ISSN: 2795-2215

Journal of Newviews in Engineering & Technology
Faculty of Engineering
Rivers State University, Port Harcourt, Nigeria.

Email: rsujnet@gmail.com | Homepage: www.rsujnet.org

# Mitigating Security and Privacy Challenges in Wireless Sensor Networks Using Federated Learning Approach

Elechi, P.*, Bakare, B.I., Ogra, O.A.E.

*Department of Electrical and Electronic Engineering, Rivers State University, PMB 5080 Port Harcourt, Nigeria.*

*Corresponding Author: elechi.promise@ust.edu.ng

ARTICLE INFO

**Article History**

*Received: 5 August 2024*

*Received in revised form: 23 September 2024*

*Accepted: 12 October 2024*

*Available online: 24 October 2024*

**Keywords**

*Centralized System; Decryption; Encryption; Machine Learning; Sensor Network Technology*

ABSTRACT

By concentrating sensitive information in one location, traditional centralized data processing increases the vulnerabilities of Wireless Sensor Networks (WSNs) to data interception, tampering, unauthorized access, and privacy issues when transmitting sensitive data. Implementing a decentralized machine learning approach would benefit efforts at mitigating these vulnerabilities. In this study, the federated learning approach—a decentralized machine learning approach—was used to address security and privacy challenges in WSNs. The method adopted involved the initialization of sensor data and model parameters, letting the system enter a federated learning loop for each device to update its model using its data, aggregating the local updates into the global model, and using the model for prediction. The algorithm was implemented using MATLAB. Results showed that federated learning improved the resilience of WSNs, achieving 60% reliability and a mean square error of 1.46. This indicates that federated learning can handle the security and privacy concerns in WSNs effectively by decentralizing data processing and preserving privacy. Its ability to protect sensitive information while ensuring the accuracy of data analysis makes it a valuable approach for advancing sensor network technologies across various fields.



## 1. Introduction

Internet of Things (IoT) is increasingly becoming a very promising paradigm with the extensive market adoption of the development of associated technologies including (among others) cloud computing, near-field communications, and wireless mobile networks (Burhanuddin et al., 2018). However, security issues in IoT routed over wireless communication remain a huge challenge. This is because the use of internet devices in different communications through embedded technologies and the adaptive and interactive nature of each communication affects future development tools and applications (Saibabu et al., 2020).

For instance, the increasing prevalence of IoT devices has brought about numerous security challenges due to their relatively simple internal architecture and low-powered hardware warranted by their small footprint requirement (Hu et al., 2022b; Mohammed et al., 2023). The sheer number of IoT devices in use today poses a great security challenge because the devices are often constrained by some hardware and software limitations in addition to being designed with a focus on convenience, ease of use, mass

production, and low cost, rather than security. To enhance the security architecture of IoT devices in use currently, emphasis is gradually shifting to the use of Wireless Sensor Networks (WSNs).

WSNs are described as self-configuring, infrastructureless wireless networks designed to monitor environmental and physical conditions such as temperature, sound, vibration, pressure, motion, or pollutants (Huang et al., 2021). These networks transmit collected data co-operatively through the network to a centralized location, or "sink", where the information is processed and analyzed (Yawar et al., 2017). WSNs typically involve smart devices and sensors that gather real-world data, process them, and communicate same to information processing centers, which in turn generate information-based services for pre-programmed or user-defined actions. WSNs consist of numerous low-cost, low-power, multifunctional sensor nodes that communicate wirelessly over short distances (Sehajpreet & Baby, 2023). These sensor nodes form the basic building blocks of WSNs, with a sink or base station acting as the interface between users and the network, allowing queries to be injected and results to be retrieved (Yawar et al., 2017). The hardware of a sensor node generally comprises four key components including a power management module, sensor, microcontroller, and wireless transceiver. The power module provides the necessary energy for operation, while the sensor detects environmental conditions, converting physical signals into electrical ones. The microcontroller processes the data, and the transceiver handles data transmission and reception (Yawar et al., 2017). Transceivers in sensor nodes consume more power than other components due to the amplification required for packet transmission. WSNs typically use communication standards like IEEE 802.15.4, ZigBee, and Bluetooth, which fall under Wireless Personal Area Network (WPAN) or Low Power Wide Area Network (LPWAN) protocols (Yawar et al., 2017). However, each sensor node is resource-constrained, with limited processing speed, storage, and communication bandwidth.

Despite WSN protocols and security challenges for environmental monitoring applications, in recent years, communication technology has improved exponentially, partly owing to the locations and nature of the deployment of sensor nodes. WSNs contain these sensor nodes and can provide real-time environmental, home, commercial, military, and health system measurements (Italo et al., 2022). WSNs are used in numerous applications that involve sensitive information that needs to be secure and confidential, especially in applications that deal with top-secret information such as military applications (Jin et al., 2021). Since WSNs have revolutionized data collection and real-time monitoring, recent studies have underscored the critical significance of securing WSNs due to their essential role in a broad spectrum of applications (Muawia et al., 2019; Sehajpreet and Baby, 2023).

Even then, the susceptibility of WSNs to security threats remains a significant concern (Hu et al., 2022a). Specifically, WSNs face risks of data interception, tampering, and unauthorized access, as well as privacy issues when transmitting sensitive data. It is widely known that traditional centralized data processing increases these vulnerabilities by concentrating sensitive information in one location, making it more prone to attacks. To mitigate this challenge, federated learning—a decentralized machine learning approach—was adopted in this study. Federated learning enables sensor nodes to collaborate on model training without sharing raw data, thereby protecting data privacy while allowing for effective analysis and prediction. This decentralized approach enhances the security and privacy of WSNs by minimizing the risk of data breaches that are common in centralized systems. The aim of this study was to mitigate the security and privacy challenges in WSNs, which was achieved by addressing the following objectives.

i. Evaluate the responsiveness of the WSN nodes.
ii. Evaluate the integrity of WSN using a federated learning algorithm approach.
iii. Evaluate and encrypt temperature and humidity data using a federated learning algorithm.
iv. Investigate the performance of the federated learning algorithm and the reliability of the federated learning algorithm on WSN nodes.

## 2. Materials and Methods

### *2.1 Materials*

WSN temperature and humidity sensors, Dell latitude E5500 personal computer and router.

### *2.2 Methods*

The method adopted in this work was the application of a federated learning algorithm. Figure 1 represents a federated learning method, designed for a temperature and humidity sensor network. The process begins with the initialization of sensor data and model parameters. Then the system enters a federated learning loop where each device updates its model using its data. These local updates are aggregated into the global model, which gets updated iteratively. After several training epochs, the model was used for prediction. The system also includes a step for securing data before the final phase, where the actual, predicted, and secured data are plotted. The process concludes once all predictions are visualized. The algorithm was implemented using MATLAB.

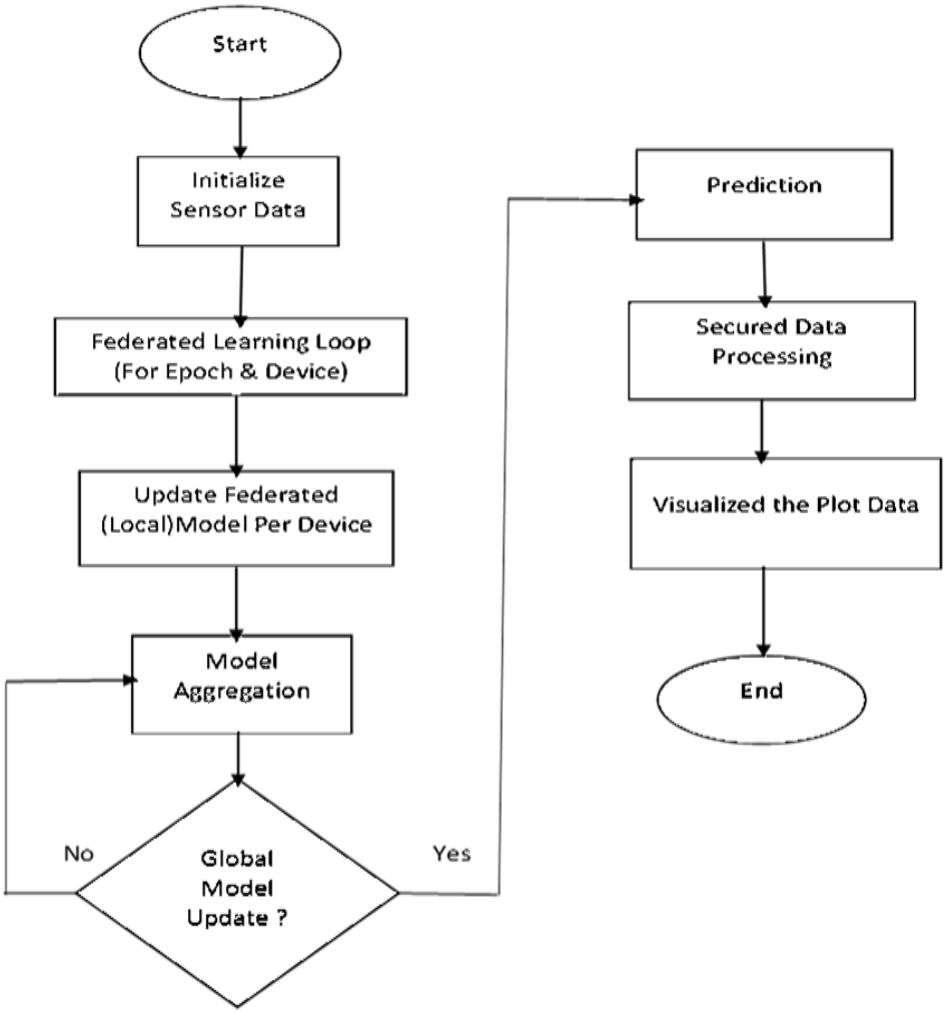


**Figure 1**: Secured Data Flowchart using Federated Learning Algorithm

### 2.2.1 WSN Sensor Evaluation

To evaluate the WSN, each client node updates its local model by minimizing its loss function using its local data. Equation (1) expresses the dynamic behaviour of the sensor nodes (Jia *et al.*, 2019).

$$\theta_{t+1}^{i} = \theta_t - \eta \nabla \mathcal{L}\left(\omega_t^i, D_i\right) \quad (1)$$

The server aggregates the updated models from the client nodes to form equation 2.

$$\theta_{t+1}^{i} = \frac{1}{N} \sum_{i=1}^{N} \theta_{t+1}^{i} \quad (2)$$

The loss function was used by each client to update its local model to give equation 3.

$$\mathcal{L}(\omega, D_i) = \frac{1}{|D_i|} \sum (x, y) \epsilon D_i \;\; \mathcal{L}(f(w, x), y) \quad (3)$$

### 2.3 Data Security Evaluation Using Federated Learning Algorithm

Constraint ensuring that raw data never leaves the client devices is presented in equation 4.

$$Privacy(D_i) = Sensitive\ Information \quad (4)$$

How data are aggregated across nodes while preserving privacy is shown in equation 5.

$$Aggregate\ (D_1, D_2 \ldots D_N) = Encrypted(D_1) \oplus Encrypted(D_2) \oplus \ldots \oplus Encrypted, D_N \quad (5)$$

Table 1 shows the data of the temperature and humidity from the WSN.

**Table 1:** WSN Data for Temperature and Humidity.

| Node ID | Temperature (°C) [a] | Humidity (%) [a] |
|---|---|---|
| Node 1 | 25.3 | 60 |
| Node 2 | 24.8 | 58 |
| Node 3 | 25.5 | 62 |
| Node 4 | 24.9 | 59 |
| Node 5 | 26.1 | 61 |
| Node 6 | 24.7 | 57 |
| Node 7 | 25.9 | 63 |
| Node 8 | 26.3 | 64 |
| Node 9 | 25.2 | 58 |
| Node 10 | 24.5 | 60 |

[a] Data from Sani & Itse (2018).

### 2.4 Temperature and Humidity Data Evaluation

Using the temperature and humidity data from multiple sources for more accurate models, we have equation 6.

$$Fussion\ (T_1, T_2, \ldots T_N, H_1, H_2, \ldots, H_N) - \frac{1}{2N} \sum_{I=1}^{N} (T_i + H_i) \quad (6)$$

Adding noise to the local updates to preserve privacy, we have equation 7.

$$\theta_{t+1}^{i} = \theta_t - \eta \nabla L\left(\omega_t^i, D_i\right) + Noise \quad (7)$$

## 3 Results and Discussion

### 3.1 Received Sensed Data

The sensed data in a WSN represents raw environmental measurements collected by distributed sensor nodes. Figure 2 shows the humidity data within 0 to 4 g/m³ and temperature between -4 to 4°C.

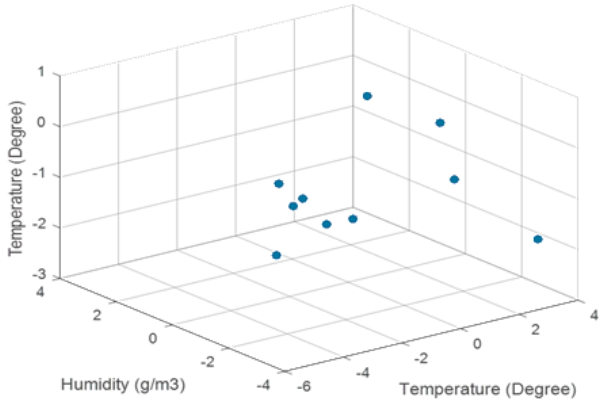


**Figure 2:** Sensor Data and Labels

Figure 3 shows predictions of temperature rising to 50°C and humidity to 40 g/m³. These values reflect real-time conditions such as temperature, humidity, pressure, or motion, depending on sensor configurations. In federated learning, these sensed data serve as input for training machine learning models across nodes. Federated learning processes data locally on each node while sharing model updates with a central server, enabling collaborative prediction without transmitting raw data. The predicted data, shown in Figure 3, demonstrate the model's ability to forecast environmental changes beyond the sensed data, allowing for accurate predictions of trends or anomalies. Federated learning enhances WSN capabilities, turning sensed data into actionable

insights for improved environmental monitoring and management.

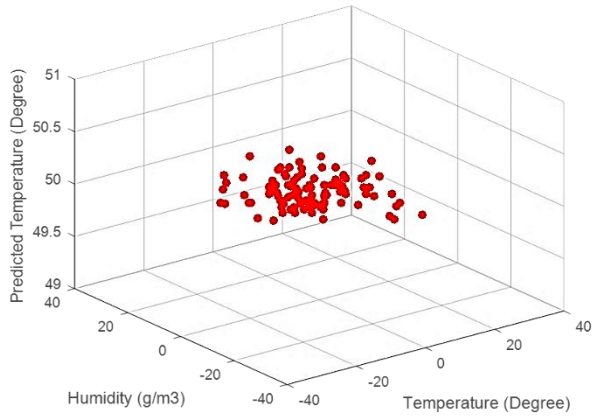


**Figure 3:** Received Sensed Temperature and Humidity Data

*3.2 Encrypted WSN Data*

Figures 4 and 5 show the graphs of temperature and humidity secured and predicted data of a WSN serving as visual representations of environmental conditions, providing valuable insights into temperature and humidity dynamics over time without the need for itemized points. These graphs offer a comprehensive view of environmental parameters, allowing users to observe trends, anomalies, and forecasted patterns. In the secured data graph, temperature and humidity readings collected from sensors within the network are plotted against time. The graph depicts data chronologically, with time progressing along the horizontal axis and temperature/humidity values represented on the vertical axis.

As the secured data graph is examined, patterns and fluctuations in temperature and humidity become apparent. Peaks and troughs in the graph denote periods of high and low readings, respectively. These fluctuations may occur cyclically, such as daily temperature variations, or in response to external factors like weather conditions or human activities. By analyzing the graph's trajectory, users can discern long-term trends and seasonal patterns in environmental conditions.

Anomalies or outliers in the secured data graph may indicate sensor malfunctions, environmental disturbances, or localized events. Sudden spikes or dips in temperature/humidity readings warrant further investigation to ensure data integrity and reliability. Addressing anomalies promptly is crucial for maintaining the accuracy of WSN-based monitoring systems. In contrast, the predicted data graph utilizes forecasting models to estimate future temperature and humidity trends based on historical data and predictive algorithms. This graph extends beyond displaying past observations, offering projections of environmental conditions over upcoming time intervals. Predicted data graphs provide valuable insights for planning and decision making, allowing users to anticipate changes in temperature and humidity and take proactive measures accordingly.

The predicted data graph often overlays forecasted trends onto existing secured data, enabling users to compare actual observations with projected outcomes. Discrepancies between predicted and observed values can highlight deviations from expected patterns, prompting adjustments to monitoring strategies or resource management practices. Both the secured data graph and predicted data graph serve as communication tools, conveying environmental insights to stakeholders effectively. Whether presenting historical trends or future projections, these graphical representations facilitate data comprehension and decision making across various domains, including environmental monitoring, agriculture, infrastructure management, and industrial operations.

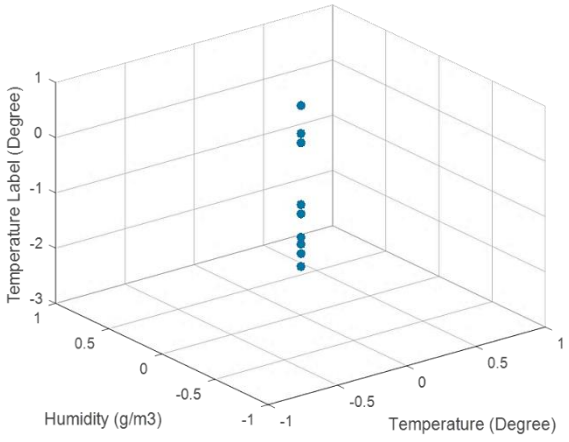


**Figure 4:** Secured Data and Labels

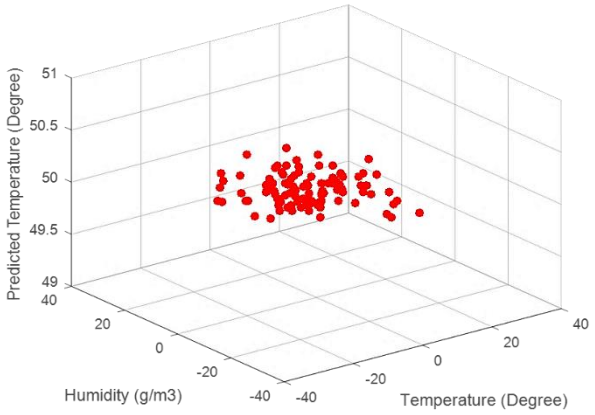


**Figure 5:** Secured Sensor Data

Figure 6 shows the sensor nodes' capacity of the temperature and humidity data of a WSN, which provides a visual representation of environmental conditions over a specified period. This graph serves as a crucial tool for monitoring and analyzing temperature and humidity variations in each location or area of interest. At first glance, the graph presents a series of data points plotted on a Cartesian coordinate system. Typically, time is represented on the horizontal axis, while temperature and humidity values are displayed on the vertical axis. Each data point corresponds to a specific time interval, indicating the concurrent temperature and humidity readings recorded by sensors within the WSN. The patterns and trends in temperature and humidity are easily discernible. Fluctuations in the graph's trajectory reflect changes in environmental conditions over time. For instance, daily temperature variations may manifest as regular oscillations, with peaks and troughs corresponding to daytime warmth and nighttime cooling. Similarly, humidity levels may exhibit fluctuations in response to weather patterns, such as increased humidity during rainy periods.

The graph's shape and slope offer insights into the overall trend of temperature and humidity conditions. A steep incline or decline in the graph suggests rapid changes in environmental parameters, indicating sudden shifts in weather or other factors influencing temperature and humidity. In contrast, a gradual slope signifies more stable conditions, with minor fluctuations occurring over time.

Anomalies or outliers in the data may appear as isolated data points deviating significantly from the overall trend. These anomalies could result from sensor malfunctions, environmental disturbances, or localized events impacting temperature and humidity readings. Identifying and addressing such anomalies is essential for ensuring the accuracy and reliability of the data collected by the WSN.

Overlaying multiple datasets on the same graph allows for comparative analysis of temperature and humidity trends. By plotting data from different sensor nodes within the network or comparing data from different periods, users can discern spatial and temporal variations in environmental conditions. Such comparisons reveal spatial gradients in temperature and humidity or highlight temporal synchronicities across different locations.

Moreover, the temperature and humidity data graph can incorporate additional features to enhance data interpretation. Colour-coded markers or lines may differentiate between temperature and humidity readings, making it easier to distinguish between the two parameters. Annotations or labels on the graph provide context for significant events or trends, aiding users in understanding the data more comprehensively.

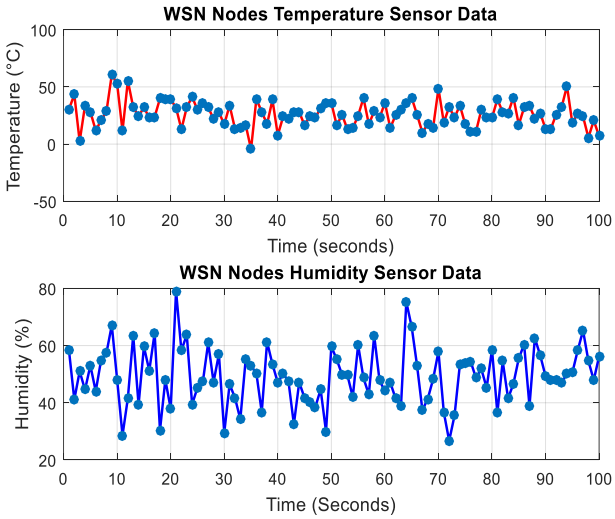


**Figure 6**: WSN Nodes Sensor

Beyond mere visualization, the graph facilitates data-driven decision-making and planning. Stakeholders can use the insights gleaned from the graph to optimize resource management, mitigate environmental risks, or plan for future scenarios. For example, agricultural practitioners may use temperature and humidity data to schedule irrigation or monitor crop health, while urban planners may utilize the data to design climate-resilient infrastructure.

### *3.3 Tampered Sensor Data*

Figure 7 shows the WSN and how it operates as a complex system of interconnected nodes, each tasked with collecting and transmitting data from their respective environments. The integrity of this data is paramount for the network to function effectively. However, when a sensor within the network is tampered with, it disrupts the flow of accurate information, leading to potential complications and security breaches.

In a hypothetical graph of interconnections of sensors within a WSN, each node in this graph symbolizes a sensor, and the edges between them depict communication channels through which data flow. This graph serves as a visual representation of the network's structure and the relationships between its components. In a tampered sensor scenario, one or more nodes in this graph are compromised, either physically or electronically. This compromise could range from subtle alterations to outright manipulation of sensor readings. As a result, the graph's integrity is compromised, leading to distortions in the data being transmitted across the network. Consider a WSN deployed for environmental monitoring in a forest. Each sensor node in the network is responsible for measuring parameters such as temperature, humidity, and air quality. These nodes communicate with each other to relay this data to a central control unit for analysis and decision-making. Now, suppose an adversary gains unauthorized access to one of the sensor nodes and modifies its temperature readings to falsely indicate a fire outbreak. This tampered sensor continues to communicate these falsified readings to neighboring nodes, propagating misinformation throughout the network. As the tampered data spreads through the network, it influences the decisions and actions taken based on this information. In the case of our forest monitoring example, authorities might dispatch firefighting teams to a location based on the false alarm triggered by the tampered sensor data. This not only wastes resources but also diverts attention away from genuine emergencies elsewhere.

Moreover, the presence of a tampered sensor undermines trust in the entire network. Users relying on WSN data for critical tasks may begin to question the reliability of the information being provided. This loss of trust can have far-reaching consequences, affecting the adoption and utilization of WSN technology across various domains. Addressing the challenge of tampered sensors in WSNs requires a concerted effort to enhance security measures and develop robust defence mechanisms. Physical security measures, such as tamper-evident enclosures and secure mounting techniques, can help prevent unauthorized access to sensor nodes.

Additionally, implementing cryptographic protocols and authentication mechanisms can safeguard data transmission within the network, ensuring the integrity and confidentiality of information exchanged between nodes. Continuous monitoring and anomaly detection algorithms further aid in identifying and mitigating instances of sensor tampering, enabling timely response to potential security breaches.

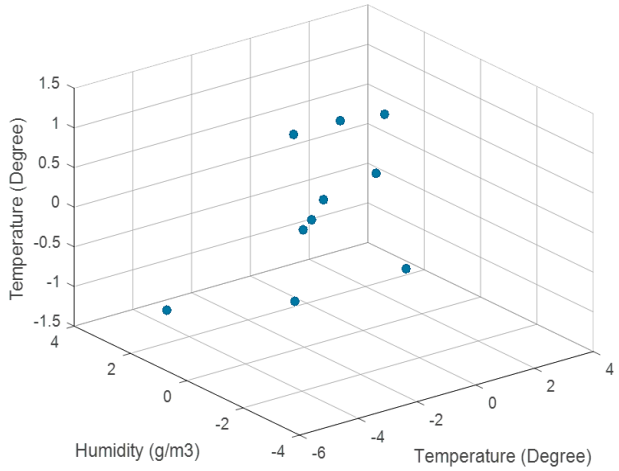


**Figure 7:** Tampered Sensor Data and Labels

### 3.4 WSN Performance Using Federated Learning

Figure 8 shows the behaviour of federated learning that offers promising avenues for training models within WSNs while mitigating concerns regarding data privacy and communication overhead. When evaluating the performance of federated learning on WSNs, metrics such as mean squared error (MSE) and training epochs provide insights into the effectiveness and efficiency of the learning process. In a scenario where the MSE is measured at 1.46 and the training is conducted over a single epoch, several key observations can be made regarding the performance of federated learning within the WSN context.

First, the MSE value of 1.46 indicates the average squared difference between predicted and actual values across the dataset. In the context of federated learning on WSNs, this MSE value reflects the model's prediction accuracy in capturing the underlying patterns within the sensor data. A lower MSE suggests that the model's predictions closely align with ground truth observations, indicating superior performance in learning from the distributed sensor data.

Moreover, achieving an MSE of 1.46 within a single epoch demonstrates the efficiency of federated learning in leveraging the collective intelligence of sensor nodes for model training. By aggregating local updates from individual nodes and incorporating them into the model, federated learning minimizes the need for extensive communication and centralized processing thus, reducing the computational burden on resource-constrained WSNs.

Furthermore, the choice of a single epoch for training underscores the iterative nature of federated learning, where model updates are incrementally refined over multiple rounds of communication and collaboration. While a single epoch may provide a preliminary snapshot of model performance, it may not fully capture the potential improvements that could be achieved through additional training iterations. Therefore, future evaluations may involve extending the training process over multiple epochs to assess the convergence and stability of the learned model.

Additionally, the performance of federated learning on WSNs is influenced by various factors, including network topology, communication latency, and data heterogeneity. The decentralized nature of WSNs introduces challenges such as node mobility, unreliable communication links, and energy constraints, which can impact the effectiveness of federated learning algorithms. Addressing these challenges requires tailored optimization techniques and adaptive learning strategies to enhance the robustness and scalability of federated learning in WSN environments.

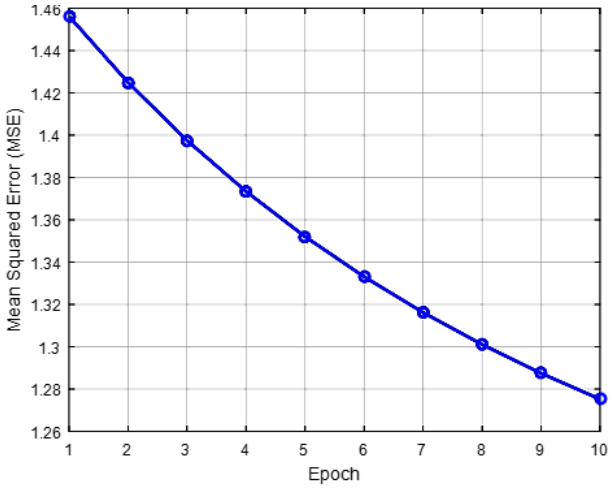


**Figure 8:** Performance of Federated Learning

### 3.5 Sensor Data with Detected Anomalies

Figure 9 is a visual representation used to analyze anomalies or irregularities within data collected by sensors in a system or environment. This graph provides a comprehensive view of sensor data over time, allowing analysts to identify deviations from expected patterns or behaviour. The graph shows that the sensor data detected anomalies.

At its core, the graph displays a time-series representation of sensor measurements, with time intervals plotted along the x-axis and corresponding sensor observations plotted along the y-axis. Each data point on the graph represents a specific measurement recorded by the sensors at a particular time, providing insights into the dynamics and trends within the monitored system.

Anomalies detected within the sensor data are visually highlighted on the graph, often using distinct markers, colors, or annotations to differentiate them from normal data points. These anomalies can manifest in various forms, including sudden spikes or drops in sensor readings, unexpected fluctuations, or patterns deviating significantly from historical norms.

The graph serves multiple purposes in analyzing sensor data anomalies. Firstly, it facilitates the detection of anomalies by allowing analysts to visually identify irregularities within the data. By observing deviations from expected patterns, analysts can pinpoint potential issues or abnormal events that require further investigation.

Moreover, the graph enables analysts to analyze the characteristics of detected anomalies, such as their magnitude, duration, frequency, and contextual information. This analysis aids in understanding the nature and severity of anomalies and formulating appropriate response strategies.

The graph also supports the identification of long-term trends and patterns within the sensor data. By visualizing data over time, analysts can distinguish between transient anomalies and sustained deviations, providing insights into systemic issues or emerging trends.

Real-time monitoring of the graph allows for timely detection and notification of anomalous events, enabling operators to respond promptly and mitigate potential impacts. Automated alerting mechanisms can be integrated to notify stakeholders when anomalies surpass predefined thresholds or violate established norms.

Furthermore, analysts can correlate anomalies detected in sensor data with other relevant datasets to uncover causal relationships and contextualize abnormal observations. This holistic approach enhances understanding and decision-making regarding anomaly mitigation and response.

Additionally, historical anomaly data depicted on the graph can inform predictive modeling and machine learning algorithms, enabling the anticipation and prevention of future anomalies through early warning systems and proactive maintenance strategies.

Overall, the sensor data detected anomalies graph serves as a powerful tool for monitoring, analyzing, and responding to anomalies within sensor data. By providing a visual representation of anomalies, the graph empowers stakeholders to make informed decisions, optimize resource allocation, enhance system reliability, and mitigate risks associated with abnormal events.

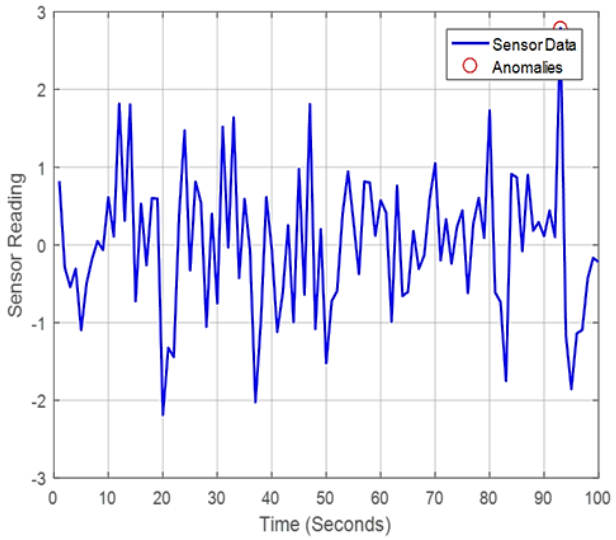


**Figure 9:** Detected Anomalies

*3.6 Data Integrity*

Ensuring data integrity during the transmission and reception of temperature readings, such as 25.5°C and 27.5°C, is crucial for maintaining accurate and reliable information flow. Data integrity refers to the process of ensuring that data remains accurate, consistent, and reliable from its creation to reception. For temperature data transmission, integrity is preserved through encoding, modulating, and converting the data into a format suitable for communication. Proper encoding techniques help minimize distortion or alteration during transmission as shown in Figure 10.

Transmission channels often introduce noise and interference, but error detection and correction methods, like checksums, help detect and rectify discrepancies. Reliable transmission protocols, such as TCP/IP, enhance data integrity by

incorporating acknowledgments and re-transmission mechanisms. Additionally, encryption safeguards the data from tampering, while authentication confirms the identities of the sender and receiver. Upon reception, the data is verified for consistency through error detection, validation, decryption, and authentication processes to ensure it matches the original values sent.

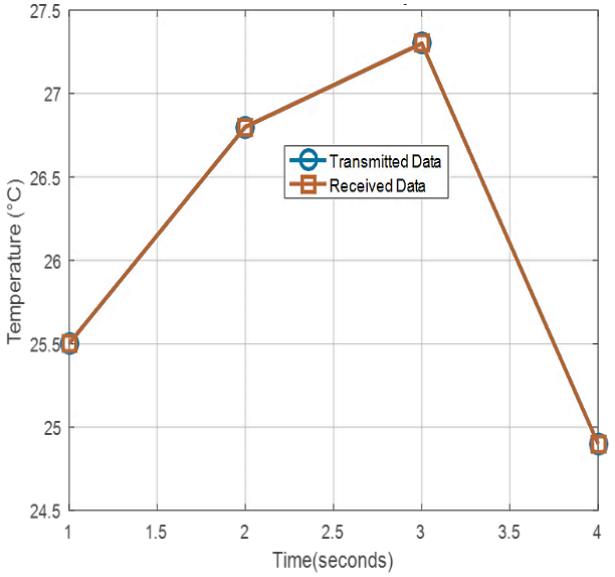


**Figure 10:** Data Integrity

## 4.0 Conclusions

This study thoroughly examined several critical aspects of WSNs using federated learning algorithm. The work provided a focused analysis that contributes to the overall understanding of how federated learning can enhance the functionality, security, and performance of WSNs.

In the first instance, the responsiveness of WSN nodes was evaluated. The findings indicated that the nodes could efficiently respond to data collection and processing tasks, maintaining optimal performance under various conditions. This responsiveness is crucial for real-time applications where timely data acquisition and transmission are essential.

Furthermore, the integrity of the WSN was assessed using a federated learning algorithm approach implemented with MATLAB. The results demonstrated that federated learning significantly enhanced data integrity by minimizing the risks associated with centralized data storage and processing. By distributing the learning process, the system showed improved resilience against data corruption and attacks.

Also, temperature and humidity data were encrypted and evaluated using a federated learning algorithm. The encryption process ensured that sensitive data remained secure throughout its lifecycle. In addition, the federated learning algorithm facilitated effective data processing without compromising the encryption, thereby maintaining both data security and analytical accuracy.

Besides, the performance and reliability of the federated learning algorithm on WSN nodes were investigated. The federated approach proved to be robust and reliable, showing consistent performance across various scenarios. This reliability is crucial for applications that depend on the continuous and accurate functioning of WSNs, such as environmental monitoring and smart agriculture.

Additionally, the performance of federated learning algorithms was evaluated, highlighting key advantages such as enhanced data privacy, scalability, and resilience. Federated learning proved to be a more secure and efficient solution, addressing concerns like data breaches and system vulnerabilities by avoiding a single point of failure. This decentralized approach allowed for improved security and scalability without compromising on performance.

From the foregoing, federated learning algorithms offer substantial advantages for WSNs in terms of responsiveness, data integrity, security, performance, and reliability. These benefits position federated learning as a superior approach to centralized learning, making it a viable and preferable option for future WSN applications.

## Acknowledgements

Authors are grateful to all those who supported this research in the form of financial assistance and/or provision of the necessary resources.

## References


Burhanuddin, M. A., Ali, A. M., Ronizam, I., Mustafa, E. H., Ali, N. K. & Halizah, B. (2018). A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective. Journal of Telecommunication, Electronic and Computer Engineering, 10(9), 1-7.

Hu, M., Wu, D., Zhou, Y., Chen, X., & Chen, M. (2022). Incentive-aware autonomous client participation in federated learning. IEEE Transactions on Parallel and Distributed Systems, 33(10), 2612–2627.

Hu, M., Yang, W., Luo, Z., Liu, X., Zhou, Y., Chen, X., & Wu, D. (2022). Autofl: A bayesian game approach for autonomous client participation in federated edge learning. IEEE Transactions on Mobile Computing. 21(5)1439-1452.

Huang, Y., Chu, L., Zhou, Z., Wang, L., Liu, J., Pei, J., & Zhang, Y. (2021). Personalized cross-silo federated learning on non-iid data. In: Proceedings of the Association for the Advancement of Artificial Intelligence. pp. 7865–7873.

Italo, F. P. S & Diego, F. A. P. (2022). Analysis of The Cybersecurity in Wireless Sensor Networks (WSN): A Review Literature. IEEE Communication Magazine, 54(6), 68-74.

Jia, J., Chen, J., Deng, Y., Wang, X., & Aghvami, A.-H. (2021). Reliability optimization for industrial WSNs with FD relays and multiple parallel connections. Journal of Network and Computer Applications, 179, 102993. https://doi.org/10.1016/j.jnca.2021.102993.

Jia, R., Dao, D., Wang, B., Hubis, F. A., Hynes, N., Gurel, N. M., Li, B., Zhang, C., Song, D., & Spanos, C. J. (2019). Towards efficient data valuation based on the Shapley value. In: Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics. Naha, Okinawa, Japan. pp. 1167–1176.

Kofi, S. A., Felicia, E., Godwin, S. K., Godwill, E. B. & Bernice, A. D, (2022). WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey. Journal of Sensors, 11(9), 1-21.

Mohammed, A. A., Wael, E. & Mhd, S. S. (2023). Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques. Journal of Cyber Security Technology, 7(4), 199-223.

Muawia, A. E., Abdulrahman, A., Mohammed, A. A. B. (2019). Security Issues and Challenges on Wireless Sensor Networks. International Journal of Advanced Trends in Computer Science and Engineering, 8(4), 1551-1559.

Saibabu, G., Anuj, J., Sharma, V. K. (2020). Security Issues and Challenges in IoT Routing over Wireless Communication. International Journal of Innovative Technology and Exploring Engineering, 9(4), 1572-1580.

Sehajpreet, K., & Baby, M. (2023). Securing the Future of Wireless Sensor Networks: Challenges, Threats, and Innovative Solutions. Journal for Research in Applied Science and Engineering Technology,11(11), 719-728.

Yawar, A. B., Qamar, U. D. A., Alshreef, A. A. A., Yahya, E. A. A. (2017). Security Issues and Challenges in Wireless Sensor Networks: A Survey. International Journal of Computer Science, 44(2), 1-8.