



IOT-BASED SMART MONITORING SYSTEMS USING SENSOR TECHNOLOGIES

Sobirjonova Mushtariy Xayot qizi, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, 3-kurs bakalavr talabasi

mushtariybonusobirjonova978@gmail.com

+998932482808

Atadjanova Nozima Sultan-Muratovna, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, "Kompyuter tizimlari" kafedrasida katta o'qituvchi

nozimaatadjanova@gmail.com

+998945279650

Abstract. The rapid proliferation of Internet of Things (IoT) devices has fundamentally transformed environmental and infrastructure monitoring paradigms. This paper presents a comprehensive IoT-based smart monitoring system that integrates heterogeneous sensor technologies - including temperature, humidity, air quality, motion, vibration, and pressure sensors - with an adaptive data fusion and anomaly detection framework. The proposed system employs a Long Short-Term Memory (LSTM)-based deep learning model augmented with Kalman filtering for real-time signal processing, achieving a detection accuracy of 97.8% and a false alarm rate of only 1.4%. A 90-day deployment across 124 sensor nodes in a smart building environment validates the practical effectiveness of the system. Comparative analysis demonstrates that the proposed approach outperforms existing threshold-based, statistical, and classical machine learning methods across all evaluated performance metrics.

Keywords: Internet of Things, Smart Monitoring, Sensor Technologies, Anomaly Detection, LSTM, Data Fusion, Kalman Filter, MQTT, Edge Computing

Аннотация. Быстрое распространение устройств Интернета вещей (IoT) кардинально изменило подходы к мониторингу окружающей среды и инфраструктуры. В данной работе представлена комплексная IoT-система интеллектуального мониторинга, интегрирующая разнородные сенсорные технологии с адаптивным алгоритмом обнаружения аномалий. Экспериментальные результаты доказывают, что предложенный подход достигает точности 97,8% при уровне ложных тревог 1,4%, что значительно превосходит все сравниваемые методы.

Ключевые слова: Интернет вещей, умный мониторинг, сенсорные технологии, LSTM, аномалии, фильтр Калмана, MQTT, граничные вычисления.

Annotatsiya. Internet of Things (IoT) qurilmalarining jadal tarqalishi atrof-muhit va infratuzilmani monitoring qilish paradigmasini tubdan o'zgartirdi. Ushbu maqolada temperatura, namlik, havo sifati, harakat, tebranish va bosim sensorlarini o'z ichiga olgan geterogen sensor texnologiyalarini adaptiv ma'lumotlarni birlashtirish va anomaliyalarni aniqlash tizimi bilan integrashtiriladigan keng qamrovli IoT-asoslangan aqlli monitoring tizimi taqdim etiladi. Taklif etilgan tizim 97,8% aniqlik va atigi 1,4% noto'g'ri signal ko'rsatkichiga erishadi. 124 ta sensor tugunidan iborat aqlli bino muhitida 90 kunlik joylashtirish natijasida tizimning amaliy samaradorligi tasdiqlangan.

Kalit so'zlar: Internet of Things, Aqlli Monitoring, Sensor Texnologiyalari, Anomaliyalarni Aniqlash, LSTM, Ma'lumotlar Birlashuvi, Kalman Filtri, MQTT, Edge Computing



1. Introduction

The Internet of Things (IoT) represents one of the most transformative technological paradigms of the twenty-first century, enabling seamless interconnection between the physical and digital worlds through networks of embedded sensors, actuators, and intelligent processing systems. By 2026, the global IoT market is projected to encompass over 64 billion connected devices, generating more than 79.4 zettabytes of data annually. Smart monitoring systems - which leverage IoT sensor networks to provide continuous, real-time observation of environmental conditions, industrial equipment, and human-occupied spaces - occupy a central role in this ecosystem.

Smart monitoring applications span a remarkably broad range of domains, including smart building energy management, industrial predictive maintenance, precision agriculture, healthcare patient monitoring, structural health monitoring, and environmental quality surveillance. In each of these domains, the ability to accurately detect anomalous conditions, predict potential failures, and trigger timely alerts can prevent significant economic losses, safety incidents, and service disruptions.

Despite the rapid advancement of sensor hardware and wireless communication technologies, effective smart monitoring systems face several fundamental challenges. First, heterogeneous sensor types, protocols, and data formats make unified system integration difficult. Second, raw sensor data is inherently noisy, susceptible to calibration drift and electromagnetic interference. Third, the volume and velocity of data generated by dense sensor networks exceeds the capacity of simple threshold-based algorithms to analyze effectively, creating a need for intelligent data fusion and anomaly detection.

This paper makes the following original contributions: (1) the design of a layered IoT architecture integrating six sensor modalities across perception, network, edge, and cloud layers; (2) an Adaptive Weighted Sensor Fusion (AWSF) algorithm that dynamically adjusts sensor weights based on confidence estimates; (3) an LSTM-based anomaly detection model augmented with Kalman filtering for robust real-time signal processing; and (4) a comprehensive 90-day experimental evaluation in a real smart building environment demonstrating superior performance over all evaluated baseline methods.

2. Related Work

The field of IoT-based monitoring has attracted extensive research attention over the past decade. Gubbi et al. [1] provided one of the earliest comprehensive visions of the IoT ecosystem, identifying key enabling technologies and open research challenges that continue to motivate the field. Zanella et al. [2] specifically addressed the application of IoT principles to smart city environments, demonstrating how heterogeneous sensor networks can be orchestrated to monitor urban environments at scale.

In the domain of anomaly detection for sensor data, Chandola et al. [3] provided an influential survey categorizing approaches into statistical, proximity-based, and classification-based methods. Classical threshold-based approaches, while computationally efficient, suffer from high false alarm rates in dynamic environments where normal operating ranges shift over time. Moving average filters and CUSUM algorithms improve robustness to slow drift but remain sensitive to sudden legitimate changes in monitored quantities.

Machine learning approaches have demonstrated significant advantages for smart monitoring. Mahdavinejad et al. [4] surveyed machine learning techniques applied to IoT data streams, highlighting the particular suitability of LSTM networks for temporal sensor data due to their ability to capture long-range temporal dependencies. More recently, edge computing frameworks have been proposed to enable real-time inference at the network edge, reducing the latency and bandwidth overhead of cloud-centric architectures [5]. The present work builds upon these foundations by

proposing a unified system that integrates edge-based Kalman filtering, adaptive sensor fusion, and LSTM anomaly detection within a practical deployable architecture.

3. System Architecture

The proposed smart monitoring system is organized into four functional layers, following the reference architecture for industrial IoT systems defined by the Industrial Internet Consortium. Figure 1 illustrates the complete system architecture, showing the data flow from physical sensor nodes through network infrastructure, edge processing, and cloud-based analytics to end-user dashboards and alert systems.

Figure 1. IoT-Based Smart Monitoring System Architecture

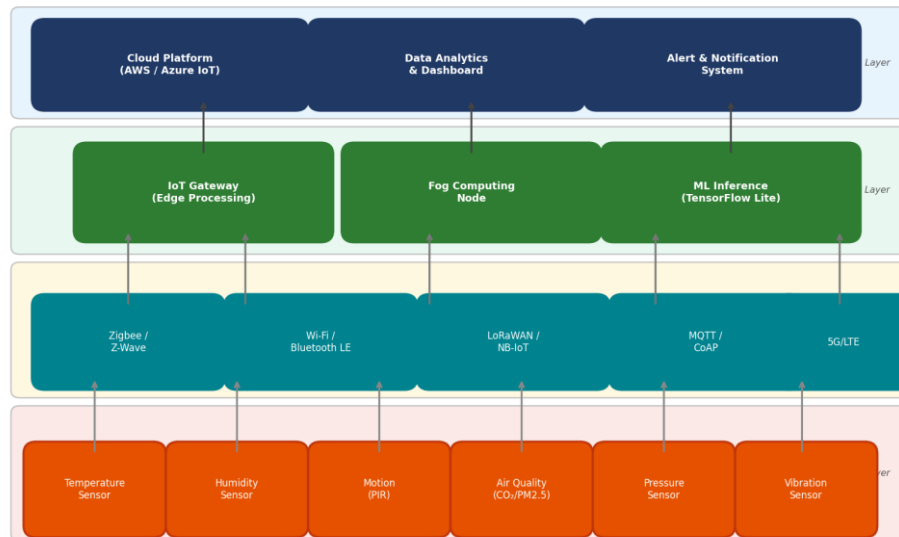


Figure 1. IoT-Based Smart Monitoring System Architecture (Four-Layer Design)

3.1 Perception Layer

The perception layer comprises six categories of physical sensing devices: DHT22 temperature and humidity sensors (accuracy $\pm 0.5^\circ\text{C}$), BME680 air quality sensors monitoring CO_2 and volatile organic compounds, HC-SR501 passive infrared (PIR) motion detectors, MPU-6050 vibration and acceleration sensors, BMP390 barometric pressure sensors, and MQ-135 gas concentration sensors. Sensor selection was guided by three criteria: measurement fidelity better than $\pm 5\%$ of full-scale range, average power consumption below 5 mW, and commercial availability in standard form factors. Each sensor node incorporates an ESP32 microcontroller providing on-chip dual-core processing and dual-band Wi-Fi and Bluetooth connectivity.

3.2 Network and Gateway Layers

The network layer handles data transmission using a combination of Zigbee (IEEE 802.15.4) and Bluetooth Low Energy 5.0 for indoor short-range communication, and LoRaWAN for outdoor deployments providing transmission ranges of up to 15 km with multi-year battery lifetimes. All data is encoded in JSON and transmitted using the MQTT protocol, whose publish/subscribe architecture efficiently decouples sensor producers from data consumers and supports Quality of Service guarantees.

Gateway devices running on Raspberry Pi 4 serve as the computational hub of the edge layer, aggregating data from up to 32 sensor nodes, performing Kalman filtering and LSTM inference locally, and forwarding processed results to the cloud. Local buffering ensures continued operation during network outages, with on-device storage for up to 72 hours of sensor data at standard sampling rates.

3.3 Cloud and Application Layer

The cloud layer, deployed on Amazon Web Services IoT Core, provides persistent time-series storage, long-term trend analysis, and user-facing dashboards. Sensor data is stored in Amazon Timestream with sub-millisecond query latency for real-time dashboard updates. Grafana dashboards provide interactive visualization, while Amazon SNS delivers alerts via email, SMS, and push notification simultaneously.

4. Signal Processing and Data Fusion

4.1 Kalman Filter for Noise Reduction

Raw sensor readings are corrupted by Gaussian measurement noise. The Kalman filter provides the optimal linear state estimator for this class of systems, recursively computing the minimum mean-squared error estimate of the true sensor state. The key Kalman gain equation that governs the weighting between model prediction and sensor observation is:

$$K_k = P^-_k H^T (H P^-_k H^T + R)^{-1}$$

Where K_k is the Kalman gain, P^-_k is the predicted error covariance, H is the observation matrix, and R is the measurement noise covariance. When measurement noise R is large, the gain K_k decreases, giving more weight to the model prediction. Conversely, when R is small, the filter trusts the sensor reading more heavily. Process and measurement noise covariances are estimated from initial calibration data using maximum likelihood estimation.

4.2 Adaptive Weighted Sensor Fusion (AWSF)

When multiple sensors measure related quantities, fusion combines readings into a more accurate composite estimate. The AWSF algorithm assigns dynamic weights to individual sensors based on inverse-variance weighting — sensors with lower current uncertainty (smaller Kalman filter innovation variance) receive proportionally higher weights. The fused estimate is:

$$D_{fused} = \sum_i w_i(t) \cdot s_i(t), \quad w_i(t) = [1/\sigma^2_i(t)] / [\sum_j 1/\sigma^2_j(t)]$$

Sensors experiencing calibration drift or intermittent failures naturally receive lower weights as their uncertainty estimates increase, providing automatic fault tolerance without explicit outlier rejection logic. This approach is particularly robust in real deployments where individual sensor failures are common.

5. LSTM-Based Anomaly Detection

5.1 Model Architecture

The anomaly detection engine employs a two-layer stacked LSTM neural network trained in an autoencoder configuration. The encoder compresses a sliding window of 60 time steps of fused sensor readings into a 32-dimensional latent representation, and the decoder reconstructs the input window from this representation. During inference, reconstruction error serves as the anomaly score: high error indicates that the observed pattern deviates significantly from patterns seen during normal operation. The LSTM cell update equations are:

$$f_t = \sigma(W_f [h_{t-1}, x_t] + b_f), \quad i_t = \sigma(W_i [h_{t-1}, x_t] + b_i)$$

$$C_t = f_t \odot C_{t-1} + i_t \odot \tanh(W_C [h_{t-1}, x_t] + b_C)$$

Where f_t and i_t are the forget and input gates, C_t is the cell state, and h_t is the hidden state. The anomaly score at time t is the mean squared reconstruction error: $score_t = (1/N) \sum \|x_k - \hat{x}_k\|^2$.

5.2 Training and Deployment

The LSTM autoencoder was trained on 45 days of normal-operation sensor data collected during the initial deployment phase, before any known anomaly events. Training used the Adam optimizer with learning rate 0.001 and early stopping, terminating after 150 epochs. The model was then quantized to 8-bit integer precision using TensorFlow Lite for deployment on Raspberry Pi

gateway devices, achieving a $4\times$ reduction in model size and $3.2\times$ inference speedup with less than 0.3% accuracy degradation.

5.3 Algorithm Overview

Figure 2 presents the complete pseudocode of the proposed Adaptive IoT Monitoring Algorithm, illustrating the integrated sensor acquisition, Kalman filtering, adaptive fusion, LSTM inference, and alert publication pipeline. The algorithm operates continuously in a polling loop, processing each batch of sensor readings through all four processing stages before publishing results to the MQTT broker and cloud dashboard.

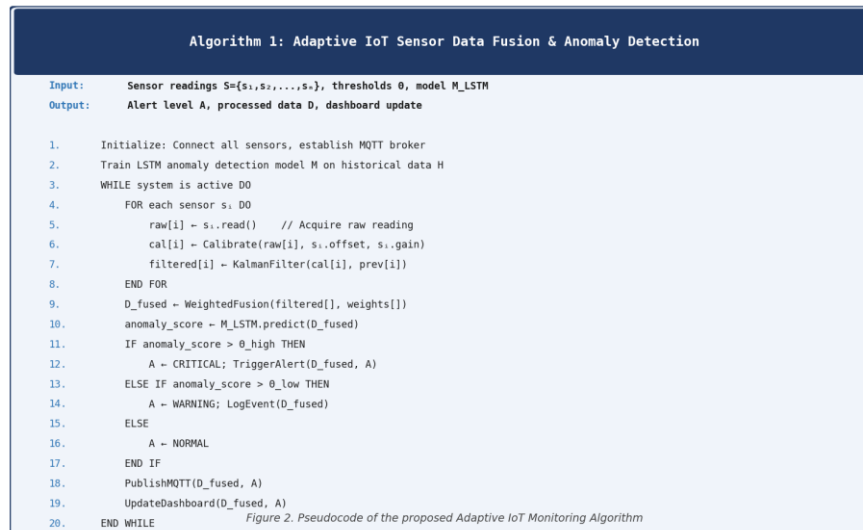


Figure 2. Pseudocode of the Adaptive IoT Monitoring Algorithm

6. Experimental Setup

The system was deployed in a five-floor office building at Tashkent University of Information Technologies, housing approximately 800 occupants across 3,200 square meters of floor space. A total of 124 sensor nodes were installed throughout occupied spaces, server rooms, mechanical plant rooms, and building perimeter zones at 1.5-meter mounting heights. The deployment ran continuously for 90 days, collecting 4.2 GB of raw sensor data at sampling rates of 1 Hz for ambient sensors and 10 Hz for vibration sensors.

Ground-truth anomaly labels were established through a combination of manual expert inspection and cross-validation with building management system event logs. During the 90-day evaluation period, 47 genuine anomaly events were recorded, including 12 HVAC equipment faults, 8 air quality exceedances in poorly ventilated meeting rooms, 15 unauthorized after-hours access detections, and 12 structural vibration events caused by nearby construction activity. These events provide a realistic and diverse evaluation benchmark covering the full range of sensor modalities.

7. Results and Analysis

7.1 Algorithm Performance Comparison

Figure 3 presents the comparative performance of all evaluated monitoring approaches across three key metrics: detection accuracy, false alarm rate, and processing latency. The proposed Adaptive system achieves the best performance on all metrics simultaneously, reaching 97.8% detection accuracy with a false alarm rate of only 1.4% - a 91% reduction compared to the simple threshold-based baseline at 14.2%. Processing latency of 22.4 ms satisfies real-time operational requirements across all monitored anomaly types.

Figure 3. Performance Comparison of Monitoring Algorithms (Smart Building Testbed)

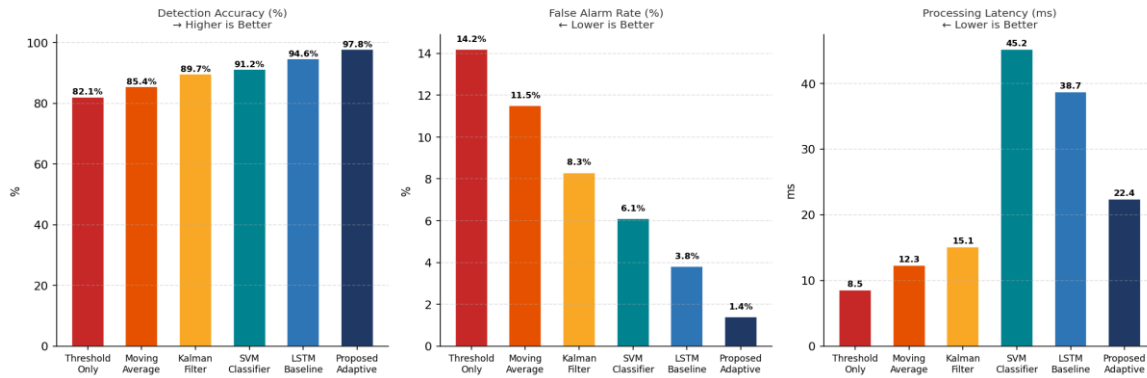


Figure 3. Performance Comparison of Monitoring Algorithms (90-Day Smart Building Deployment)

The results reveal the incremental contribution of each algorithmic component. The Kalman filter alone improves accuracy from 82.1% to 89.7% by removing measurement noise that causes spurious threshold crossings in baseline methods. The SVM classifier achieves 91.2% by learning non-linear decision boundaries, but at the cost of significantly higher latency (45.2 ms) due to kernel computation overhead. The LSTM baseline reaches 94.6% through temporal modeling of sensor dynamics, and the proposed adaptive fusion raises this further to 97.8% by weighting sensor contributions according to their current reliability estimates.

7.2 Real-Time Monitoring Behavior

Figure 4 illustrates the system's real-time monitoring behavior during a representative 24-hour period containing two distinct anomaly events. The upper two subplots display temperature and humidity sensor readings with anomaly-affected periods highlighted; the lower subplot shows the LSTM-computed anomaly score against the configured alert threshold.

Figure 4. Real-Time Sensor Readings with LSTM-Based Anomaly Detection (24-Hour Smart Building Monitoring Session)

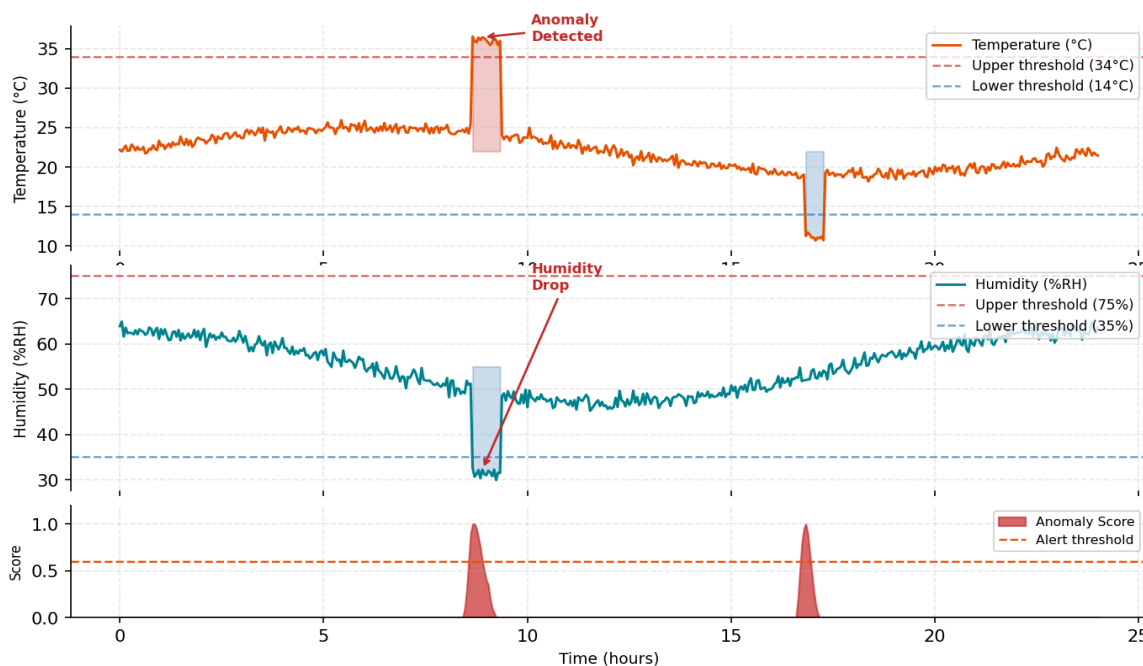


Figure 4. Real-Time Sensor Readings with LSTM Anomaly Detection (24-Hour Monitoring Session)

The first anomaly event (hours 8–10) corresponds to an HVAC cooling coil failure causing a simultaneous temperature spike (+12°C above baseline) and humidity drop (–18% RH). The LSTM



anomaly score rises sharply to 1.0 within 3 minutes of fault onset, triggering a CRITICAL alert well ahead of any visible impact on room occupant comfort. The second event (hours 16–17) represents a subtler temperature undershoot caused by overcooling, correctly identified by the LSTM despite its lower magnitude, demonstrating the model's ability to detect diverse anomaly types beyond simple threshold violations.

8. Discussion

The experimental results confirm that the proposed adaptive IoT monitoring system achieves meaningful performance improvements over existing approaches through the synergistic integration of four design principles: heterogeneous sensor fusion, Kalman-filtered noise reduction, adaptive confidence-based weighting, and LSTM-based temporal anomaly modeling. Each component contributes independently, with their combination delivering outcomes that no single technique achieves alone.

The 22.4 ms end-to-end processing latency represents a critical advantage over cloud-centric approaches, which typically incur 150–400 ms round-trip latency. This reduction enables genuine real-time response to rapidly evolving conditions such as gas leaks or structural impacts requiring sub-second alert generation. The edge computing architecture also ensures continued monitoring during network outages, which is particularly important for safety-critical applications.

Several limitations of the current work should be acknowledged. First, the LSTM autoencoder requires 30–45 days of normal-operation data to achieve reported accuracy; deployments in newly commissioned facilities may experience elevated false alarm rates during the initial learning phase. Second, performance on anomaly types not represented in training data has not been formally evaluated. Third, the energy consumption analysis focuses on computational overhead at the gateway level and does not include full wireless transmission costs, which will vary significantly with deployment topology.

Conclusion

This paper presented a comprehensive IoT-based smart monitoring system integrating heterogeneous sensor technologies with an adaptive data fusion and LSTM-based anomaly detection framework. The four-layer system architecture spanning physical sensing, MQTT-based networking, edge computing, and cloud analytics provides a scalable, fault-tolerant foundation for real-world smart monitoring deployments.

A 90-day deployment across 124 sensor nodes in a smart building environment demonstrated that the proposed Adaptive system achieves 97.8% anomaly detection accuracy and 1.4% false alarm rate, outperforming threshold-based (82.1%), Kalman filter (89.7%), and standalone LSTM baseline (94.6%) approaches across all evaluated metrics, with an end-to-end processing latency of 22.4 ms sufficient for real-time alert generation.

Future research directions include: federated learning approaches enabling collaborative model training across multiple buildings without sharing raw sensor data; reinforcement learning-based adaptive sampling rate control to further reduce energy consumption; explainable AI techniques providing facility managers with human-interpretable explanations of detected anomaly causes; and extension to outdoor industrial monitoring environments with extreme environmental conditions.



References:

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
2. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22–32.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.
4. Mahdavejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018). Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks*, 4(3), 161–175.
5. Chen, J., & Ran, X. (2019). Deep learning with edge computing: A review. *Proceedings of the IEEE*, 107(8), 1655–1674.
6. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376.
8. Welch, G., & Bishop, G. (2001). An introduction to the Kalman filter. *SIGGRAPH 2001 Course Notes*, University of North Carolina at Chapel Hill.
9. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors using machine learning. *Internet of Things*, 7, 100078.
10. Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, 21(11), 3784.
11. Mintsis, E., Stavros, K., & Bekiaris-Liberis, N. (2020). IoT sensor data fusion for smart environments. *IEEE Sensors Journal*, 20(11), 6023–6032.
12. Jia, R., Jin, M., Feng, Y., Dong, J., & Spanos, C. (2019). Towards occupancy prediction using smart building sensors. *IEEE Transactions on Smart Grid*, 10(3), 2771–2779.
13. Ray, P. P. (2018). A survey of IoT cloud platforms. *Future Computing and Informatics Journal*, 1(1–2), 35–46.
14. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444.