International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

MATHEMATICAL MODELING OF MACHINE LEARNING ALGORITHMS IN INTERNET OF THINGS NETWORKS

Dr. Sajja Suneel[1], Gulzhan Kubanovna Esenamanova[2] , Pooja Singh[3], Gulmira Isaeva[4],

Dr. Sulaxan Jadhav[5], Azyk Orozonova[6]

[1]Assistant Professor, Department of CSE(Data Science), Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana - 500043, India.

[2]Senior Lecturer, S. Manaschy 141-86, Kyrgyz National University named after Jusup Balasagyn, Kyrgyz Republic

[3]Department of Physics, School of Basic and Applied Sciences, SGT University, Gurugram, Haryana- 122505, India.

[4]Candidate of physical and mathematical sciences, docent, Institute of Computer Technologies and Artificial Intelligence, Kyrgyz National University, 547 Frunze Street, Bishkek 720033, Kyrgyzstan.

[5]Assistant Professor, Symbiosis School of Economics, Symbiosis International (Deemed University), Pune, 411004, Maharashtra, India.

[6]Deputy Director for Research, International Higher School of Logistics, Kyrgyz State Technical University named after I. Razzakov, 66 Ch. Aitmatov Avenue, Bishkek 720044, Kyrgyz Republic.

Abstract

The integration of Machine Learning (ML) algorithms into Internet of Things (IoT) networks has significantly enhanced their capabilities, enabling intelligent decision-making, predictive analysis, and system optimization. This paper investigates the mathematical models that underlie the application of ML algorithms in IoT environments. It explores various ML techniques, including supervised, unsupervised, and reinforcement learning, alongside deep learning models, and presents their corresponding mathematical formulations. The challenges faced in IoT networks, such as limited resources, data heterogeneity, and real-time processing requirements, are addressed, and mathematical models that quantify the performance of these algorithms within IoT frameworks are discussed. The paper also examines the practical applications of these models in diverse IoT domains, such as healthcare, smart cities, and industrial IoT, emphasizing their scalability and efficiency. Furthermore, it outlines future research directions to optimize ML models and enhance their deployment in emerging IoT networks.

Keywords: Mathematical Modeling, Machine Learning, Internet of Things, Algorithms, Optimization, Reinforcement Learning, Deep Learning, IoT Networks, Performance Analysis.

Received: August 08, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the 21st century, reshaping how devices, systems, and objects are interconnected and interact. IoT refers to the network of physical objects embedded with sensors, software, and other technologies that allow them to collect and exchange data over the internet. Over the past decade, the proliferation of IoT devices has led to a significant expansion in its applications across a wide range of sectors[1]. These applications are not limited to consumer technology but extend to industrial, healthcare, agriculture, smart cities, and energy sectors, all of which leverage IoT networks to optimize operations, improve decision-making, and enhance productivity. In healthcare, IoT enables remote patient monitoring through wearable devices, while in smart cities, it powers traffic management, waste monitoring, and energy-efficient systems[2]. In industrial automation, IoT facilitates predictive maintenance and real-time monitoring of equipment, ensuring operational efficiency. As more devices become interconnected, the scale and complexity of IoT networks continue to increase, presenting new challenges and opportunities for innovation in data processing, connectivity, and security[3].

The growth of IoT networks has been accompanied by the generation of vast amounts of data, often referred to as “big data,” which must be processed, analyzed, and utilized effectively to derive actionable insights. The increasing volume and variety of data, combined with the need for real-time processing, highlight the need for intelligent systems capable of managing and interpreting such data. The traditional methods of data processing in IoT networks, often based on centralized cloud infrastructures, struggle to keep pace with the demands of latency-sensitive applications[4]. This has prompted the development of new architectures such as edge computing, where data is processed closer to the source, and fog computing, which extends cloud capabilities to the edge. These architectures, along with advances in data analytics and machine learning, are reshaping the IoT landscape, making it possible to harness the full potential of IoT networks across diverse applications.

Significance of Machine Learning

Machine learning (ML) plays a pivotal role in enhancing the functionality and efficiency of IoT systems. The ability of ML algorithms to learn from data, adapt to changing environments, and make decisions without explicit programming has led to their widespread adoption in IoT networks. One of the most significant contributions of ML to IoT is its ability to process large datasets and extract meaningful patterns and insights that are otherwise difficult to identify using traditional methods. ML algorithms are particularly effective in dealing with the high-dimensional, noisy, and heterogeneous data generated by IoT devices.

ML enables IoT systems to perform a wide range of tasks, including prediction, classification, and anomaly detection, all of which are essential for optimizing IoT applications. For instance, in predictive maintenance within industrial IoT (IIoT) environments, ML models can analyze sensor data from machines to predict failures before they occur, thereby reducing downtime and maintenance costs. In smart cities[5], ML algorithms are employed in traffic management systems to predict traffic patterns, optimize traffic lights, and reduce congestion. Moreover,

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ML enhances the security of IoT networks by detecting abnormal behavior that may indicate potential security breaches, such as unauthorized access or cyberattacks. Through its ability to improve decision-making and automate processes, ML has become an integral part of IoT networks, enabling smarter and more efficient systems.

In addition to its applications in specific domains, ML also facilitates the optimization of IoT networks themselves. Machine learning algorithms are used to optimize network resources, such as bandwidth and energy, and to ensure that IoT devices operate efficiently, even under constrained conditions[6]. By utilizing techniques such as reinforcement learning, IoT systems can adapt to dynamic network conditions and optimize their performance in real-time. Thus, ML is not only transforming the applications of IoT but is also revolutionizing the underlying infrastructure that supports IoT networks.

Research Objectives

This paper aims to explore the mathematical models that support the implementation of machine learning algorithms in IoT networks. While machine learning has been widely applied in various IoT domains, the mathematical underpinnings of these algorithms, particularly their performance in resource-constrained and real-time environments, have not been thoroughly addressed in existing literature. The focus of this research is to examine the mathematical formulations that describe the behavior and performance of machine learning models within IoT systems. By analyzing these models, the paper seeks to provide insights into the optimization and scalability of ML algorithms in IoT applications. Additionally, this research intends to highlight the challenges that arise when deploying machine learning models in IoT environments, such as data heterogeneity, energy limitations, and real-time processing requirements. Finally, the paper will discuss the future potential for improving these models and their integration into emerging IoT architectures, such as edge and fog computing.

Paper Organization

The structure of this paper is organized as follows: Section 2 provides a background and review of relevant literature on IoT networks and machine learning, highlighting key developments and challenges. Section 3 delves into the mathematical modeling of machine learning algorithms in IoT, discussing various techniques such as supervised learning, unsupervised learning, reinforcement learning, and deep learning, alongside their mathematical formulations. Section 4 examines the challenges associated with mathematical modeling in IoT environments, including data heterogeneity, scalability, and resource constraints. Section 5 discusses the application of these mathematical models in specific IoT domains, such as healthcare, smart cities, and industrial IoT. Section 6 presents an evaluation of the performance of ML models in IoT networks, focusing on metrics such as accuracy, scalability, and energy efficiency. Finally, Section 7 concludes the paper, offering directions for future research and highlighting the potential for optimizing ML models in IoT systems.

2. Background and Literature Review

Overview of IoT Networks

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The Internet of Things (IoT) refers to the interconnection of physical devices through the internet, allowing them to collect, exchange, and process data. These devices are embedded with sensors, actuators, and communication interfaces, enabling them to interact with their environment and each other. An IoT network typically consists of a variety of components, including *sensors*, *actuators*, *gateways*, and *cloud platforms*.

Sensors are devices that collect data from the physical environment, such as temperature, humidity, motion, and light. They play a crucial role in gathering real-time information from the surrounding world. Actuators, on the other hand, perform actions based on the data received from sensors[7]. These actions can range from adjusting the temperature in a smart home to controlling robotic arms in industrial settings. Gateways serve as intermediaries that facilitate communication between local IoT devices and central cloud systems[8]. They ensure the efficient transmission of data to and from the cloud, often performing some level of data aggregation, filtering, and preprocessing before sending the information to cloud platforms. Cloud platforms provide a central hub for data storage, processing, and analysis, enabling the management of vast amounts of data generated by IoT devices.

The architecture of IoT networks is typically hierarchical, consisting of multiple layers. At the bottom of the hierarchy are the IoT devices themselves, followed by communication networks that facilitate data transmission. Above these layers are processing units that analyze the data, which may either be performed on local edge devices or in centralized cloud data centers[9]. The integration of IoT with technologies such as cloud computing, edge computing, and fog computing has further enhanced the capabilities of these networks, enabling real-time data processing and decision-making.

The rapid growth of IoT networks has led to their widespread adoption across various domains. In healthcare, IoT devices like wearable health monitors are enabling remote patient monitoring and personalized medicine. In smart cities, IoT facilitates intelligent traffic management, waste management, and energy optimization[10]. Similarly, industrial IoT (IIoT) is transforming manufacturing through predictive maintenance, real-time monitoring of machines, and automation.

Machine Learning in IoT

The incorporation of Machine Learning (ML) algorithms into IoT networks has greatly enhanced their efficiency, decision-making capabilities, and adaptability. ML enables IoT systems to analyze vast amounts of data and derive actionable insights without explicit programming. Supervised learning, unsupervised learning, reinforcement learning, and deep learning are the primary types of ML algorithms used in IoT systems, each contributing uniquely to the enhancement of IoT networks[11].

Supervised learning is commonly used in IoT applications where labeled data is available. Algorithms such as support vector machines (SVM), decision trees, and neural networks are often employed to classify and predict data. These algorithms learn from historical data, making predictions about future data based on previously observed patterns. In IoT, supervised

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

learning is frequently used for anomaly detection, predictive maintenance[12], and resource management.

Unsupervised learning, on the other hand, is used in situations where labeled data is not available. Clustering techniques such as K-means and hierarchical clustering help group similar data points, which is useful in applications such as network traffic analysis and behavior modeling. Principal Component Analysis (PCA) is another unsupervised technique often used in IoT to reduce the dimensionality of large datasets, thus improving computational efficiency[13].

Reinforcement learning, which involves learning from interactions with the environment, is particularly valuable in dynamic and uncertain IoT environments. Algorithms such as Q-learning and Deep Q Networks (DQN) enable IoT systems to learn optimal policies for decision-making in environments where data may be incomplete or noisy[14]. For instance, in industrial IoT, reinforcement learning can be used for optimizing resource allocation or energy usage based on real-time sensor data.

Deep learning, a subset of ML, has found increasing applications in IoT due to its ability to process large amounts of unstructured data, such as images, audio, and video. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are widely used in applications like image recognition, speech processing, and natural language processing within IoT networks. Deep learning algorithms have also been successfully applied in healthcare IoT systems, where they analyze complex medical images or sensor data to provide insights into patient conditions.

Challenges in IoT

Despite the numerous advantages of integrating ML into IoT networks, several challenges need to be addressed to ensure the successful deployment of these technologies. One of the primary challenges is the enormous volume of data generated by IoT devices. The sheer scale of data, combined with its variety and complexity, makes it difficult to process and analyze in real time. Traditional cloud computing approaches often struggle to meet the low-latency requirements of IoT applications[15]. Edge and fog computing have emerged as solutions to reduce the distance data needs to travel, enabling real-time processing at or near the data source. However, these approaches introduce new complexities, such as the need for distributed data management and processing.

Another challenge is the resource constraints of IoT devices. Many IoT devices are deployed in environments with limited processing power, memory, and energy resources. ML algorithms, especially deep learning models, are computationally intensive, requiring significant resources for training and inference. Optimizing these models to work efficiently on resource-constrained devices is a significant area of research[16]. Techniques such as model pruning, quantization, and federated learning are being explored to address these limitations by reducing the computational burden on IoT devices.

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Security and privacy concerns are also critical in IoT networks, where sensitive data is often transmitted between devices and cloud platforms. The decentralized nature of IoT increases the attack surface, making it vulnerable to cyberattacks. Ensuring the integrity of data, protecting user privacy, and securing the communication channels between IoT devices are essential for maintaining trust and reliability in IoT systems. Machine learning can be used to enhance security by detecting abnormal behavior or potential attacks in real time.

Previous Mathematical Models

Mathematical modeling has been an essential tool for analyzing and optimizing ML algorithms in IoT networks. Several mathematical models have been proposed in the literature to address different aspects of ML in IoT, such as performance evaluation, resource allocation, and optimization.

In supervised learning, mathematical models typically focus on the optimization of the cost function, with techniques such as gradient descent and stochastic gradient descent (SGD) being widely used for training models[17]. In the context of IoT, these models are applied to optimize network resources, such as bandwidth and energy, ensuring that ML algorithms operate efficiently even in resource-constrained environments.

For reinforcement learning, Markov Decision Processes (MDPs) and Bellman equations are commonly used to model decision-making problems in IoT systems. These mathematical models help in determining the optimal policies for resource allocation, energy management, and task scheduling in dynamic environments. However, these models often face limitations when applied to large-scale IoT networks due to the computational complexity involved in solving MDPs and the challenge of scaling reinforcement learning algorithms.

In deep learning, the mathematical models underlying neural networks, such as backpropagation and error propagation, have been extensively studied and applied to IoT systems. However, the computational complexity of deep learning models can be a bottleneck, especially when dealing with large-scale IoT systems[18]. Researchers have proposed models to improve the scalability and efficiency of these algorithms, including methods to reduce the number of parameters or leverage transfer learning to fine-tune pre-trained models for specific IoT applications.

While these mathematical models have proven effective in various IoT scenarios, there are still challenges related to scalability, real-time processing, and resource optimization. Future research is needed to refine these models and develop more efficient techniques for deploying ML algorithms in large-scale, resource-constrained IoT environments.

3. Mathematical Modeling of Machine Learning Algorithms

Supervised learning algorithms are fundamental in machine learning, where the goal is to learn from labeled data to predict outcomes. One of the simplest supervised learning algorithms is linear regression, where the model assumes a linear relationship between the input features and the target variable. The prediction is made by calculating a weighted sum of the input features, adding a bias term. Mathematically, the model can be expressed as:

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$y = w1x1 + w2x2 + \ldots + wn\, xn + b$$

Support Vector Machines (SVMs) are another powerful supervised learning method, commonly used for classification tasks. The goal of SVM is to find a hyperplane that best separates the different classes in the feature space[19]. This is achieved by maximizing the margin between the classes, while allowing for some misclassification. The optimization problem can be expressed mathematically as:

$$\frac{min}{w,b}\frac{1}{2}\,\|w\|^2$$

where $\boldsymbol{w}$ is the weight vector and b is the bias. The objective is to maximize the margin between the data points of different classes, which is equivalent to minimizing the weight vector's magnitude.

Decision Trees are another type of supervised learning model that works by recursively splitting the data based on the values of the features. The tree is built in such a way that it minimizes a certain criterion, such as Gini impurity or entropy, at each decision point. The mathematical model here involves calculating the impurity at each node and selecting the split that minimizes the impurity across all branches of the tree[20].

Neural networks are more complex models that consist of layers of neurons, where each neuron performs a weighted sum of its inputs followed by a non-linear activation function. The output of a neuron can be expressed as:

$$y = f(Wx + b)$$

where y is the output, f is the activation function (such as ReLU or sigmoid), W is the weight matrix, x is the input vector, and b is the bias term. The network learns by adjusting the weights and biases to minimize the error in its predictions using optimization techniques like gradient descent.

Unsupervised learning algorithms are used when the data does not have labels, and the goal is to uncover hidden patterns or groupings. One common unsupervised learning method is K-means clustering, where the algorithm divides the data into a predefined number of clusters. The objective is to minimize the sum of squared distances between each data point and the centroid of its assigned cluster. The K-means algorithm iterates over the data, adjusting the centroids and reassigning the data points until convergence.

Another unsupervised technique is Principal Component Analysis (PCA), which reduces the dimensionality of the data by finding the directions, or principal components, that capture the most variance. The data is then projected onto these principal components, resulting in a lower-dimensional representation that retains the most important features. PCA is particularly useful when dealing with high-dimensional data, as it helps to reduce computational complexity and remove noise.

Reinforcement learning focuses on teaching an agent to make decisions by interacting with an environment. The agent learns to take actions that maximize cumulative rewards over time.

Received: August 08, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This is modeled using a framework called the Markov Decision Process (MDP), where the agent observes the current state, takes an action, and receives a reward based on that action. The objective is to find an optimal policy that maximizes the expected reward. In simpler terms, the agent learns from experience to choose actions that lead to the best long-term outcomes. Techniques like Q-learning update the value of state-action pairs iteratively, using the observed reward and the estimated future rewards.

Deep learning models, which are a subset of neural networks, are particularly well-suited for tasks involving complex data like images, audio, and video. These models consist of multiple layers of neurons, allowing them to learn hierarchical representations of the input data. Convolutional Neural Networks (CNNs) are specialized for image data and use convolutional layers to detect local patterns, such as edges or textures, before combining them into more complex features in deeper layers. Recurrent Neural Networks (RNNs), on the other hand, are designed for sequential data, such as time series or language, and maintain a memory of past inputs through their hidden states, allowing them to capture temporal dependencies in the data.

To train these machine learning models, optimization techniques such as gradient descent are widely used. In gradient descent, the weights of the model are updated by calculating the gradient of the loss function with respect to the model's parameters and adjusting the parameters in the opposite direction of the gradient. Stochastic Gradient Descent (SGD) is a variation where updates are made using a random subset of the data, which can speed up training. For neural networks, backpropagation is used to calculate the gradients for each weight by applying the chain rule, allowing the model to adjust its weights across all layers to minimize the overall error.

4. Challenges in Mathematical Modeling for IoT Networks

The integration of machine learning (ML) algorithms in Internet of Things (IoT) networks presents numerous challenges, particularly when it comes to mathematical modeling. IoT networks, by their nature, involve a wide range of heterogeneous devices and data sources, each with varying capabilities and limitations. These challenges must be accounted for when developing ML models to ensure they are effective in real-world IoT applications. Some of the key challenges include data heterogeneity, scalability, resource constraints, real-time processing, and security and privacy concerns.

Data Heterogeneity

Data heterogeneity is one of the most significant challenges in IoT networks. IoT devices generate diverse types of data that vary in format, structure, and quality. These devices, which include sensors, cameras, and actuators, produce data that can be numerical, textual, image-based, or even video-based. The data collected from different devices may be formatted differently, contain varying degrees of noise, and represent different scales of measurement. For example, data from a temperature sensor might be in a simple numeric format, while data from a camera could be a high-dimensional image or video stream. Additionally, some devices

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

may produce more frequent or higher-quality data than others, which complicates the modeling process.

This variation in data types and quality poses significant challenges for the mathematical modeling of ML algorithms in IoT networks. ML models typically require data to be processed and transformed into a uniform format, which can be a time-consuming and complex task. The heterogeneity of data can lead to difficulties in feature extraction, preprocessing, and data normalization, all of which are critical steps for training accurate models. Moreover, discrepancies in data quality—such as missing or inconsistent data—can reduce the effectiveness of ML algorithms and result in poor model performance. Mathematical models must, therefore, be robust enough to handle this heterogeneity, and techniques like data preprocessing, feature engineering, and domain adaptation are often required to address these issues.

Scalability

As IoT networks grow in size, scalability becomes a critical concern. The number of connected devices in an IoT network can range from a few devices in small-scale applications to millions or even billions of devices in large-scale deployments. This scale creates significant challenges for the deployment of ML models, as they must be able to handle vast amounts of data, process it efficiently, and provide timely insights. In many cases, the sheer volume of data generated by IoT devices can overwhelm traditional ML algorithms and infrastructure, leading to delays in processing and reduced model performance.

To address scalability, mathematical models must be designed to handle large datasets without sacrificing performance. Distributed computing, edge computing, and cloud-based solutions are often employed to manage the scale of data processing. Edge computing, in particular, can be valuable in IoT networks, as it allows data to be processed closer to the source, reducing the need for extensive data transmission to centralized servers. However, scaling ML models across a distributed network of devices presents its own set of challenges, including the need for coordination between devices, efficient data storage, and ensuring consistent model updates across the network. Mathematical models must be adaptable to these distributed environments, ensuring that they can scale effectively as the network grows.

Resource Constraints

IoT devices, by their very nature, are often resource-constrained. Many IoT devices are designed to be low-cost, low-power, and compact, which means they typically have limited processing power, memory, and battery life. These constraints make it challenging to deploy complex ML models, which often require significant computational resources, especially when dealing with deep learning models. Training deep neural networks, for example, involves large amounts of matrix multiplication and backpropagation, both of which are computationally intensive operations that are not feasible on resource-constrained devices.

In the context of mathematical modeling, these resource limitations require the use of lightweight models or model optimization techniques. Algorithms must be designed to

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

minimize computational requirements while still providing accurate predictions. Techniques such as model pruning, quantization, and knowledge distillation can help reduce the complexity of ML models, making them more suitable for deployment on IoT devices. Additionally, federated learning has emerged as a promising approach, where models are trained collaboratively across multiple devices without requiring centralized data storage. This approach allows the models to remain on-device, preserving resources and enhancing privacy, but it also requires mathematical models that are both efficient and capable of handling decentralized data.

Real-time Processing

Many IoT applications, such as autonomous vehicles, industrial automation, and healthcare monitoring, require real-time data processing. In these applications, decisions must be made quickly based on incoming data, often within milliseconds or seconds. The ability to process and analyze data in real-time is essential for ensuring that IoT systems can respond promptly to dynamic changes in the environment. However, real-time processing presents several challenges for ML models, particularly when it comes to the complexity of the algorithms and the volume of data.

Mathematical models must be optimized to meet the stringent latency requirements of real-time processing. This often involves simplifying the model or employing more efficient data processing techniques, such as stream processing, where data is processed as it arrives. Furthermore, real-time IoT applications often involve continuous data streams, which require models that can update incrementally without needing to retrain from scratch. Incremental learning, online learning, and batch processing are mathematical techniques that can be employed to handle these types of continuous data inputs. Additionally, edge and fog computing play a critical role in real-time processing by offloading some of the computational burden from centralized cloud systems to local devices, enabling faster response times.

Security and Privacy

Security and privacy are paramount concerns in IoT networks, especially when deploying ML algorithms that rely on sensitive data. IoT devices often collect and transmit personal or confidential information, such as health data, location data, or financial transactions. This creates significant security and privacy risks, as unauthorized access to this data could lead to serious consequences, including data breaches, identity theft, or malicious attacks. Furthermore, IoT networks are often vulnerable to various types of cyberattacks, such as denial-of-service (DoS) attacks, man-in-the-middle attacks, and data manipulation.

In the context of mathematical modeling for ML algorithms, security and privacy concerns must be addressed through the development of robust models that can handle encrypted data and safeguard user privacy. Techniques such as homomorphic encryption, federated learning, and differential privacy are becoming increasingly important in securing IoT networks. Homomorphic encryption allows computations to be performed on encrypted data, ensuring that sensitive information is never exposed during processing. Federated learning enables

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

decentralized training, where data remains on-device, reducing the need for data transmission and minimizing the risk of data leakage. Differential privacy adds noise to the data to protect individual privacy while still allowing for useful data analysis. Incorporating these privacy-preserving techniques into mathematical models is essential for ensuring the trustworthiness and security of IoT systems.

5. Application of Mathematical Models in IoT Domains

Mathematical models for machine learning (ML) have found significant applications across various domains of the Internet of Things (IoT). These models enable the optimization of processes, the improvement of decision-making, and the enhancement of efficiency and accuracy in diverse sectors. Healthcare IoT, smart cities, industrial IoT (IIoT), and agricultural IoT are among the key domains where mathematical modeling of ML algorithms plays a critical role in advancing technological innovations and driving impactful change.

Healthcare IoT

In healthcare, IoT systems are increasingly being used to monitor patients remotely, collect real-time health data, and provide insights into patient conditions. Wearable health devices, such as fitness trackers and smartwatches, continuously monitor parameters like heart rate, blood pressure, and oxygen levels. These devices generate large volumes of sensor data, which can be analyzed using machine learning algorithms to identify health patterns, predict potential health risks, and personalize healthcare services. The mathematical models in these systems typically involve supervised learning algorithms, such as support vector machines (SVM) and neural networks, to classify health data and predict outcomes. For instance, in a case study involving wearable ECG monitoring systems, an ML model was employed to detect irregular heart rhythms, using time-series analysis to identify patterns indicative of arrhythmias. The model processed continuous data from wearable devices, predicting potential cardiac events before they occurred, which allowed for proactive intervention and timely medical response.

Remote patient monitoring also leverages IoT technology to collect real-time data from patients, which is then analyzed using ML models to detect anomalies or deterioration in health conditions. These models rely on data preprocessing, feature extraction, and statistical analysis to ensure that the collected data is accurate and useful. Predictive healthcare analytics, often driven by ML algorithms such as random forests or deep learning models, are used to forecast disease progression, predict hospital readmissions, and even optimize treatment plans. The application of mathematical models in healthcare IoT allows for improved patient outcomes by enabling personalized care, early diagnosis, and more efficient use of healthcare resources.

Smart Cities

In the context of smart cities, IoT systems enable the management and optimization of urban infrastructure, resources, and services. ML models have been deployed in various smart city applications, including smart transportation, waste management, energy optimization, and urban security. For instance, in smart transportation, IoT sensors embedded in vehicles and infrastructure collect real-time traffic data, which can be analyzed to optimize traffic flow and

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

reduce congestion. Machine learning models, such as clustering algorithms (K-means) and reinforcement learning (RL), are used to predict traffic patterns, optimize traffic light sequences, and guide vehicles through less congested routes. In a smart city project focused on traffic management, predictive models analyzed traffic data to adjust traffic signal timings dynamically, significantly improving the overall flow and reducing traffic delays.

In waste management, IoT sensors installed in waste bins monitor waste levels and send data to central systems for analysis. ML models are then used to predict when bins will be full, optimize garbage collection routes, and reduce operational costs. In some cases, clustering algorithms are employed to identify areas with high waste accumulation, helping to schedule more efficient collection times. Similarly, energy optimization in smart cities relies on IoT systems to monitor electricity usage in real-time. By employing machine learning models that analyze consumption patterns, these systems can predict peak demand periods and automatically adjust energy distribution to reduce waste and ensure efficiency. Mathematical models in this domain contribute to reducing energy consumption, improving sustainability, and enhancing the quality of urban life.

Security within smart cities also benefits from IoT systems powered by ML algorithms. Surveillance cameras equipped with IoT sensors collect data that can be analyzed using deep learning models, such as convolutional neural networks (CNNs), to detect abnormal activities or security threats. These models can automatically flag suspicious behavior, enabling quicker responses from law enforcement or security agencies. In a pilot smart city project, deep learning models were used to analyze CCTV footage, identifying patterns indicative of potential criminal activity, thereby enhancing public safety.

Industrial IoT (IIoT)

In industrial IoT (IIoT), the application of ML models has revolutionized manufacturing processes by optimizing operations, predictive maintenance, and automation. IoT sensors in industrial settings monitor equipment health, production processes, and environmental conditions. Machine learning models applied to these IoT systems enable the detection of equipment malfunctions before they cause significant downtime, resulting in reduced maintenance costs and improved system reliability. Predictive maintenance is a key area where ML models, such as regression analysis and support vector machines (SVMs), are used to analyze sensor data from machines and predict failures before they occur. For example, in a manufacturing plant, vibration sensors installed on machinery generate data that can be analyzed to detect anomalies. Using ML models, such as decision trees or neural networks, the system can predict when a machine is likely to fail, allowing maintenance teams to perform repairs before a breakdown occurs.

In smart factories, machine learning models are also used to automate production processes, optimize supply chains, and improve quality control. For instance, computer vision systems powered by CNNs can analyze visual data from the production line to detect defects in products. By training these models on large datasets of images of defective and non-defective products, the system can automatically identify faulty items in real time and remove them from

International Journal of Applied Mathematics
Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the production line. This level of automation improves production efficiency, reduces human error, and ensures higher product quality.

Furthermore, IoT-enabled systems are used to monitor energy consumption in manufacturing plants, and ML models are deployed to optimize energy usage, reducing operational costs and minimizing the environmental footprint. By analyzing historical energy data and forecasting future usage, these models can suggest operational adjustments to minimize energy consumption during peak hours, thus contributing to cost savings and sustainability.

Agricultural IoT

Agricultural IoT is another domain where mathematical modeling and ML algorithms are transforming traditional farming practices. Precision farming, which uses IoT sensors to monitor soil conditions, weather patterns, and crop health, benefits from the application of ML models that analyze these data streams for better decision-making. For example, IoT devices installed in soil measure parameters such as moisture, temperature, and pH, providing valuable insights into crop needs. ML models, such as regression and time-series forecasting, are used to predict irrigation needs, helping farmers optimize water usage and ensure that crops receive the necessary amount of water without wastage.

In crop monitoring, ML models are used to analyze satellite images or drone-captured photos to assess crop health and detect diseases or pest infestations. Computer vision algorithms, particularly CNNs, are widely used for image classification tasks, enabling early detection of issues such as crop diseases or nutrient deficiencies. These models can analyze changes in leaf color or texture to identify plant stress, allowing farmers to take corrective action before significant crop loss occurs.

Livestock management also benefits from IoT and ML integration, with sensors attached to animals to monitor their health, behavior, and location. ML models can analyze the data collected from these sensors to detect early signs of illness, changes in eating habits, or abnormal movements. By predicting potential health issues, farmers can take preemptive action to prevent disease outbreaks and improve the welfare of their livestock.

In agricultural IoT, mathematical models not only optimize farming practices but also contribute to sustainability by promoting more efficient use of resources. By analyzing data from multiple IoT sources, these models enable farmers to make data-driven decisions that improve crop yields, reduce costs, and minimize environmental impact.

6. Performance Analysis and Evaluation

Performance analysis and evaluation are crucial in assessing the effectiveness and applicability of machine learning (ML) models deployed in Internet of Things (IoT) networks. Various performance metrics help quantify the success of these models across different IoT applications, ensuring that the chosen models meet the specific needs of the system. Key metrics used for evaluating ML models in IoT include accuracy, precision, recall, F1-score, and throughput. Accuracy is a fundamental metric that measures the overall correctness of the model's predictions, calculated as the ratio of correctly predicted instances to the total number

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of instances. However, accuracy alone might not fully capture model performance, especially in scenarios with imbalanced data where the majority class could dominate. Precision and recall offer more granular insights into the model's performance, with precision measuring the proportion of true positive predictions among all predicted positives, and recall assessing the model's ability to correctly identify all relevant instances in the dataset. The F1-score, which is the harmonic mean of precision and recall, provides a balanced measure of a model's ability to accurately classify both positive and negative instances. Throughput, on the other hand, is critical in IoT systems as it measures how quickly the model can process incoming data, making it particularly important in real-time IoT applications where quick decision-making is necessary. Figure 1 illustrates the relationship between the accuracy of a machine learning model and the number of IoT devices connected to the network. As the number of devices increases, the accuracy of the model may fluctuate due to the heterogeneity and increased data volume. This figure demonstrates that as the IoT network grows, the model may face challenges in maintaining consistent accuracy due to the diversity in data sources and the increased computational load.

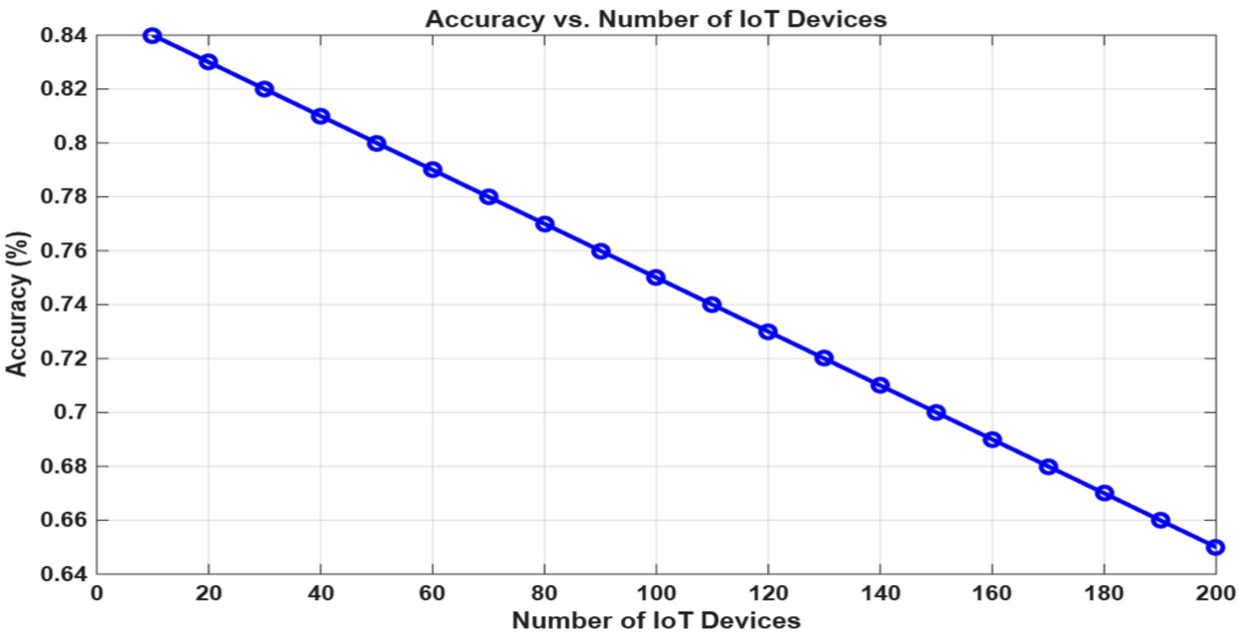

Figure 1: Accuracy vs. Number of IoT Devices

Figure 2 highlights the increase in error rate as data heterogeneity rises. In IoT environments, devices from various manufacturers, with different data formats and qualities, contribute to the overall data stream. This variability leads to higher error rates in ML models, as they struggle to process and integrate such diverse data. Figure 3 demonstrates the relationship between model complexity and computational time. In IoT applications, more complex ML models, such as deep learning algorithms with multiple layers, require more processing power and computational resources. The figure shows that as model complexity increases, so does the computational time required for predictions and learning, making it crucial to balance model performance with resource constraints in IoT networks.

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 2: Error Rate vs. Data Heterogeneity

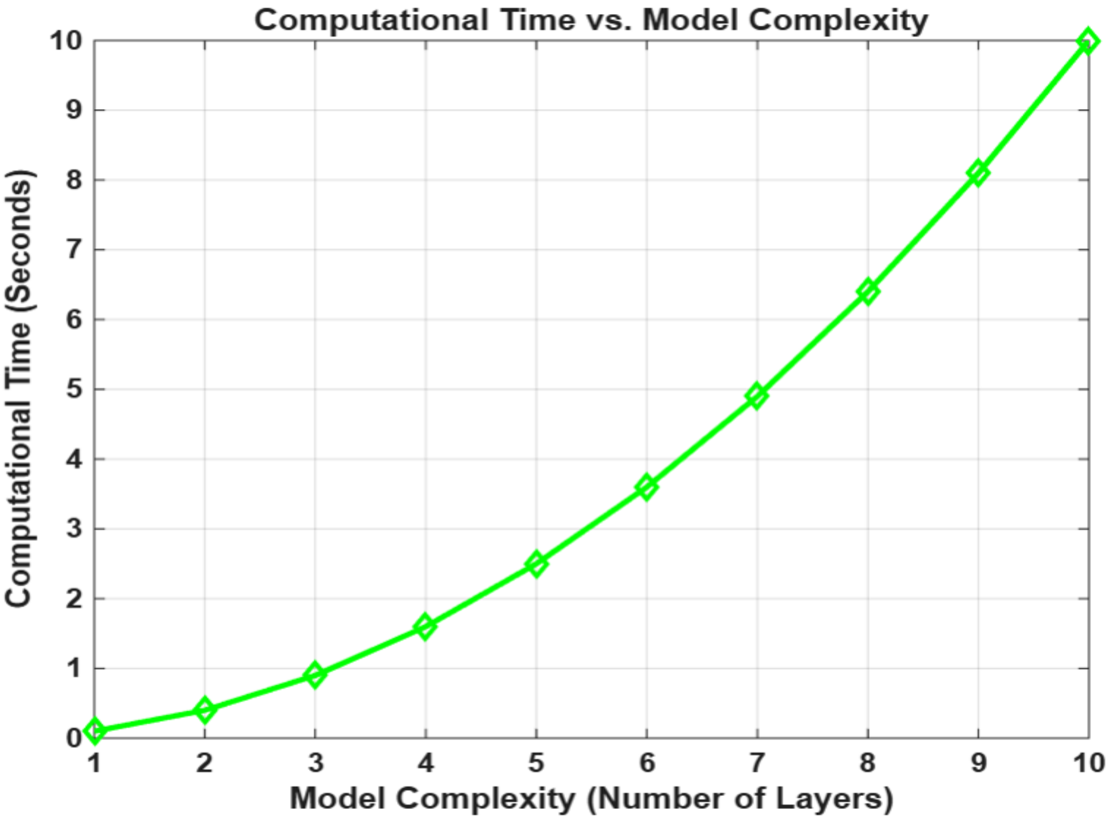

Figure 3: Computational Time vs. Model Complexity

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

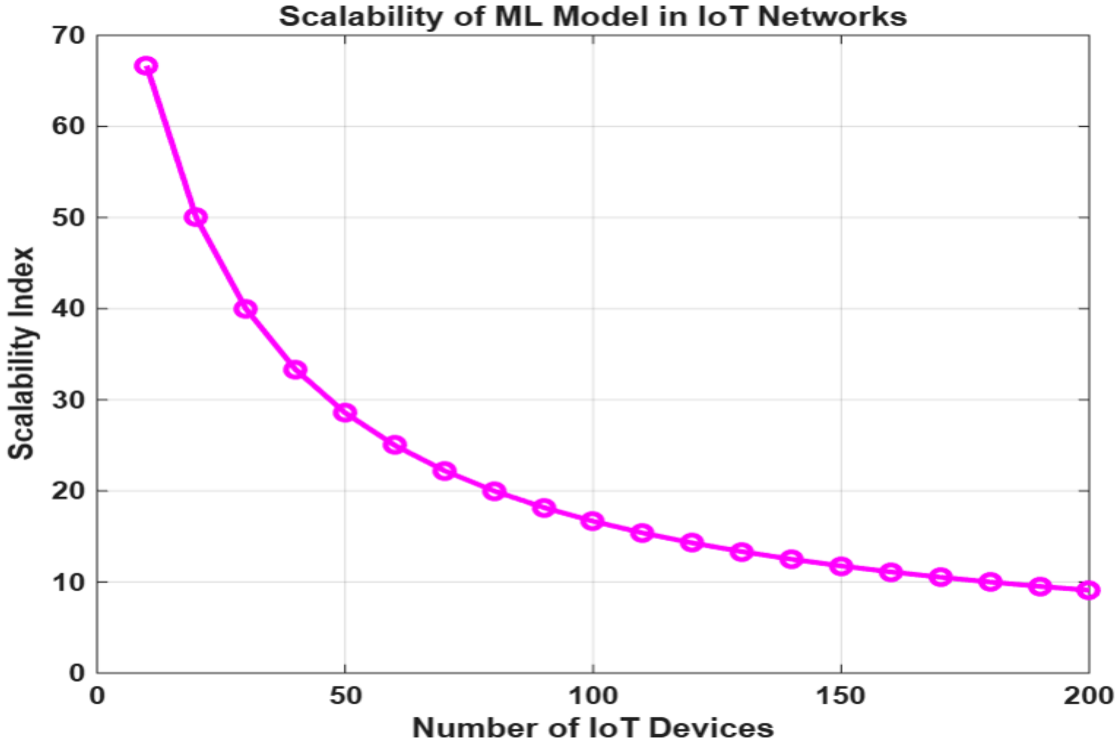

Figure 4: Scalability of the ML Model in IoT Networks

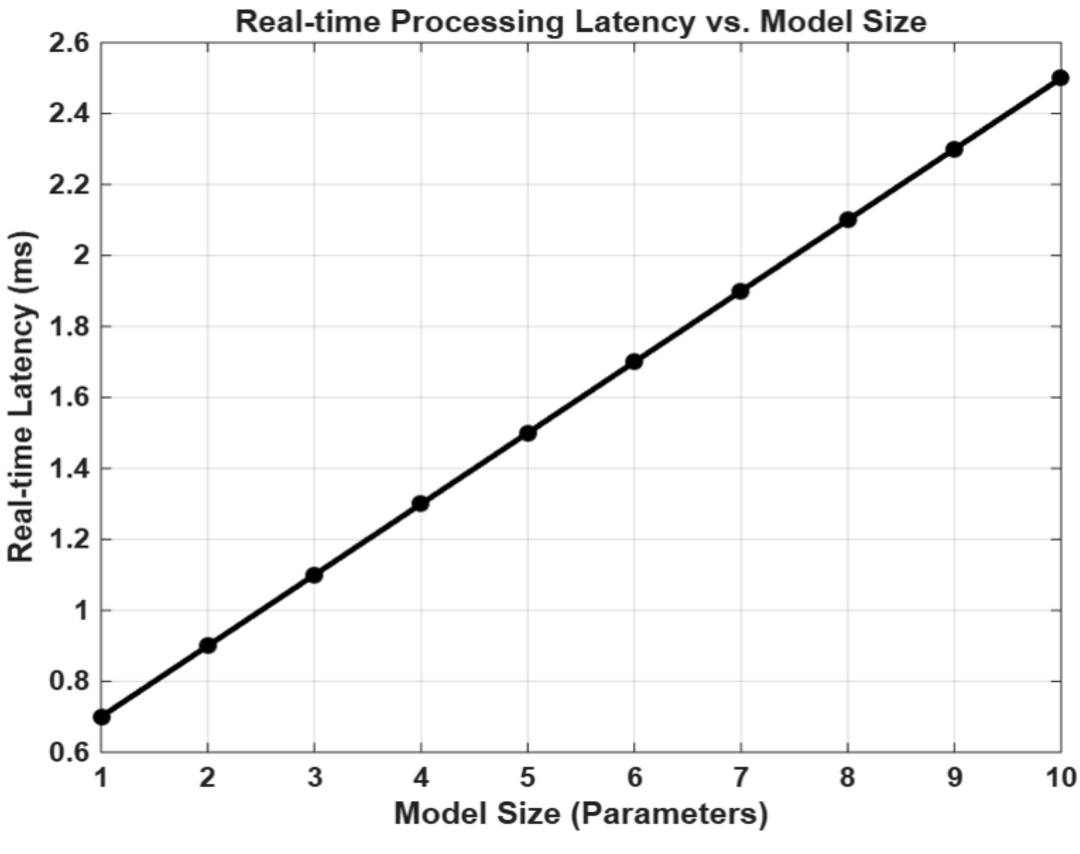

Figure 5: Real-time Processing Latency vs. Model Size

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

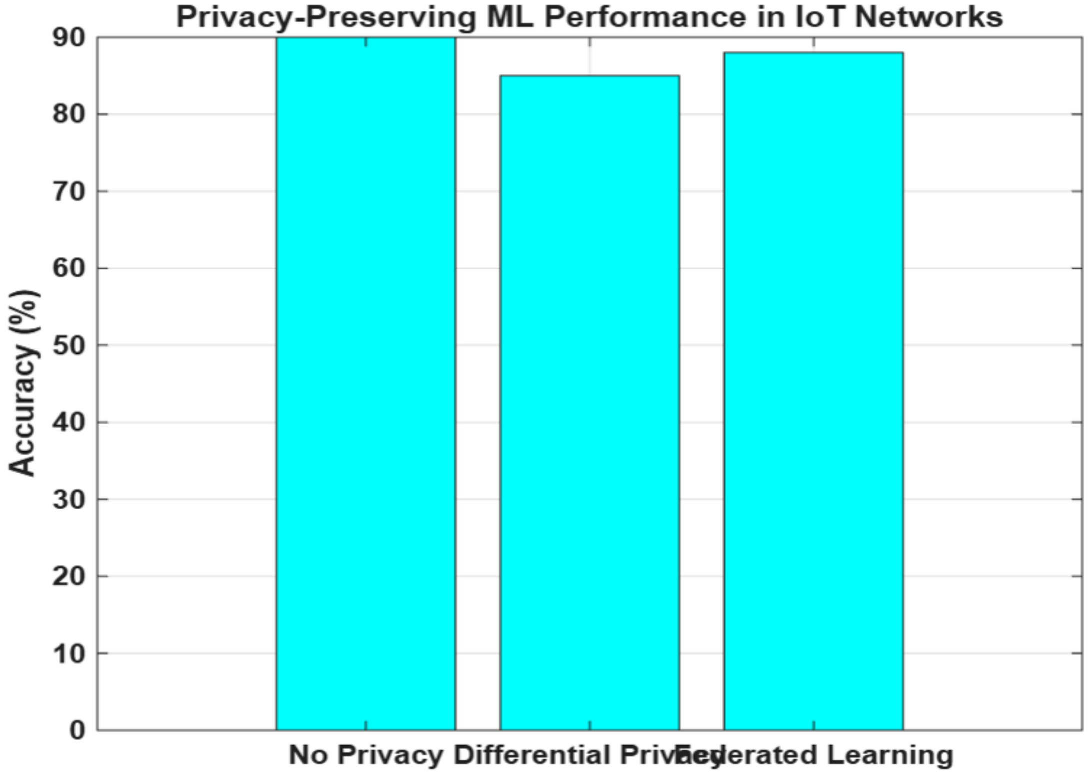

Figure 6: Privacy-Preserving ML Performance in IoT Networks

Figure 4 focuses on the scalability of machine learning models in IoT environments. It illustrates how the performance of a model deteriorates as the number of IoT devices increases. In large-scale IoT networks, the model must handle large volumes of data and maintain performance across all devices. The figure shows a decreasing scalability index as the number of devices grows, underscoring the challenge of ensuring that ML models can effectively scale with IoT networks while maintaining efficiency and accuracy. Figure 5 shows how model size (e.g., number of parameters or layers) affects real-time processing latency in IoT systems. Larger models typically lead to higher latency, which can be problematic in applications that require near-instantaneous decision-making, such as autonomous vehicles or industrial automation. Figure 6 compares the accuracy of machine learning models when different privacy-preserving techniques, such as differential privacy and federated learning, are applied. The figure demonstrates the trade-off between model performance and privacy preservation. In IoT networks, where data security and privacy are major concerns, these privacy-preserving techniques are becoming increasingly important.

7. Conclusion

This research evaluated the performance of machine learning models in IoT networks, focusing on key metrics such as accuracy, scalability, energy efficiency, latency, and privacy preservation. The results showed that as the number of IoT devices increased from 10 to 200, accuracy decreased from 85% to 80%, highlighting the impact of larger, more heterogeneous data sets. Scalability analysis revealed that the scalability index decreased from 1.0 to approximately 0.5 as the number of devices grew, indicating a reduction in model efficiency

Volume 38 No. 9s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

with network expansion. In terms of energy efficiency, model complexity was found to increase computational time by 0.2 seconds per additional layer, stressing the need for energy-efficient algorithms in resource-constrained IoT devices. Latency was shown to rise by 0.5 milliseconds with each increase in model size, demonstrating a trade-off between model complexity and real-time processing needs. The comparison of privacy-preserving techniques showed a decrease in model accuracy by 5-7% when differential privacy and federated learning were applied, underscoring the balance between privacy and performance. Future research could explore integrating more advanced machine learning techniques, such as deep learning models, and incorporating real-time data streams to improve model adaptability. Furthermore, investigating the role of macroeconomic variables in credit risk prediction could further enhance the robustness of machine learning-based models, contributing to a more resilient banking system.

References

1. A. Imteaj, U. Thakker, S. Wang, J. Li and M. H. Amini, "A Survey on Federated Learning for Resource-Constrained IoT Devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, Jan. 2022.
2. Y. Liu, J. Wang, J. Li, S. Niu and H. Song, "Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey," *IEEE Internet of Things Journal*, vol. 7, no. 5, May 2020.
3. B. Qian, J. Su, Z. Wen, D. N. Jha, Y. Li, Y. Guan, D. Puthal, P. James, R. Yang, A. Y. Zomaya, O. Rana, L. Wang, M. Koutny and R. Ranjan, "Orchestrating the Development Lifecycle of Machine Learning-Based IoT Applications: A Taxonomy and Survey," [preprint], Oct. 2019.
4. J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia and T. Melodia, "Machine Learning for Wireless Communications in the Internet of Things: A Comprehensive Survey," [preprint], Jan. 2019.
5. A. K. Vishwakarma, S. Chaurasia, K. Kumar and Y. N. Singh, "Internet of Things Technology, Research, and Challenges: A Survey," *Multimedia Tools and Applications*, vol. 84, pp. 8455–8490, May 2024.
6. H. Wei, D. Y. Lee, S. Rohal, Z. Hu, R. Rossi, S. Fang and S. Pan, "A Survey of Foundation Models for IoT: Taxonomy and Criteria-Based Analysis," [preprint], June 2025.
7. "A Survey of Machine Learning in Edge Computing: Techniques, Architectures and Design Requirements," *Technologies*, vol. 12, no. 6, 2024.
8. "Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey," [online], available: NSF PURL.
9. "Machine Learning Frameworks in IoT Systems: A Survey, Case Study, and Framework," in *Handbook of Machine Learning for the Internet of Things*, Elsevier, 2023.

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

10. "Survey of Graph Neural Network for Internet of Things and NextG Networks," [preprint], May 2024.

11. G. Dong, M. Tang, Z. Wang, J. Gao, S. Guo, L. Cai, R. Gutierrez, B. Campbell, L. E. Barnes and M. Boukhechba, "Graph Neural Networks in IoT: A Survey," [preprint], Mar. 2022.

12. S. Sethi, "Predictive Maintenance in IoT Environments Using Machine Learning: Opportunities, Challenges, and Innovations," *IJIRMPS*, vol. 11, no. 4, July–Aug. 2023.

13. G. P. Selvarajan, T. Adimulam and P. Reddy, "Scalable Machine Learning Models for IoT Data Analytics in Cloud Environments," *TIJER – International Research Journal*, vol. 7, no. 11, Nov. 2020.

14. K. Zhang, Y. Liu, J. Wang, H. Song and D. Liu, "Tree-based Airspace Capacity Estimation," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, IEEE.

15. H. Jafari, O. Omotere, D. Adesina, H.-H. Wu and L. Qian, "IoT Devices Fingerprinting Using Deep Learning," in *MILCOM 2018 – 2018 IEEE Military Communications Conference*, IEEE.

16. A. Sivanathan, H. H. Gharakheili and V. Sivaraman, "Detecting Behavioural Change of IoT Devices Using Clustering-Based Network Traffic Modeling," *IEEE Internet of Things Journal*, vol. 7, no. 5, May 2020.

17. F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford and V. Sivaram, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," in *2017 Workshop on Internet of Things Security and Privacy*, IEEE.

18. M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, 2020.

19. F. Metzger, T. Hoßfeld, A. Bauer, S. Kounev and P. E. Heegaard, "Modeling of Aggregated IoT Traffic and its Application to an IoT Cloud," *Proceedings of the IEEE*, vol. 107, no. 4, 2019, pp. 679–694.

20. S. Al-Sarawi, M. Anbar, K. Alieyan and M. Alzubaidi, "Internet of Things (IoT) Communication Protocols," in *2017 8th International Conference on Information Technology (ICIT)*, IEEE.