pandey, “Intelligent IoT data processing using machine learning models,” *Future Gener. Comput. Syst.*, vol. 108, pp. 836–843, 2020.
[20] A. Bashir and M. Ahmad, “Machine learning techniques for IoT network optimization,” *Int. J. Mach. Learn. Cybern.*, vol. 10, no. 7, pp. 1453–1462, 2019.
[21] S. Hussain and K. Ghafoor, “A comprehensive survey of machine learning techniques in IoT networks,” *IEEE Access*, vol. 7, pp. 147273–147296, 2019. doi: 10.1109/ACCESS.2019.2946172.
[22] R. Nawaz and S. Hassan, “Internet of Things (IoT): Applications, security challenges and future directions,” *J. Netw. Comput. Appl.*, vol. 149, p. 102471, 2020.
[23] M. Shah and A. Singh, “A survey of machine learning techniques for IoT-based healthcare systems,” *Wirel. Commun. Mob. Comput., vol. 2019, p. 2871530, 2019. doi: 10.1155/2019/2871530.
[24] S. Rani and V. Kumari, “Application of machine learning in IoT: A review of techniques, challenges, and future trends,” *Soft Comput, vol. 24, no. 8, pp. 5723–5745, 2020.
[25] M. Sultana, “Machine learning in IoT: A comprehensive survey,” *Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 2, pp. 37–47, 2019.
[26] D. H. Hussein and S. Askar, "Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment," in *IEEE Access*, vol. 11, pp. 141723-141739, 2023, doi: 10.1109/ACCESS.2023.3343613.

[27] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in *IEEE Access*, vol. 12, pp. 39936-39952, 2024, doi: 10.1109/ACCESS.2024.3376670.
[28] M. A. Ibrahim and S. Askar, "An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm," in *IEEE Access*, vol. 11, pp. 133607-133622, 2023, doi: 10.1109/ACCESS.2023.3337034.
[29] D. H. Abdulazeez and S. K. Askar, "Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment," in *IEEE Access*, vol. 11, pp. 12555-12586, 2023, doi: 10.1109/ACCESS.2023.3241881.
[30] V. Srinivasan and S. Karthikeyan, "Machine learning for IoT applications: A survey," Soft Comput., vol. 24, no. 8, pp. 6057–6074, 2020.
[31] D. Sharma and S. Bansal, "A systematic review on machine learning applications for IoT-based smart healthcare systems," *Future Gener. Comput. Syst.*, vol. 105, pp. 130–149, 2020.
[32] S. Sharma and D. B. Rawat, "A comprehensive survey on IoT and machine learning integration for smart city applications," *Int. J. Comput. Appl.*, vol. 178, no. 1, pp. 12–18, 2019.
[33] O. Akdemir and M. Yildirim, "Machine learning for IoT in the healthcare domain: A survey," in *Proc. IEEE 11th Int. Conf. Cloud Comput.*, 2018, pp. 10–18.
[34] A. Sharma and R. Rana, "A survey of machine learning techniques for IoT-based anomaly detection systems," *Comput. Mater. Continua*, vol. 65, no. 2, pp. 943–960, 2020.
[35] F. Hussain and A. Raza, "IoT-based smart cities: The role of machine learning in optimizing traffic management," *J. Comput. Sci.*, vol. 44, p. 101095, 2020.
[36] M. Bansal and S. K. Sood, "Machine learning techniques for IoT and big data analytics in healthcare systems," *J. King Saud Univ.-Comput. Inf. Sci.*, 2019. doi: 10.1016/j.jksuci.2019.03.007.
[37] Y. Himeur et al., "AI-big data analytics for building automation and management systems: A survey, actual challenges and future perspectives," *Artif. Intell. Rev.*, vol. 56, no. 6, pp. 4929–5021, 2023. doi: 10.1007/s10462-022-10286-2.
[38] Mina Othman, Shavan Askar, Daban Ali, Media Ibrahim, Nihad Abdullah. Deep Learning Based Security Schemes for IoT Applications: A Review. The Indonesian Journal of Computer Science, vol 13, No. 2, 2024.
[39] Media Ibrahim, Shavan Askar, Mohammad Saleem, Daban Ali, Nihad Abdullah. Deep Learning in Medical Image Analysis Article Review. The Indonesian Journal of Computer Science, vol 13, No. 2, 2024.
[40] Harikumar Pallathadka, Shavan Askar, Ankur Kulshreshta, M. K. Sharma, Sabir Widatalla, & Mudae, I. (2024). Economic and Environmental Energy Scheduling of Smart Hybrid Micro Grid Based on Demand Response. International Journal of Integrated Engineering, 16(9), 351-365.

[41] B. H. Husain and S. Askar, "Smart Resource Scheduling Model in Fog Computing," *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)*, Erbil, Iraq, 2022, pp. 96-101, doi: 10.1109/IEC54822.2022.9807469.
[42] Zhang, L., Askar, S., Alkhayyat, A., Samavatian, M., & Samavatian, V. (2024). Machine learning-driven detection of anomalies in manufactured parts from resonance frequency signatures. Nondestructive Testing and Evaluation, 1–23. https://doi.org/10.1080/10589759.2024.2431143
[43] H. Hua et al., "Edge computing with artificial intelligence: A machine learning perspective," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–35, 2023. doi: 10.1145/3555802.
[44] Y. Wang and Y. Zhang, "A survey on machine learning for IoT: Applications, challenges, and future directions," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2247–2265, 2019.
[45] S. Li, Y. Li, and H. Li, "Machine learning for IoT: A survey," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4357–4371, 2020.
[46] S. Gupta and V. Gupta, "Machine Learning Techniques for IoT Performance Optimization: A Comprehensive Review," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 33, no. 1, pp. 1–12, 2021.
[47] J. Zhang and Y. Zhao, "A survey on machine learning techniques for IoT," *J. Netw. Comput. Appl.*, vol. 126, pp. 1–16, 2019.
[48] P. Kumar and R. Singh, "IoT and Machine Learning: A Review of Applications and Challenges," *Int. J. Comput. Appl.*, vol. 975, no. 8, pp. 25–30, 2020.
[49] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[50] Y. Yang and J. Wu, "Machine Learning-Based Approaches for IoT Security: A Survey," *IEEE Access*, vol. 9, pp. 134435–134456, 2021.
[51] R. Bhatia and A. Kumar, "Machine Learning Techniques in IoT for Smart Cities: A Survey," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 3, pp. 1151–1165, 2020.
[52] A. Alharbi and F. Alzahrani, "Machine Learning Techniques for IoT Data Analysis: A Review," *J. Comput. Netw. Commun.*, vol. 2021, Article ID 9970201, 2021.
[53] N. Mavridis and V. Koutkias, "Machine Learning in the Internet of Things: A Systematic Review," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 3, pp. 1856–1870, 2020.
[54] H. Kaur and S. Kaur, "Performance Evaluation of Machine Learning Algorithms in IoT Applications," *Int. J. Comput. Appl.*, vol. 975, no. 8, pp. 25–30, 2020.
[55] M. Mohsin and H. Zafar, "Enhancing IoT Performance with Machine Learning: A Review," *Wirel. Commun. Mob. Comput.*, vol. 2021, Article ID 8856132, 2021.
[56] M. Asadullah and M. Khan, "Applications of Machine Learning in IoT: A Review," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–35, 2020.
[57] W. Khan and M. Rehman, "Machine Learning Techniques in IoT: Challenges and Opportunities," *J. Sensors*, vol. 2021, Article ID 8843278, 2021.

[58] N. Zaman and M. Rahman, “Smart IoT Systems: Machine Learning Approaches for Performance Enhancement,” *J. Netw. Comput. Appl.*, vol. 152, Article ID 102530, 2020.
[59] Yang, Y., Patil, N., Askar, S. et al. Machine learning-guided study of residual stress, distortion, and peak temperature in stainless steel laser welding. Appl. Phys. A 131, 44 (2025). https://doi.org/10.1007/s00339-024-08145-8
[60] S. Askar, G. Zervas, D. K. Hunter and D. Simeonidou, "Classified cloning for QoS provisioning in OBS networks," 36th European Conference and Exhibition on Optical Communication, Turin, Italy, 2010, pp. 1-3, doi: 10.1109/ECOC.2010.5621339.
[61] F. E. F. Samann, S. Y. Ameen and S. Askar, "Fog Computing in 5G Mobile Networks: A Review," 2022 4th International Conference on Advanced Science and Engineering (ICOASE), Zakho, Iraq, 2022, pp. 142-147, doi: 10.1109/ICOASE56293.2022.10075567.
[62] Omer, S.M., Ghafoor, K.Z. & Askar, S.K. Lightweight improved yolov5 model for cucumber leaf disease and pest detection based on deep learning. SIViP 18, 1329–1342 (2024). https://doi.org/10.1007/s11760-023-02865-9.
[63] M. Chen, Y. Ma, Y. Li, D. Wu, and Y. Zhang, “Big data analytics for intelligent transportation systems: A survey,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 2, pp. 204–218, 2017.
[64] J. Bzai et al., “Machine Learning-Enabled Internet of Things (IoT): Data, Applications, and Industry Perspective,” *Electronics*, vol. 11, p. 2676, 2022.
[65] C. M. Mohammed and S. Askar, “Machine Learning for IoT Healthcare Applications: A Review,” *Int. J. Sci. Bus., vol. 5, no. 3, pp. 42–51, 2021. doi: 10.5281/zenodo.4496904.
[66] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Comput. Netw., vol. 54, pp. 2787–2805, 2010.
[67] Statista, “IoT Connected Devices Worldwide 2019–2030.” Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. [Accessed: Jun. 25, 2022].
[68] S. Askar, C. M. Muhammed, and S. W. Kareem, "Deep Learning in IoT systems: A Review," *International Journal of Science and Business*, vol. 5, no. 6, pp. 131–147, 2021. doi: 10.5281/zenodo.5221646.