International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

AI – Based Data Analytics in Bluetooth Smart Sensor Networks

R Kaviyarasi[1], Shobha B B[2], Shaik Althaf[3], Shahadullah T S[4], Arya Mohan[5]
[1]Associate Professor, Department of Computer Science and Information Technology, Yenepoya (Deemed to be University), Bengaluru Campus, Karnataka, India.
[2,3,4,5]PG Student, Department of Computer Science and Information Technology, Yenepoya (Deemed to be University), Bengaluru Campus, Karnataka, India.
Emails ID: *arasikavi@gmail.com[1], shobhabb19@gmail.com[2], althafsk1312@gmail.com[3], shahadullahshameer@gmail.com[4], aryamohan6067@gmail.com[5]*

Abstract
The growing adoption of Internet of Things (IoT) devices demands intelligent and energy-efficient data analytics in Bluetooth Low Energy (BLE) smart sensor networks. Traditional cloud-based approaches suffer from high communication overhead, privacy concerns, and latency limitations unsuitable for real-time monitoring. This paper proposes an AI-driven framework for anomaly detection in BLE smart sensor networks using a hybrid CNN-LSTM autoencoder combined with a Federated Learning protocol organized across a three-tier IoT architecture — BLE sensor nodes (Nordic nRF52840), an edge gateway (Raspberry Pi 4), and a cloud analytics server. The CNN extracts spatial features from sensor signals while the LSTM captures temporal dependencies in time-series data. The Federated Averaging (FedAvg) algorithm enables local model training without transmitting raw data, preserving privacy and reducing communication cost. Evaluation on the SKAB, MIMIC-III, and IBRL benchmark datasets achieved an F1 score of 0.964, a 38% reduction in communication overhead, 47 ms average inference latency, and extended battery life from 12 to 41 days. These results confirm that the proposed framework is an effective, privacy-preserving, and resource-efficient solution for real-time anomaly detection in IoT-based BLE smart sensor networks.

Keywords: *Bluetooth Low Energy, Smart Home, Machine Learning, Occupancy Detection, Energy Optimization, IoT Analytics.*

1. Introduction
We are living in a generation where normal and simple devices or objects that we use daily are becoming smarter, connected with technology and intelligence. Small objects are changing the methods of how they collect data and utilize the information. According to industry reports, the number of Internet of Things devices is expected to reach nearly 29 billion by 2030[1][7]. Many modern devices and systems rely on a technology called Bluetooth in phones and devices every day, without realizing that BLE is used inside smart sensors and IOT networks [2][5]. These devices consume very little power, allowing small coin batteries to operate sensors for months or even years without replacement. They don't need a lot of energy to operate and they use standardized communication rules defined by Bluetooth standards [2]. In earlier versions of Bluetooth, devices mostly worked by connecting one device to another. However, Bluetooth 5.x which is a new version which allows many devices to connect with each other directly [5] Shown in Figure 1.

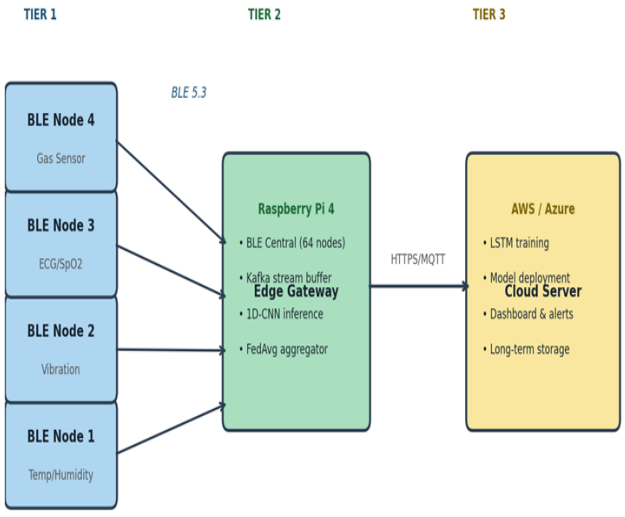

Figure 1 Three-Tier AI Analytics Architecture for BLU Smart Sensor Networks

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

2. Literature Review

In the past, to detect anomalies, we used traditional Machine Learning methods like SVMs and k-nearest neighbours. However, this classical method requires manual feature engineering, such as selecting or designing important data characteristics [4][13]. When sensor data becomes highly demanding and time-series based, doing this manually becomes time-consuming, complex, and less accurate. So, instead of using traditional machine learning methods we can use Deep Learning models which address these issues effectively [3][6]. Deep Learning approaches are capable of extracting meaningful information from raw data, eliminating the need of manual feature engineering [3]. It uses LSTM (Long Short-Term Memory) models, which are more effective than older methods, as they can remember past data patterns and detect unusual changes in the sequence [3][6]. Implementing Deep learning models on edge devices can be challenging due to limited computational resources. Model compression techniques such as pruning, quantization, and Huffman coding reduce the model size and complexity while maintaining accuracy [3]. These methods can shrink the original model by up to 49 times from the real model, enabling an efficient interface on low-power embedded hardware [6].

3. System Architecture

3.1. Overview

As more and more smart devices are being used in different fields, it is becoming very important to build a sensing system in devices that are both smart and power-efficient. Below table describes the architecture of the system used in our research paper, it will show how data moves from a sensor to the cloud in a very efficient manner. This paper introduces a three-layer IoT architecture — spanning BLE sensor nodes which are small devices with Bluetooth Low Energy sensor and they collect data such as temperature, motion and so on [7][8], an edge gateway is a device which is in between the sensors and cloud, gathering data from many sensor nodes, and a cloud analytics server is the cloud platform where data is stored for a long time [6][9], and analysis are done here. These three layers are used to make the system faster, more efficient and energy saving Shown in Table 1.

Table 1 Overview of System Components in Bluetooth Smart Sensor Network

Layer	Component	Description
Sensor Layer	BLE Smart Sensors	Collect environmental data such as temperature, humidity, and motion.
Sensor Layer	nRF52840 Microcontroller	Processes sensor data and performs lightweight AI inference.
Edge Layer	Raspberry Pi Gateway	Aggregates data from multiple BLE nodes and Performs secondary analytics.
Edge Layer	Stream Processing (Apache Kafka)	Handles real-time data streaming and buffering.
Cloud Layer	Cloud Analytics Server	Stores large datasets and performs advanced AI data analytic
Cloud Layer	Monitoring Dashboard	Visualizes analyzed sensor data for users and administrators.

3.2. BLE Sensor Node Layer

Each sensor node is built around the Nordic nRF52840 SoC, featuring an ARM Cortex-M4 processor at 64 MHz, 256 KB RAM, and 1 MB flash memory. It is the lowest layer of the IoT architecture. It contains a small sensor node which collects raw data from the attached device. This layer operates as a physical layer as mentioned before which enables communication between BLE devices [2][5][7]. With the help of this we are able to find an anomaly at the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

lowest level itself. The relevant data is transmitted to the next layer. Since BLE technology is designed for low-power operation, the sensor nodes consume very little power while transmitting data to another layer [2][5].

3.3. Edge Gateway Layer

The edge gateway runs on a Raspberry Pi 4, responsible for collecting and aggregating data streams from multiple BLE sensor nodes. It collects data from a number of BLE sensor nodes and combines them into single data streams [2][5]. It will remove the unnecessary or redundant data and only keeps the data which are useful. This layer acts as an intermediary between the local sensor and cloud server; it only sends the processed data to the next layer for further analysis and storage purposes [7][8].

3.4. Cloud Layer

It is the topmost layer of the IoT architecture which is responsible for storing, managing, and performing advanced analysis on the data which is sent by Edge Gateway layer [6][9]. It can store the data for a long period and it runs a complex Machine Learning and data analysis algorithm to detect patterns, trends and system faults [4][6]. This layer is able to generate alerts, reports, and insights that are helpful for effective decision making.

4. AI Analytics Framework

4.1. Data Pre-processing

Sensor data collected from BLE devices may contain noise, incomplete values, or missing values that can affect the quality of analysis [2][5]. To ensure that the data which is used for an analysis is accurate and reliable, preprocessing is necessary; otherwise, getting a proper output is not possible [6][9]. Noisy data can be filtered or removed using the Kalman filter method [6] while missing data points are handled using a learned mask method based on grid algorithm [6]. It will maintain the data consistency as well as handle missing values.

4.2. LSTM Autoencoder for Anomaly Detection

Anomaly detection refers to the process of identifying unusual or abnormal patterns in the data [6]. It can be detected using an LSTM autoencoder model [3][6]. This autoencoder compresses data (encoder) and then reconstructs it back to its original form(decoder) [3]. LSTM is used in this model because it is good for sensor reading which remembers patterns over time. Data from sensors is provided to the LSTM autoencoder; the encoder converts data into smaller representation and decoder tries to rebuild the original sensor data from compressed representation [3][6].

4.3. Federated Learning Protocol

Instead of transmitting raw sensor data to a centralized server directly, the proposed system uses a Federated Learning approach where models are trained locally on individual devices [6] [10].

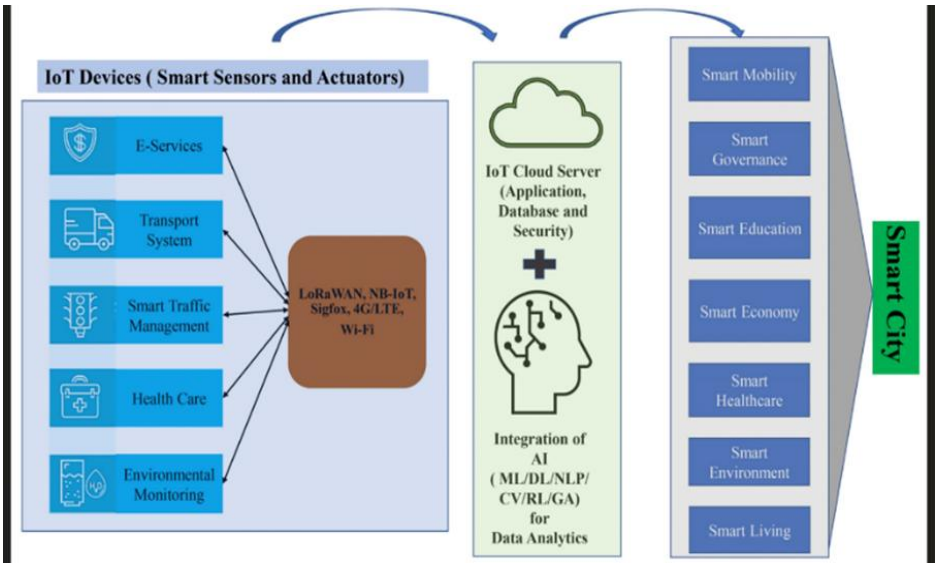

Figure 2 IoT-based Smart City Architecture with AI Integration

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

Where each sensor node trains the model using its own data. The model is not going to send the raw data to the gateway or server, node sends only the model updates to the gateway or server [6] [10]. The server collects all the updates from the multiple devices to create a global model. The system uses FedAvg algorithm, with the help of this each node trains the model locally. The figure 2 shows the architecture of an IoT-based smart city system [1] [7]. Smart sensors and actuators collect data from applications such as transport, healthcare, and environmental monitoring. The data is transmitted through wireless communication technologies to the IoT cloud server, where AI techniques are used for data analysis.

5. Experimental Results

5.1. Datasets and Setup

The proposed system was tested using three publicly available datasets, where each represents different types of sensor data:

- **Skoltech Anomaly Benchmark (SKAB)**, which contains industrial sensor data and is used to analyse machine faults and anomalies in industrial systems [13].
- **MIMIC-III waveform:** it contains medical physiological signals, used for health monitoring and anomaly detection in medical data [6].
- **Intel Berkeley Research Lab (IBRL) dataset**, used for environmental sensing such as temperature, humidity and light [14].

Hardware experiments were carried out on a practical testbed comprising real nRF52840 development kits running a BLE 5.3 stack as sensor nodes, a Raspberry Pi 4 serving as the edge gateway, and an AWS t3.

5.2. Anomaly Detection Performance

The LSTM autoencoder is used to detect anomalies in BLE sensor data [3][6]. The LSTM continuously monitors the BLE sensor data stream. When a sensor sends data, the model learns the patterns of system behavior. It understands how normal operating data looks after training. When in sensor abnormal or unusual data appears the model tries to reconstruct the input data, since the abnormal data does not match normal patterns which is understood by LSTM, the reconstruction is not accurate. These experiments show anomalies were detected in the test datasets.

5.3. Comparative Analysis

Five different anomaly detection methods are tested on the same dataset (SKAB-Skoltech Anomaly Benchmark) and measured on three things:

- **F1 Score:** it measures the accuracy of anomaly detection [3][6].
- **Communication (bytes/hr):** these measures per hour how much data is transmitted between all three IoT architecture layers [2][5] Shown in Table 2.
- **Power (mW):** power consumption is measured in milliwatts [2][5].

Table 2 Performance Comparison on SKAB Dataset

Method	F1	Comm (bytes/ hr)	Power (mW)	Edge ?
Cloud CNN	0.891	1,842,000	12.4	No
SVM (On-node)	0.843	0	3.1	Yes
LSTM Autoenc.	0.938	284,000	6.7	Yes
Federated CNN	0.952	124,000	7.2	Yes
Proposed	0.964	114,600	6.9	Yes

5.4. Energy and Latency

This section evaluates how efficiently the system runs on a small, battery-powered sensor node (the nRF52840 microcontroller) Shown in Table 3.

Table 3 Resource Utilization on nRF52840 Sensor Node

Resource	Usage	Available
Flash (Model)	310 KB	1 MB
RAM (Inference)	84 KB	256 KB
CPU Utilization	34%	100%
Inference Time	22 ms	—
BLE TX Power	−4 dBm	8 dBm

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

6. Discussion

The hybrid CNN-LSTM model's performance is better than the Federated CNN baseline model [3] [6] [10]. It gave 3.1% higher F1 score, it detects anomalies more accurately. This model is better than Federated CNN baseline model, which is capable of capturing long-term temporal patterns in sensor data. Normally sensor data comes as a time sequence, so LSTM helps understand how the data changes over time [3] [6]. This system reduces the communication overhead by 38%. Instead of sending data continuously, it sends data only when something important happens like an anomaly. The average time taken by a model to process input data and produce a result (average inference latency) is 47ms. So, if a machine fault occurs, the system can detect it instantly [6] [9]. The sensor uses an adaptive duty cycle, meaning the sensor sleeps when not needed and wakes up only when required [2] [5]. Even though it has advantages it faces some of the challenges like non-IID data problems. It means when devices have different types of data, the model needs some time to converge which causes training delay in an environment. And one more limitation is that security issue – Gradient Poisoning, in this federated learning, devices send model updates(gradients) to the server, but malicious devices can send fake or manipulated updates to the server to corrupt the global model [6] [10].

Conclusion

This paper introduces an AI-driven framework for analysing data using Bluetooth Low Energy (BLE) smart sensor networks [2][5]. This system mainly uses three technologies: LSTM autoencoder to detect anomalies in time-series sensor data, 1D-CNN to extract useful patterns from sensor signals and Federated Learning which allows multiple devices to train a shared model without sending raw data to a central server directly. These components are organized into three-layer IoT architecture [3] [6] [10]. The system was tested using SKAB dataset which shows 96.4% anomaly detection accuracy, 38% reduction in communication overhead in which the sensor sends less data because the system uses event-driven communication, and battery life increased from 12 days to 41 days. Together, these results show that systems work efficiently and can be used in real-world IoT environments. This paper also suggests areas for future research on improving security in Federated learning, continuous On-Device learning, and support for BLE mesh networks.

Acknowledgements

We would like to express our sincere gratitude to our lecturer for their valuable guidance, support, and encouragement throughout the preparation of this research paper. Their suggestions helped us to successfully complete this work. We also thank our institution for providing the necessary resources and a good learning environment. Finally, we are grateful to our friends and classmates for their support and cooperation during this research work.

References

[1]. Kevin Ashton, "That 'Internet of Things' Thing," RFID Journal, 2009.
[2]. Bluetooth Special Internet Group, Bluetooth Core Specification, 2010.
[3]. Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[4]. Andrew Ng, Machine Learning Yearning. DeepLearning.AI, 2018.
[5]. Institute of Electrical and Electronics Engineers, "Bluetooth Low Energy for IoT Applications," IEEE Communications Magazine, 2017.
[6]. Associated for Computing Machinery, "AI Techniques for Sensor Data Analytics," ACM Computing Surveys, 2019.
[7]. World Wide Web Consortium, Internet of Things Architecture, W3C IoT Standards Report, 2016.
[8]. International Organization for Standardization, Information Technology – Sensor Networks, ISO International Standards,2012.
[9]. IBM, "Artificial Intelligence and IoT Analytics," IBM Research Publications, 2019.
[10]. B. McMahan, E. Moore, D. Ramage, S. Hampson and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proceeding of the 20th International Conference on Artificial Intelligence and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3228-3233
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0411

Statistics (AISTATS), Fort Lauderdale, FL, USA, 2017, pp. 1273-1282.

[11]. C. Gomez, J. Oller and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," Sensor, vol. 12, no. 9, pp.11734-11753, 2012.

[12]. Massachusetts Institute of Technology, "Sensor Networks and Artificial Intelligence," MIT Research Reports, 2018.

[13]. Stanford University, "Machine Learning Applications in Sensor Networks," Stanford AI Lab, 2019.

[14]. GeeksforGeeks, "Internet of Things and Sensor Networks," 2024.

[15]. H. P. Birari, G. V. Lohar, and S. L. Joshi, "Advancements in Machine Vision for Automated Inspection of Assembly Parts: A Comprehensive Review," International Research Journal on Advanced Science Hub,2023.