FMDB *Transactions on Sustainable Computer Letters*

An Improved Deep Learning Based Security Framework for Sensitive Traffic Management for High-Density WSN

Suman Avdhesh Yadav[1], Pinki Sharma[2], Rahat Naz[3], Pramod Kumar Sagar[4], Birendra Kumar Saraswat[5,*], Angeles Quezada[6]

[1]School of Computer Science and Engineering, IILM University, Gautam Buddha Nagar, Uttar Pradesh, India.
[2]Department of Computer Applications, JSS Academy of Technical Education, Gautam Buddha Nagar, Uttar Pradesh, India.
[3]National School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India.
[4]Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, India.
[5]Department of Information Technology, GL Bajaj Institute of Technology and Management, Gautam Buddha Nagar, Uttar Pradesh, India.
[6]Department of Systems and Computing, Institute of Tijuana, Tijuana, Baja California, Mexico.
suman.avdheshyadav@gmail.com[1], pinkiabes2@gmail.com[2], nazrahat38@gmail.com[3], pksagar1975@gmail.com[4], saraswatbirendra@gmail.com[5], angeles.quezada@tectijuana.edu.mx[6]

Abstract: Wireless Sensor Networks (WSNs) have been widely applied across various sectors, leading to a vast increase in the transmission of sensitive data in these networks. Hence, the security of traffic in this concentration of wireless sensor networks has become an imperative problem. Traditional security measures failed to provide sufficient security in WSN environments; researchers have proposed alternatives. To handle the significant traffic in D2D high-density WSNs, researchers propose a deep learning-based security architecture. The multi-branch deep learning architecture proposed in this work is a major gateway for this industry, identifying different types of sensitive traffic in content and behaviour. The proposed model obtained 83.94% energy consumption, 80.95% data confidentiality, 89.95% scalability and 92.97% Communication overhead. This approach is better than the more conventional approaches at identifying sensitive messages and prioritising them. It relies on a routing trick that uses the network's real-time state to reroute critical data along alternative paths. This is intended to preserve the privacy of private data by minimising the likelihood of theft or loss. It allows the network to recognise and discount malignant antipodes that act to pervert the network or halt the private data transaction. There is also a recommendation for an artificial intelligence intrusion detection system capable of learning new attack patterns and adapting its defence to them.

Keywords: High-Density; Encryption and Authentication; Access Control; Network Traffic; Sensitive Data; Data Transaction; Intrusion Detection System; WSN Environments.

Received on: 16/02/2025, **Revised on:** 01/05/2025, **Accepted on:** 14/06/2025, **Published on:** 03/01/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2026.000596

Cite as: S. A. Yadav, P. Sharma, R. Naz, P. K. Sagar, B. K. Saraswat, and A. Quezada, "An Improved Deep Learning Based Security Framework for Sensitive Traffic Management for High-Density WSN," *FMDB Transactions on Sustainable Computer Letters*, vol. 4, no. 1, pp. 1–13, 2026.

[*]Corresponding author.

1. Introduction

A prominent function in a high-density wireless sensor network is traffic management. In congested networks, the limited capacity of links makes it crucial to transmit data accurately and efficiently [1]. Whitespace management in a high-occupancy application in an active environment is a demanding challenge. The limited amount of radio spectrum resources causes interference and collisions between nodes, which is the main problem in high-density wireless sensor networks [2]; [3]. As a result, this can lead to network congestion, which ultimately significantly affects the efficiency and trustworthiness of data transmission [4]. They are intended to help speed up and better use the road network's information pipeline. Quality of Service (QoS) mechanisms must ensure that essential traffic is carried at the required level of service [5]. A fundamental process in Networking is sorting Network data into categories. QoS may be used to ensure the timely, guaranteed transfer of relevant data; real-time and control data are prioritised over other types of data [6]. Routing protocols are developed as an integral part of highly sensitive traffic management in WSNs to facilitate the management of data-rich environments [7]. However, optimising how data hops from one node to another depends on factors such as energy constraints, network structure, and density [8]; [9].

An adaptive high-traffic can adjust to new data in the network, which is critical for managing sensitive traffic in dense WSNs [10]. Various QoS and Routing protocols are designed to exploit the unique characteristics of WSNs, which offer a highly secure and reliable environment and many routing criteria for data management in high-density networks [11]. This is crucial for the proper operation of high-density wireless sensor networks, which have many applications [12]. WSNs consist of numerous low-resource nodes deployed in a designated field to detect and monitor a diverse range of environmental parameters [13]. Traffic and Administration issues: In high-density wireless sensor networks, where multiple nodes are densely packed in a narrow space. Careful traffic control can be achieved by conserving energy at nodes, enabling the network to remain operational longer [14]. Transmitting and harvesting large volumes of sensitive data increases the risk of data breaches and unauthorised access. Encryption and authentication systems are critical elements of managing sensitive traffic because they ensure the safe transport of information and prevent unauthorised access [15]. The main contribution of the research is as follows:

- The proposed scheme is anticipated to enhance the application of WSN for sensitive traffic, thereby ensuring the timely delivery of vital data while minimising transmission latency for non-sensitive data.
- The dense sensor nodes characterised the paradigm, algorithms, and protocols designed for use with highly dense WSNs. These approaches give you confidence that sensitive data will reach its final destination securely and reliably, regardless of network conditions and data sensitivity.
- Sensitive traffic management methods by allocating priority to sensitive traffic and addressing congestion hot spots through adaptive generation of network transmission paths and sensitive joint data rate. The overall dependability and performance of WSNs are improved as a result.

2. Related Words

Kalpana and Ajitha [16] proposed a strategy to enhance security and detect rogue nodes in WSNs. Heuristics and problem-solving methods have been integrated with deep learning algorithms to detect and prevent potential hazards in WSNs. Such an approach will improve the performance and precision of WSNs, making them more resilient to attacks. Naveed et al. [17] presented an optimal phase timing and successfully monitored and adjusted the condition of traffic flow. This technology also uses sensor data collected by roaming sensors, providing real-time data to adapt traffic lights. This increases road efficiency and safety. Al-Quayed et al. [18] discussed techniques that analyse historical data to identify trends and predict potential threats, thereby enabling the development of preventive measures. It enhances the capabilities of industrial environments for intrusion detection and prevention, improving effectiveness and efficiency. Srinivasan et al. [19] have reported on a new concept that combines IoT and WSN to achieve better performance and sustainability in smart cities. It enables real-time data monitoring and analysis, which , in turn, facilitates intelligent decision-making and resource optimisation, making cities more sustainable and efficient. Raveendranadh and Tamilselvan [20] reported a specific type of deep neural network, the exponential polynomial kernel-centred DNN, for effectively detecting attacks in wireless sensor networks. As a result, it provided adequate network protection and successfully identified various types of attacks. Overall, the DNN was trained using data from various sensors.

Kumar et al. [21] outlined an architecture that combines the security advantages of the blockchain with the advanced features of deep learning to preserve privacy in a cooperative intelligent transport system (C-ITS). It uses secure communication protocols and decentralised data storage to enable the safe sharing of information between vehicles without compromising the privacy of drivers and passengers. Asha et al. [22] studied the optimisation of smart applications in a smart city, aiming to develop a better, faster method for predicting the performance of smart city software. By using a modified honey badger algorithm, the system continues to improve performance and accuracy throughout this process. Arunachalam and Kanmani [23] discussed a security threat in WSNs in which an attacker causes surrounding nodes to expend energy, thereby diminishing the network's overall effectiveness. To address this, a safe routing strategy using a weighted RNN and an optimal path is proposed,

improving energy efficiency while maintaining data integrity in WSNs. Ding [24] introduced a GAN that generates fake nodes in a WSN to attract potential attackers and collect information on their methods. This data is used to enhance network security and to devise countermeasures to prevent an attack from happening again. Alrowais et al. [25] proposed a security technology to detect and classify hostile activity via an arithmetic-estimation-based and density-based clustering approach using deep learning algorithms. This technology utilises data analytics and machine learning models to detect potential security weaknesses and defend against cyberattacks.

Meenakshi and Karunkuzhali [26] discussed the self-attention mechanism and a variational auto-encoder for generating fraudulent packets, which are then trained with a generative adversarial network for subsequent detection. This improves the WSN's ability to identify and stop cyber threats while reducing power consumption and computational load. The self-learning-based clustering and load-balancing method previously used for distributing real-time traffic data in wireless networks was optimised, as discussed by Jain et al. [27]. It allows it to learn to produce the cluster in a way that favours data spread. This helps alleviate network congestion and improve the transmission of time-critical information across diverse applications. Rameshkumar et al. [28] proposed a method that uses deep learning with transfer learning to tune the model for DDOS attacks and variants over the years, thereby providing an efficient model for detection and classification to diminish this class of attack. Khatri et al. [29] studied machine learning techniques for analysing and predicting traffic trends in VANET networks. By utilising vehicle speed, location, and traffic flow data, these models can enhance traffic control methods. Bukhari et al. [30] proposed protecting critical data and identifying unwanted network activity while maintaining users' privacy. This is achieved through encryption, authentication, and anonymisation mechanisms that guarantee a secure communication landscape and minimise the risk of cyberattacks. Table 1 presents a thorough examination of the current systems.

Table 1: Comprehensive analysis

Authors	Advantage	Limitation
Kalpana and Ajitha [16]	Integrates efficient feature extraction and high accuracy while ensuring robustness against malicious attacks.	Limited to a specific type of network and may not perform well on other types of networks.
Naveed et al. [17]	Real-time traffic monitoring and efficient traffic flow management, leading to reduced congestion and improved safety on roads.	Reliance on accurate sensor data and potential interference from other wireless devices may affect system performance.
Al-Quayed et al. [18]	It can more accurately detect and prevent attacks by continuously adapting to changing environments and behaviours in industrial settings.	This approach may not be effective against new, unknown cyber threats, as it relies on past data and patterns for detection and prevention.
Srinivasan et al. [19]	Improved efficiency and sustainability in smart cities	The proposed approach may not account for social and cultural factors that can affect the efficiency and sustainability of smart cities.
Raveendranadh and Tamilselvan [20]	Improved defence against network attacks	Dependence on the availability and accuracy of training data for the neural network to accurately detect attacks.
Kumar et al. [21]	Improved security and confidentiality of data.	The framework may not handle highly dynamic network environments, such as sudden increases or decreases in traffic volume.
Asha et al. [22]	Improved prediction accuracy enables more efficient use of IoT and WSN resources, resulting in better performance in smart city applications.	One limitation is that it may not be suitable for all types of IoT and WSN applications, as they may have different performance requirements and characteristics.
Arunachalam and Kanmani [23]	Improved network security and resilience through timely identification and prevention of attacks, leading to uninterrupted data transmission and reliable network performance.	One limitation is that this method may not be effective against multiple simultaneous vampire attacks across different parts of the network.

Ding [24]	Improved protection against cyber-attacks by using a network of honeypots to deceive and gather information on potential malicious activity.	Training data used to generate fake nodes may not accurately reflect attacker behaviour, leading to incomplete and biased results.
Alrowais et al. [25]	Enhances intrusion detection accuracy by identifying detailed patterns and malicious behaviours using advanced mathematical techniques.	The limitation is that it relies heavily on the quantity and quality of training data for effective detection.
Meenakshi and Karunkuzhali [26]	Improved protection of sensitive data and prevention of cyber-attacks on WSN through advanced machine learning techniques.	Complexity and computational resources required for training and implementation may be a limitation.
Jain et al. [27]	Increased efficiency in the real-time distribution of traffic data, leading to improved network performance and user experience.	Inaccurate clustering decisions due to changes in traffic flow patterns or network conditions.
Rameshkumar et al. [28]	The model can continuously adapt to new and evolving attack patterns, improving detection accuracy and reducing false alarms.	One limitation is that it may require a large amount of labelled data from previous attacks to effectively train the model for new, unseen attacks.
Khatri et al. [29]	Improved traffic flow efficiency due to real-time data collection, analysis and prediction capabilities of machine learning models in VANET-based traffic management.	Obtaining large amounts of training data can be difficult and may not accurately reflect real-world scenarios.
Bukhari et al. [30]	Real-time identification of potential intrusions without compromising sensitive data or exposing system vulnerabilities.	The limitation is that some intrusion detection techniques may not be suitable for large-scale sensor networks due to resource constraints.

2.1. Research Gaps

- The traditional deep learning systems, which have been resilient and need to learn all the features to improve their capability. The models are vulnerable to adversarial attacks, in which a small perturbation in the input data can cause the neural network to misclassify or produce incorrect outputs. This introduces a significant security threat, especially when the neural network's predictions are important.
- Most current models have complex architectures and depend on large quantities of data, making it impossible to get an explanation of the logic leading to its decisions. This feature of non-explainability makes it easier to examine and address potential security vulnerabilities present in the model.
- Most existing models require vast amounts of data for training, including sensitive and personal data. This raises concerns about data privacy and the risk of bias and discrimination in the model's predictions.

Deep learning algorithms have transformed computer security by enabling more effective and accurate threat identification. In this framework, researchers propose an advanced deep learning-based security architecture that leverages recent advances to enhance system security. This allows our technology to sift through large amounts of data and identify trends to describe a variety of attacks, including malware, phishing, and data breaches. Also, our system has multiple layers, each a buffer against a different security threat. That provides a complete and efficient defence against known or unknown threats.

3. Proposed System

The sink acts as a central base station in a WSN. The system gathers information from every node within the network and sends it to a specified location. The sink oversees and regulates the communication protocols and tasks present within the network. A cluster in a wireless sensor network is a collection of nodes situated in proximity to one another and linked via a shared cluster head. Clustering facilitates effective data collection and transmission while also promoting energy conservation within the network:

$$X_{new} = \frac{X_i - \mu}{\sigma} \quad (1)$$

By determining the connection between data points and eliminating those with strong correlation, the goal is to achieve dimensionality reduction:

$$Conv(Z,k)_{(i,j)} = \sum_{y,r}^{Y,R} Z_{(y,r).y(i+k+l)} \quad (2)$$

The most crucial component of the CNN structure is the convolutional layer, which convolves small regions of the input to extract features and produce more sophisticated ones:

$$Conv(Z,k)_{(i,j)} = \sum_{m}^{M} Z_{(n).y(i,j,m)} \quad (3)$$

$$Attention(Q,K,V) = soft\,max\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (4)$$

$$X_{norm} = \frac{X - X_{min}}{Xmin_{max}} \quad (5)$$

Figure 1 shows the basic block diagram.

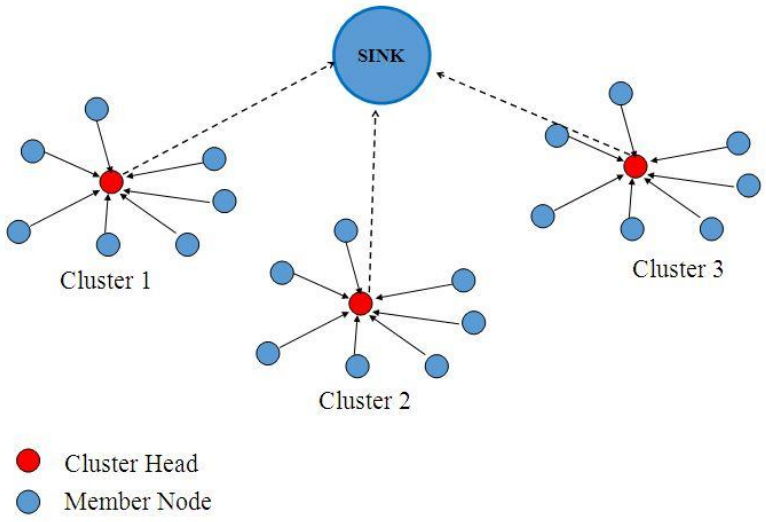

Figure 1: Block diagram

The cluster head also handles network communication and routing within the cluster. It also performs data processing and conservation techniques to reduce energy consumption and extend its lifespan. Cluster2 and Cluster3 are additional clusters within the network, connected to the sink via their respective cluster heads. These clusters work with Cluster1 (the sink's cluster) to efficiently collect and transmit data and ensure network stability:

$$\tau_n^{up}(t) = \frac{\gamma_n i_n(t)}{B\,log_2\left(1+\frac{P_n(t)h_n(t)}{BN_0}\right)} \quad (6)$$

$$E_n^{up}(t) = \frac{P_n(t)\gamma_n i_n(t)}{B\,log_2\left(1+\frac{P_n(t)h_n(t)}{BN_0}\right)} \quad (7)$$

All the components mentioned above work together to achieve efficient data collection and transmission within the wireless sensor network:

$$P(i,j) = \frac{cne(X,Y)}{\sqrt{sd^2(X)sd^2(Y)}} \quad (8)$$

The sink manages and controls the clusters, while the cluster heads coordinate within their clusters to collect and forward data. Member nodes perform their tasks within their clusters and communicate with their cluster head. This cooperation between components helps optimise energy use and maintain network stability in a wireless sensor network.

3.1. Functional Working Model

Cluster heads are high-powered nodes that coordinate and manage communication within a cluster of sensor nodes. Cluster locations refer to the physical placement of cluster heads within the network. These locations are strategically chosen to optimise network coverage and minimise energy consumption:

$$f(G_m) = \sum_{m=1}^{i} f_{out}(L_m) \quad (9)$$

$$f(L_m) = \sum_{n\varepsilon N} f_{in}(n) + \sum_{n\varepsilon N} f_{out}(n) \quad (10)$$

$$f(n) = \sum_{c=1}^{i} f_c(n) + \sum_{d=1}^{i} f_d(n) \quad (11)$$

The base station is the central node in the network that acts as the data sink:

$$f_c(n) = f_{cin}(n) + f_{count}(n) \quad (12)$$

It receives data from the cluster heads and processes it for further analysis:

$$\sum_{n\varepsilon N} b_n \leq \lambda \quad (13)$$

$$b_n \leq B_r/N \quad (14)$$

The base station is also responsible for sending commands and information to the cluster heads. The functional block diagram is presented in Figure 2:

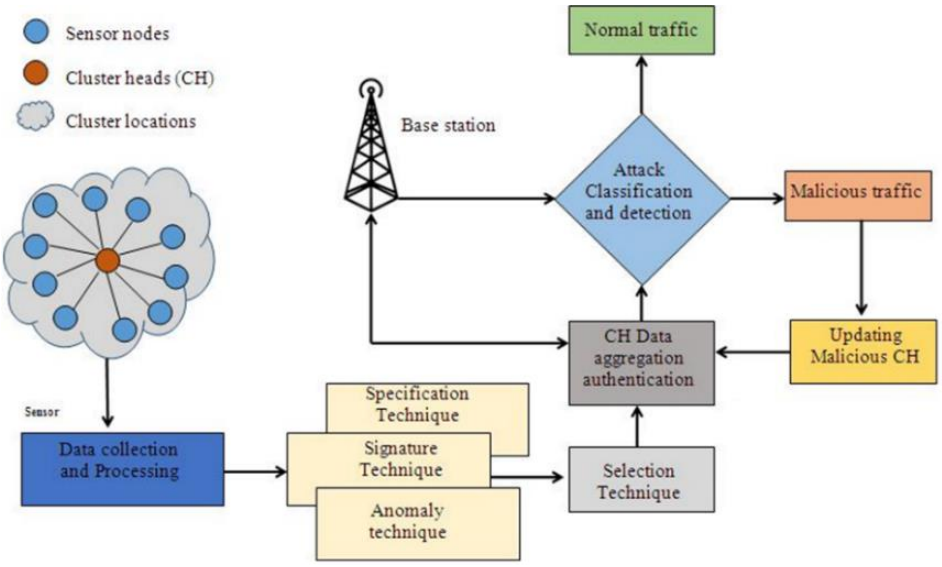

Figure 2: Functional block diagram

It is referred to as normal traffic when sensor nodes send data to the base station in a legitimate manner. This broadcast is governed by a set of rules and used to monitor external factors. Sensor networks can be attacked in various ways. Malicious traffic occurs when unauthorised data is sent, potentially causing the sensor network to stop functioning. These threats may originate from external agents or compromised sensor nodes. After a cluster head is compromised, security measures must be updated to prevent further attacks. This process involves updating the route protocols and changing the authentication keys to prevent the malicious CH from joining the network. Authentication procedures ensure that the data gathered by the cluster heads is accurate and legitimate. They verify the data source and look for any alterations made to it during transmission. At the base station, data from the cluster head is received and processed to extract useful information. Let X be a discrete variable, and the possible outcomes are x1,x2,...,xn, the formal definition of entropy is:

$$H(x) = \sum_{i=1}^{n} p(x_i)\, log_2 \frac{1}{p(x_i)} \quad (15)$$

$$H_\alpha(X) = \frac{1}{1-\alpha} log_2(\sum_{i=n}^{N} p_i(\alpha)) \quad (16)$$

According to the law of large numbers, the entropy rate H(x) of two random processes is the same:

$$H(X) = \lim_{n\to\infty} \frac{1}{n}(x_1, x_2, .., x_n) \quad (17)$$

$$X_m = \frac{x - min(x)}{max(x) - min(x)} \quad (18)$$

Specification methods define rules for what data may be carried in a sensor network. Following these rules and ensuring that all nodes behave accordingly allows for a more secure and usable network. Signature methods use digital signatures to ensure data transfers are genuine and to verify their integrity. This technique uses cryptographic algorithms to assign each data packet a unique signature. This makes it impossible for attackers to fake the data. Anomaly detection techniques search for anomalous trends or behaviours in a sensor network. Selection methods determine which cluster head each sensor node should send its data to. In this process, factors such as distance, energy information, and network activity need to be considered when selecting the best CH for data transfer. As data is generated and captured from multiple devices, it is aggregated, meaning that multiple pieces of data are collected together and summarised before being transferred to the sink node. This reduces the data that needs to be transmitted, therefore saving on power. The aggregated data is then transmitted to the sink node, which acts as a central data collection point:

$$Y_i = f(c_i) \quad (19)$$

$$C_i = \sum v_{ij} Y_i + d_i \quad (20)$$

Now, the activation function is expressed as follows:

$$H\theta(x) = \frac{1}{1 + exp(-\theta^T x)} \quad (21)$$

Where Θ is the parameter cost function:

$$H(m) = \frac{1}{1 + e^{-m}} \quad (21)$$

$$MSE = \frac{1}{n} \sum_{t=1}^{n} e_t^2 \quad (22)$$

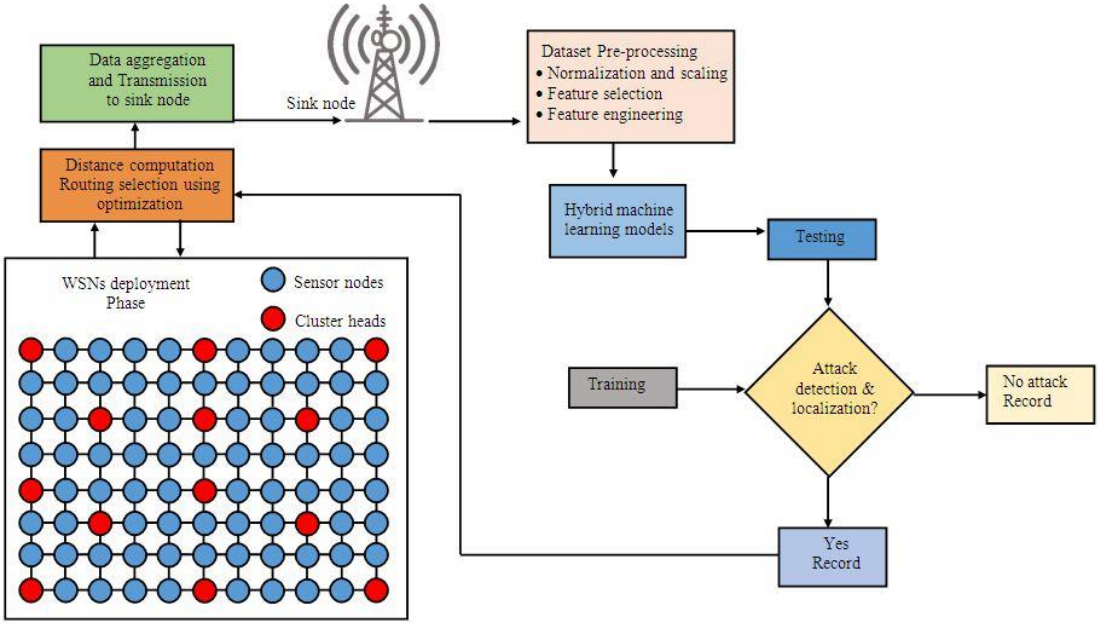

Figure 3: Operational flow diagram

The sink node is responsible for gathering, processing, and storing data received from sensor nodes. This node has a significant amount of energy resources and is connected to the internet for submitting data to a remote server for external processing:

$$RMSE = \sqrt{\frac{1}{n}\sum_{t=1}^{n} e_t^2} \quad (23)$$

Before aggregation and transmission, data have to be preprocessed. Normalising means transforming data so that it falls within a common range, while scaling changes the range of values. These techniques improve the accuracy of data analytics. The operational flow diagram is shown in Figure 3. Sensors could generate a large number of features. Feature selection identifies the most relevant characteristics for the analysis and removes less significant ones. This improves the accuracy of analysis and decision-making. The locations of sensor nodes and the sink node have a profound, but detrimental, effect on data aggregation and transmission. In other words, minimise energy consumption, prolong network lifespan, and achieve high data throughput. Perhaps prediction and decision-making are key in VANET:

$$MAE = \frac{1}{n}\sum_{t=1}^{n}|e_t| \quad (24)$$

$$\alpha_u = \frac{\sum j\varepsilon N_u \tau_j}{N_u} \quad (25)$$

During the deployment phase, sensor nodes are placed strategically to cover the target area and ensure efficient data collection. Wireless sensor network performance is optimised by considering certain factors. These nodes are low-cost and low-power, used to acquire and transfer data to the sink node. These devices are self-powered and use sensors to collect various data streams:

$$\sum_{u\varepsilon U} x_u \leq R \quad (26)$$

$$F(x) = z + \rho C(x) \quad (27)$$

The data is tested for integrity and accuracy after aggregation and transmission. This involves comparing the received data with the original data sent by the sensor nodes to detect abnormalities. Training is the process of using collected data to build an ML model to improve results. This streamlines pattern recognition and improves forecasting precision. WSNs are vulnerable to various attack vectors, including data tampering, denial-of-service attacks, and others. To detect and localise attacks, anomaly and intrusion detection techniques are employed. Such a process guarantees the protection of the wireless sensor network and preserves the collected data for later analysis. Otherwise, if there are no attacks, that data is used unmodified for future analysis. It helps maintain data accuracy and consistency for decision-making.

4. Result and Discussion

The proposed DLFWSN (Deep Learning Framework for Wireless Sensor Networks) has been compared with the existing IDLTM (Improved Deep Learning Traffic Management), SFWN (Security Framework for Wireless Networks) and WSNAML (Wireless Sensor Network Anomaly Detection). Here, the WSN traffic dataset is used, and the Python simulator is used to execute the results [31].

4.1. Energy Consumption

The performance of the proposed model will be evaluated using energy consumption as the parameter. This will ensure the framework efficiently implements energy conservation, boosting the overall performance and lifetime of the WSN. Table 2 shows the comparison of Energy consumption between the existing and proposed models.

Table 2: Comparison of energy consumption (in %)

Authors	Model	No. of Inputs				
		100	**200**	**300**	**400**	**500**
Yao et al. [1]	IDLTM	65.53	67.20	69.14	71.15	73.79
Karthikeyan et al. [2]	SFWN	70.81	71.93	72.33	74.28	75.06
Kavitha et al. [4]	WSNAML	79.22	82.19	83.74	85.71	82.68
Proposed Model	DLFWSN	88.05	89.32	91.20	92.48	83.94

Figure 4 illustrates the comparative analysis of energy consumption among sensor nodes. The proposed DLFWSN achieved an energy consumption rate of 83.94% in computational terms.

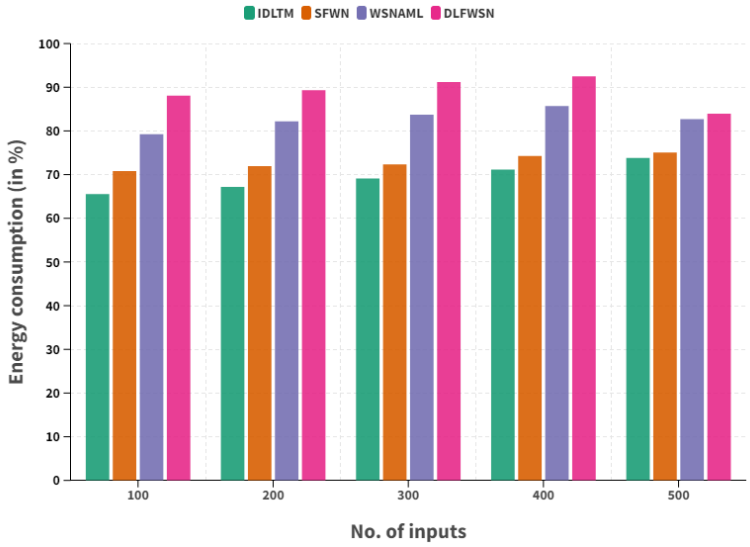

Figure 4: Comparison of energy consumption

The current IDLTM achieved an energy consumption rate of 73.79%, while SFWN recorded 75.06% and WSNAML recorded 82.68%.

4.2. Data Confidentiality

Data confidentiality, an important parameter, is a key factor in the success of a proposed framework for sensitive traffic in high-density WSNs. Sensitive traffic data is vulnerable to cyber threats and unauthorised access, so robust encryption and access controls must be employed to protect it. Figure 5 shows the comparison of Data confidentiality between existing and proposed models.

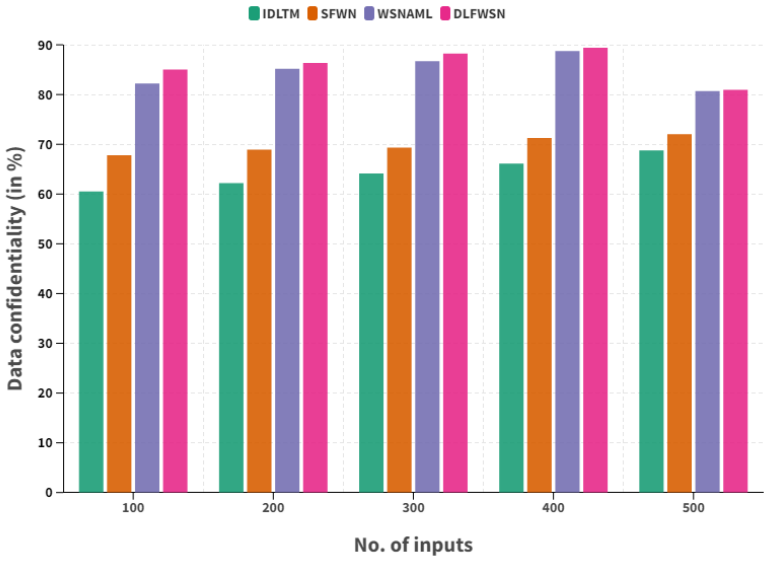

Figure 5: Comparison of data confidentiality

Figure 5 illustrates the comparative analysis of data confidentiality among sensor nodes. The proposed DLFWSN achieved a data confidentiality rate of 80.95% from a computational perspective (Table 3). The current IDLTM achieved a data confidentiality rate of 68.77%, SFWN attained 72.04%, and WSNAML reached 80.69%.

Table 3: Comparison of data confidentiality (in %)

Authors	Model	No. of Inputs				
		100	200	300	400	500
Yao et al. [1]	IDLTM	60.53	62.20	64.14	66.12	68.77
Karthikeyan et al. [2]	SFWN	67.81	68.93	69.35	71.29	72.04
Kavitha et al. [4]	WSNAML	82.21	85.18	86.73	88.75	80.69
Proposed Model	DLFWSN	85.05	86.34	88.26	89.40	80.95

4.3. Scalability

The scalability parameter would investigate whether the security architecture is sufficiently robust to handle a large amount of sensitive traffic in a high-density WSN.

Table 4: Comparison of scalability (in %)

Authors	Model	No. of Inputs				
		100	200	300	400	500
Yao et al. [1]	IDLTM	55.52	57.27	59.19	61.11	63.77
Karthikeyan et al. [2]	SFWN	62.84	63.98	64.34	66.22	67.07
Kavitha et al. [4]	WSNAML	85.25	88.18	89.74	81.76	82.69
Proposed Model	DLFWSN	83.02	84.35	86.26	87.41	89.95

This will ensure the architecture can scale to larger structures while maintaining its efficacy and performance. Table 4 compares the scalability of the existing and proposed models. Figure 6 illustrates the comparative analysis of sensor node scalability.

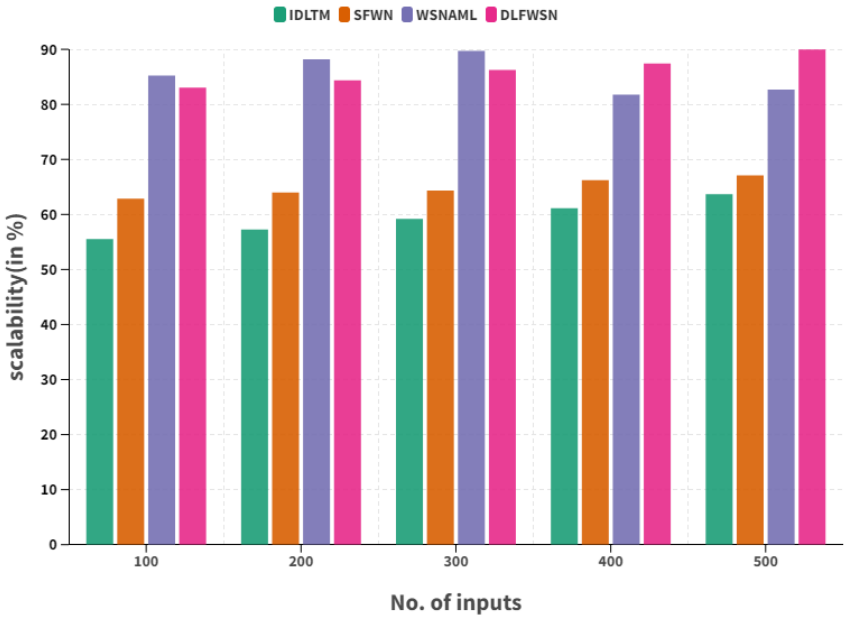

Figure 6: Comparison of scalability

The proposed DLFWSN achieved a scalability of 89.95% from a computational perspective. The current IDLTM achieved a scalability of 63.77%, SFWN achieved 67.07%, and WSNAML achieved 82.69%.

4.4. Communication Overhead

Communication latency is one of the most significant parameters to analyse in any security framework, especially in high-density WSNs.

Table 5: Comparison of communication overhead (in %)

Authors	Model	No. of Inputs				
		100	200	300	400	500
Yao et al. [1]	IDLTM	50.50	52.22	54.14	56.18	58.79
Karthikeyan et al. [2]	SFWN	60.85	61.93	62.31	64.23	65.07
Kavitha et al. [4]	WSNAML	88.25	91.19	82.73	84.75	85.64
Proposed Model	DLFWSN	81.06	82.30	84.21	89.41	92.97

In the enhanced deep learning-based approach, overhead can be evaluated in terms of network latency, data packet collisions, and energy consumption due to additional communication between nodes. Table 5 compares the communication overhead between the existing and proposed models. Figure 7 illustrates the comparison of communication overhead for sensor nodes.

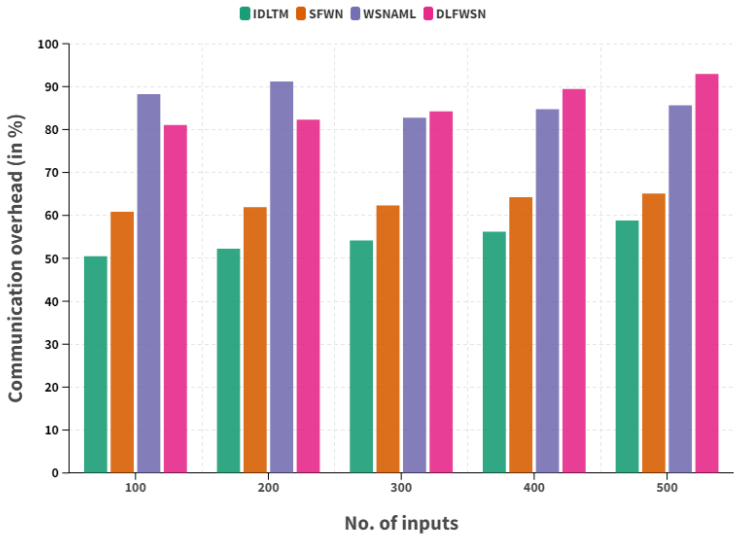

Figure 7: Comparison of communication overhead

The proposed DLFWSN achieved a communication overhead of 92.97% from a computational perspective. The current IDLTM achieved 58.79%, SFWN 65.07%, and WSNAML 85.64% in terms of communication overhead.

5. Conclusion

The suggested security framework based on deep learning makes it much easier to handle sensitive traffic in high-density Wireless Sensor Networks (WSNs). In today's WSN systems, sensor nodes constantly exchange large amounts of data, increasing the risk of cyberattacks, data breaches, and other malicious activities. To solve these problems, the proposed framework uses powerful deep learning methods to detect unusual patterns in network behaviour and spot problems in real time. The system uses smart learning methods to make it easier to spot suspicious behaviour, prevent unauthorised access, and ensure data is sent securely over the network. The framework's main goal is to improve various aspects of WSN security, including energy efficiency, data privacy, scalability, and communication overhead. Resource management is crucial in WSNs, as sensor nodes often have limited battery life and processing power. The suggested model reduces processing overhead and optimises resource use, making it a good choice for networks with heavy traffic and limited resources. As a result, the framework keeps the network stable and well protected against potential attacks.

The proposed method performs well in experiments, achieving 83.94% energy efficiency, 80.95% data secrecy, 89.95% scalability, and 92.97% optimisation of communication overhead. These results show that the model not only makes the network safer but also improves its overall performance. The framework ensures reliable communication in dense WSN deployments by balancing security measures with efficient network operation. This study makes a significant difference in keeping sensitive data safe in WSNs by providing a robust, smart security architecture. It helps develop more advanced security plans for critical applications, including healthcare monitoring, environmental surveillance, military systems, and smart infrastructure. Future work can further improve this framework by adding adaptive learning models, real-time threat

intelligence, and large-scale investigations of real-world deployments, thereby making WSNs more resilient and reliable in complex operating environments.

Acknowledgment: N/A

Data Availability Statement: The authors affirm that the data supporting this study on a deep learning–driven security framework for managing sensitive traffic in high-density wireless sensor networks are included within the paper, and additional details can be made available upon reasonable request.

Funding Statement: The authors declare that no external financial support or funding was received for conducting this research or preparing the manuscript.

Conflicts of Interest Statement: The authors collectively state that there are no conflicts of interest related to this work, and all referenced materials have been appropriately acknowledged.

Ethics and Consent Statement: The authors confirm that ethical guidelines were strictly followed, with necessary approvals obtained from relevant organisations and informed consent obtained from all participants involved in the data collection process.

References

1. C. Yao, Y. Yang, K. Yin, and J. Yang, "Traffic anomaly detection in wireless sensor networks based on principal component analysis and deep convolution neural network," *IEEE Access*, vol. 10, no. 9, pp. 103136–103149, 2022.
2. M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm-based WSN-IoT security enhancement with machine learning for intrusion detection," *Scientific Reports*, vol. 14, no. 1, p. 231, 2024.
3. T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev, and Z. Ahmad, "A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids," *IEEE Access*, vol. 12, no. 7, pp. 91715–91733, 2024.
4. T. Kavitha, N. Pandeeswari, R. Shobana, V. R. Vinothini, K. Sakthisudhan, A. Jeyam, and A. J. G. Malar, "Data congestion control framework in wireless sensor network in IoT-enabled intelligent transportation system," *Measurement: Sensors*, vol. 24, no. 12, p. 100563, 2022.
5. S. Godala and M. S. Kumar, "A weight optimized deep learning model for cluster-based intrusion detection system," *Optical and Quantum Electronics*, vol. 55, no. 14, p. 1224, 2023.
6. N. M. S. Kumar, E. Suryaprabha, and K. Hariprasath, "Machine learning-based hybrid model for energy-efficient secured transmission in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 2, pp. 887-902, 2022.
7. G. Kaur and D. Kakkar, "Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET," *Ad Hoc Networks*, vol. 136, no. 11, p. 102961, 2022.
8. K. Radhakrishnan, D. Ramakrishnan, O. I. Khalaf, M. Uddin, C. L. Chen, and C. M. Wu, "A novel deep learning-based cooperative communication channel model for wireless underground sensor networks," *Sensors*, vol. 22, no. 12, p. 4475, 2022.
9. S. Nelavalli, R. R. Dondeti, N. Gottimukkala, and S. R. Samudrala, "Balancing energy efficiency with robust security in wireless sensor networks using deep reinforcement learning-enhanced particle swarm optimization," *Telecommunications and Radio Engineering*, vol. 84, no. 1, pp. 9–26, 2025.
10. A. Duraisamy, M. Subramaniam, and C. R. R. Robin, "An optimized deep learning based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities," *Studies in Informatics and Control*, vol. 30, no. 2, pp. 121–131, 2021.
11. O. Ahmed, "Enhancing intrusion detection in wireless sensor networks through machine learning techniques and context awareness integration," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, no. 8, pp. 244–258, 2024.
12. S. B. Balasubramanian, P. Balaji, A. Munshi, W. Almukadi, T. N. Prabhu, K. Venkatachalam, and M. Abouhawwash, "Machine learning based IoT system for secure traffic management and accident detection in smart cities," *PeerJ Computer Science*, vol. 9, no. 3, p. e1259, 2023.
13. T. Mahmood, J. Li, T. Saba, A. Rehman, and S. Ali, "Energy optimized data fusion approach for scalable wireless sensor network using deep learning-based scheme," *Journal of Network and Computer Applications*, vol. 224, no. 4, p. 103841, 2024.

14. Z. A. Khan, S. Amjad, F. Ahmed, A. M. Almasoud, M. Imran, and N. Javaid, "A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks," *IEEE Access*, vol. 11, no. 3, pp. 31036–31051, 2023.
15. Y. Y. Ghadi, T. Mazhar, T. A. Shloul, T. Shahzad, U. A. Salaria, A. Ahmed, and H. Hamam, "Machine learning solution for the security of wireless sensor network: A review," *IEEE Access*, vol. 12, no. 1, pp. 12699–12719, 2024.
16. D. Kalpana and P. Ajitha, "A hybrid heuristic-assisted deep learning for secured routing and malicious node detection in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 17, no. 5, pp. 2758–2780, 2024.
17. Q. N. Naveed, H. Alqahtani, R. U. Khan, S. Almakdi, M. Alshehri, and M. A. A. Rasheed, "An intelligent traffic surveillance system using integrated wireless sensor network and improved phase timing optimization," *Sensors*, vol. 22, no. 9, p. 3333, 2022.
18. F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation-based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0," *IEEE Access*, vol. 12, no. 3, pp. 34800–34819, 2024.
19. S. Srinivasan, M. S. Vinmathi, S. N. Sivaraj, A. Karthikayen, C. Alakesan, and M. Preetha, "A novel approach integrating IoT and WSN with predictive modelling and optimization for enhancing efficiency and sustainability in smart cities," *Journal of Electrical Systems*, vol. 20, no. 4s, pp. 2228–2237, 2024.
20. B. Raveendranadh and S. Tamilselvan, "An accurate attack detection framework based on exponential polynomial kernel-centred deep neural networks in the wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 3, p. e4726, 2023.
21. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16492–16503, 2021.
22. A. Asha, R. Arunachalam, I. Poonguzhali, S. Urooj, and S. Alelyani, "Optimized RNN-based performance prediction of IoT and WSN-oriented smart city application using improved honey badger algorithm," *Measurement*, vol. 210, no. 3, p. 112505, 2023.
23. R. Arunachalam and E. D. R. Kanmani, "Detection and mitigation of vampire attacks with secure routing in WSN using weighted RNN and optimal path selection," *Computers & Security*, vol. 145, no. 10, p. 103991, 2024.
24. W. Ding, "A GAN-based security strategy for WSN networks based on honeypot algorithm," *Physical Communication*, vol. 62, no. 2, p. 102260, 2024.
25. F. Alrowais, R. Marzouk, M. K. Nour, H. Mohsen, A. M. Hilal, I. Yaseen, M. I. Alsaid, and G. P. Mohammed, "Intelligent intrusion detection using arithmetic optimization enabled density-based clustering with deep learning," *Electronics*, vol. 11, no. 21, p. 3541, 2022.
26. B. Meenakshi and D. Karunkuzhali, "Enhancing cyber security in WSN using optimized self-attention-based provisional variational auto-encoder generative adversarial network," *Computer Standards & Interfaces*, vol. 88, no. 3, p. 103802, 2024.
27. A. Jain, T. Mehrotra, A. Sisodia, S. Vishnoi, S. Upadhyay, A. Kumar, C. Verma, and Z. Illés, "An enhanced self-learning-based clustering scheme for real-time traffic data distribution in wireless networks," *Heliyon*, vol. 9, no. 7, p. e17530, 2023.
28. S. Rameshkumar, R. Ganesan, and A. Merline, "Progressive transfer learning-based deep Q network for DDOS defence in WSN," *Computer Systems Science & Engineering*, vol. 44, no. 3, pp. 2379–2394, 2023.
29. S. Khatri, H. Vachhani, S. Shah, J. Bhatia, M. Chaturvedi, S. Tanwar, and N. Kumar, "Machine learning models and techniques for VANET-based traffic management: Implementation issues and challenges," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1778–1805, 2021.
30. S. M. S. Bukhari, M. H. Zafar, M. A. Houran, S. K. R. Moosavi, M. Mansoor, M. Muaaz, and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability," *Ad Hoc Networks*, vol. 155, no. 3, p. 103407, 2024.
31. W. B. Kasasbeh, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *Kaggle*, 2022, [Accessed by 12/12/2024].