Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 1 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i01.50953

PAPER

Enhancing Cybersecurity in Wireless Sensor Networks: Innovative Framework for Optimized Data Aggregation

Rakesh Kumar Godi[1], Vikranth Bhoothpur[2], Bhanushree K J[3], Ambika B J[4](✉), Naveen Chandra Gowda[5]

[1]Department of Computer Science, School of Computer Sciences, Central University of Karnataka, Kalaburagi, Karnataka, India

[2]CVR College of Engineering, Hyderabad, Telangana, India

[3]Department of Computer Science and Engineering, Bangalore Institute of Technology, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

[4]Department of Computer Science and Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, Karnataka, India

[5]School of Computer Science and Engineering, REVA University, Bengaluru, Karnataka, India

ambika.bj@manipal.edu

ABSTRACT

The various cyberattacks in wireless sensor networks (WSNs) have made confidentiality and data integrity as crucial principles in data aggregation. Therefore, several applications are presented to control the sharing of data and information as well as the associated cybersecurity aspects that must be preserved during data transfer. Most cybersecurity breaches that occur these days are categorized as cyberattacks. The WSN's resource-constrained architecture makes cybersecurity lapses and insider attacks possible. This study proposes a novel technique named multi-objective pigeon-inspired optimal long short-term memory (MPI-OLSTM) networks to develop the data aggregation in cybersecurity model. Initially, the WSN-detection systems (WSN-DS) dataset is collected and pre-processed using min-max normalization. For extracting features, the principal component analysis (PCA) is employed. The model's predictive power is assessed using the following metrics: accuracy (96.5%), precision (92.3%), and recall (90.4%). The findings demonstrate that, in comparison to existing techniques, our approach yielded more accurate results.

KEYWORDS

cybersecurity, wireless sensor networks (WSNs), data aggregation, data transfer, cyberattack

1 INTRODUCTION

In recent years, wireless sensor networks (WSNs) have gathered significant researcher attention, encouraging a need for complete exploration and in-depth understanding of the domain. As we know, WSNs include a limited number of sensor devices collaborating to execute tasks such as data transmission, environmental sensing, and decision-making [1]. Due to the numerous ways in which these sensors might be attacked, data security is becoming more and more crucial. There are a lot of sensor nodes in the WSNs with limited resources because of their design. WSNs might be vulnerable to various threats [2]. Maintaining transmitted data secure and unaffected by unauthorized access is the goal of cybersecurity. Unauthorized access

Godi, R.K., Vikranth, B., Bhanushree, K.J., Ambika, B.J., Gowda, N.C. (2025). Enhancing Cybersecurity in Wireless Sensor Networks: Innovative Framework for Optimized Data Aggregation. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(1), pp. 151–164. https://doi.org/10.3991/ijoe.v21i01.50953

Article submitted 2024-07-06. Revision uploaded 2024-09-09. Final acceptance 2024-09-09.

to data is caused by lax security protocols. Inappropriate access to sensitive data might have more costly effects for an Internet of Things (IoT)-using organization. Strong authentication, data encryption, monitoring tools, and other methods are some of the ways to prevent unwanted access [3]. The cybersecurity issues associated with WSN's open characteristics make it simpler for an attacker and intruder to access the network during network connections along with information transmission. When used as a general security technique, anomaly detection can quickly identify clues that point to the presence of malicious data modification and unauthorized data interceptions during transmission [4]. The qualified medical practitioner is given the text data for remote diagnosis when it has been authenticated [5]. The transmission of medical text data across an open communication channel makes it quite vulnerable to cybersecurity and privacy breaches. [6] This paper tries to analyze many of the available cyberattack datasets and compare them with many of the fields that are used to detect and predict cyberattack, such as the IoT traffic-based, network traffic-based, cyber-physical system, and web traffic-based. [7] This study paper presents novel and effective solution for predicting denial-of-service (DoS) and DDoS attacks in network security scenarios is presented in this work by employing an effective model, called CNN-LSTM-XGBoost, which is an innovative hybrid approach designed for intrusion detection in network security. [8] The objective of this review paper was to determine the documented security risks that are related to the use of graphical passwords, together with the measures that have been taken to prevent them. The study identifies several critical issues related to cybersecurity with respect to WSNs. Due to resource constrained architecture, there is chance of cyber-attacks. The study identifies the need for robust data aggregation methods that maintains integrity and confidentiality in highly vulnerable environments. This work develops the data aggregation cybersecurity model utilizing deep learning (DL) networks and suggests a unique method called multi-objective pigeon-inspired optimal long short-term memory (MPI-OLSTM), which aims to improve the predictive accuracy, precision, and recall in detecting cyber-attacks within WSNs. The proposed model also introduces innovative techniques for data preprocessing and feature extraction, further contributing to the robustness and efficiency of the cyber-security system.

The paper's sections are as follows: Section 2 offers a review of the literature and a presentation, along with a detailed explanation of the recommended technique, which are provided in Section 3. Discussion of experimental datasets and simulation findings are in Section 4. Section 5 concludes the study and offers suggestions for more research.

2 LITERATURE REVIEW

The research presented in [9] introduces a feature selection technique, termed rule-based particle swarm optimization (RBPSO), which integrates PSO and fuzzy neuro-genetic classification algorithm (FNGCA) for enhancing WSN security. Meanwhile, [10] explores the application of machine learning (ML) techniques in IoT for smart city development. [11] investigates node behavior assessment, trust level evaluation, and abnormal node identification to combat selection forwarding attacks. The authors in [12] introduce hierarchical chimp optimization (HChOA) for multi-hop routing and clustering tasks. Additionally, [13] proposes a novel authentication method for secure data connection in multi-gateway IoT-enabled WSNs.

The authors in [14] suggest an intrusion detection system (IDS) utilizing ML architectures and integrated secure medium access control (MAC) principles. [15] addresses a cybersecurity multi-class classification issue for attack detection, focusing on multi-node data censoring. [16] presents a strategy for clustering quality of service (QoS) based on trust for secure data transport. [17] compares ML classification techniques for WSN cyber-attack detection. Authors in [18] introduce the fuzzy analytical hierarchy process (AHP) for enhancing security control analysis. Authors in [19] propose ANT particle swarm optimization ad hoc on-demand distance vector (ANTPSOAODV) for safe information gathering. [20] evaluates network aspects and recommends information aggregation using a male lion optimization algorithm (DA-MOMLOA). Finally, [21–28] devises the safe aggregation and transmission scheme (SATS) for secure and lightweight data transmission.

3 PROPOSED WORK

The suggested cybersecurity system utilizes a hybrid model combining both DL and ML techniques. Figure 1 depicts the architecture of the proposed system.

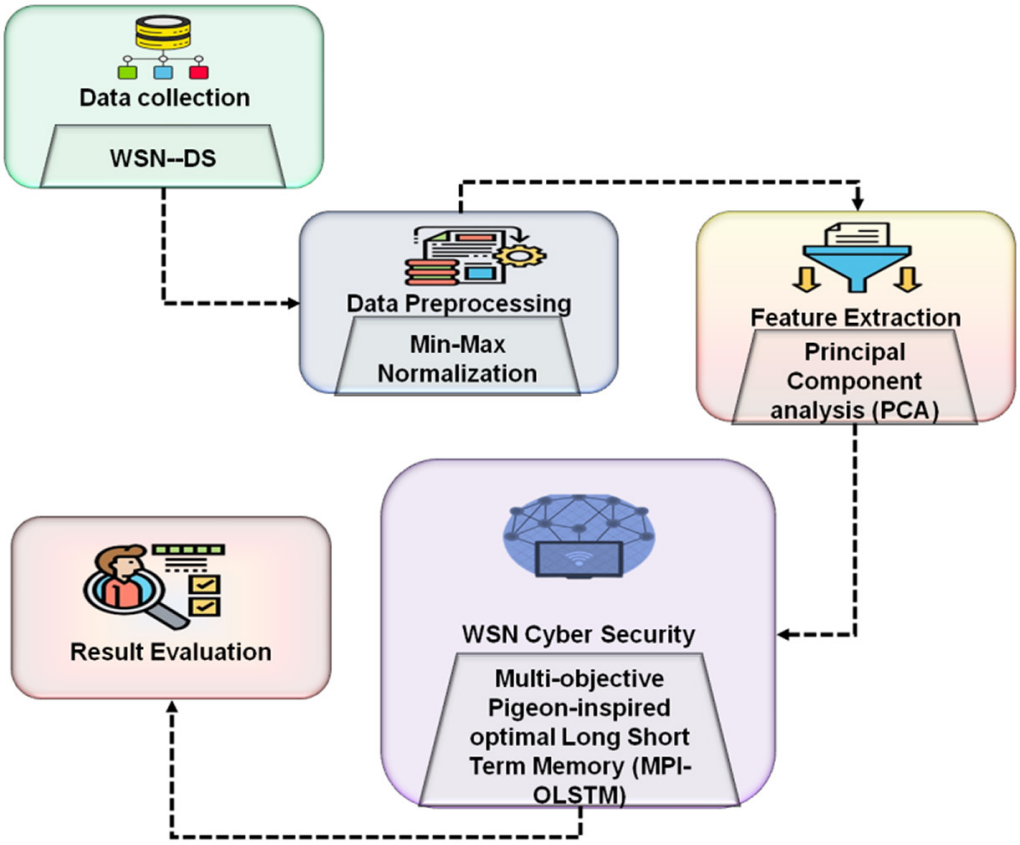

Fig. 1. Proposed system structure

The flowchart for the proposed cybersecurity system using the MPI-OLSTM algorithm follows the steps in Figure 2:

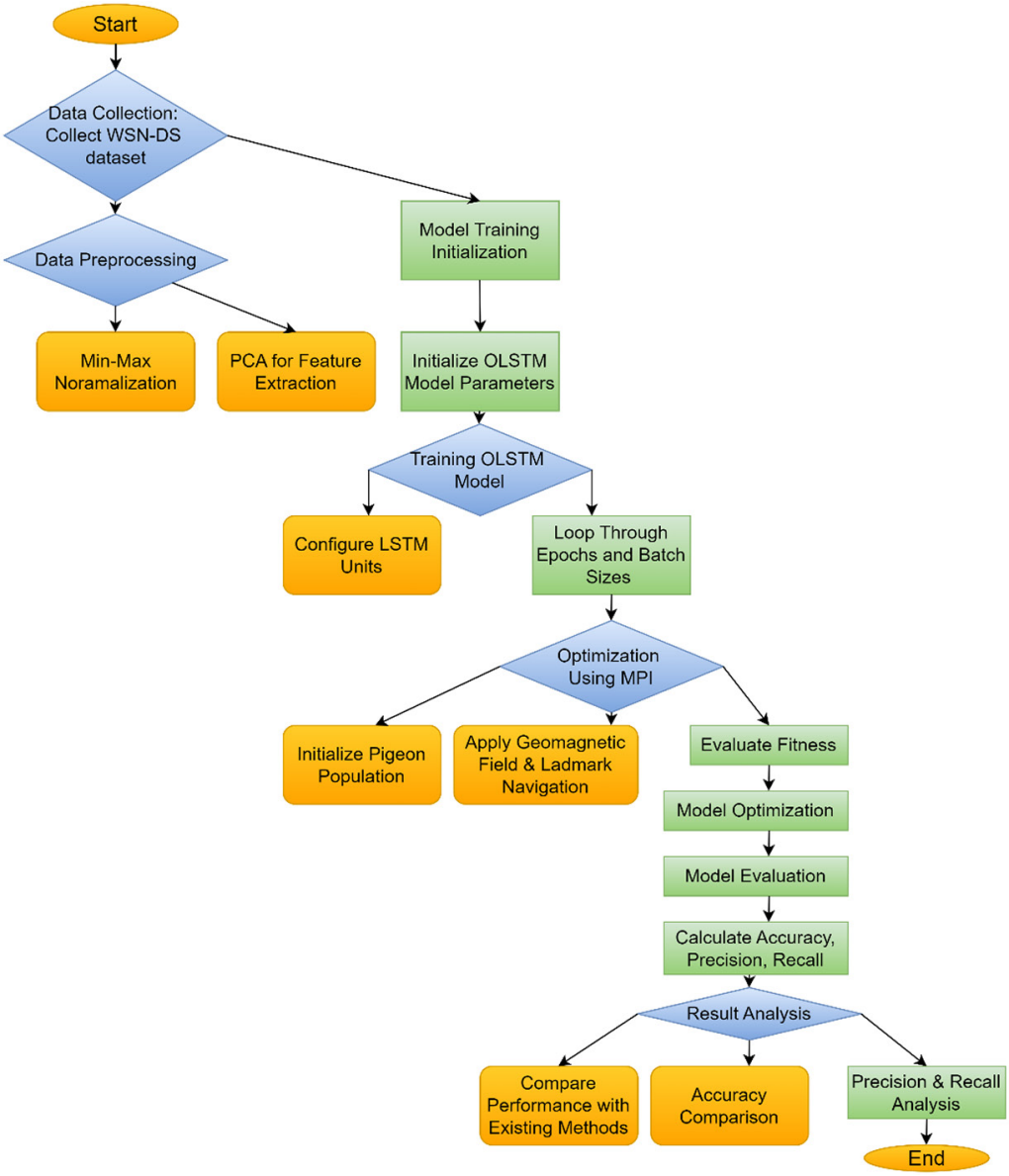

Fig. 2. Flowchart of the multi-objective pigeon-inspired optimal long short-term memory (MPI-OLSTM) algorithm

3.1 Data collection

The dataset utilized in this study, WSN-detection systems (WSN-DS), is specifically designed for WSNs employing hierarchical clustering architectures. Insider attacks manifest in four distinct forms: flooding, TDMA scheduling, black hole, and gray hole. In a gray hole attack, cluster heads (CHs) deliberately or randomly discard segments of communication packets before transmitting them to a base station (BS), constituting a form of DoS attack. Black hole attacks involve malicious CHs discarding all packets destined for the BS, effectively obstructing communication, also categorized as DoS attacks. Flooding occurs when malevolent nodes

masquerade as CHs and continuously transmit signals, depleting the energy of neighboring sensors. Malicious CHs may utilize TDMA scheduling to assign multiple cluster members to the same time slot, leading to packet collisions and subsequent data loss.

Table 1. Summary of dataset

Type of Data	Group	Volume	Percentage (%)	Total
The initial unbalanced dataset	Gray hole	340,066	90.77	374,661
	Normal	14,596	3.90	
	Flooding	6,638	1.77	
	Black hole	10,049	2.68	
	Scheduling	3,312	0.88	
Balanced Dataset Extracted	Normal	13,000	50	26,000
	Black hole	3,250	12.5	
	Gray hole	3,250	12.5	
	Flooding	3,250	12.5	
	Scheduling	3,250	12.5	

For our simulations, we created a balanced dataset by extracting a representative subset from the original WSN-DS dataset, which contained 374,661 samples, as detailed in Table 1. In this balanced version, there are 3,250 samples for each of the four types of attacks, along with the standard samples, resulting in a total of 26,000 data points. Balancing the dataset was crucial to prevent bias during model training and ensure the model's ability to detect all types of attacks with equal effectiveness.

3.2 Data preprocessing using min-max normalization

Min-max normalization, also referred to as min-max scaling, involves adjusting the range of initial data linearly. This straightforward technique ensures that the data is accurately scaled to fit within a predefined range. Normalization is vital in ML models, particularly in neural networks, as it prevents any feature from dominating due to its larger scale, thereby improving model convergence and stability during training. Employing the min-max normalization method, as described by equation (1).

$$A' = \left(\frac{A - \min value of\ A}{Max} \right) * (D - C) + C \tag{1}$$

In the context where A' represents a set of min-max normalized data, the predefined boundaries $[C, D]$ should be used if A represents the original data range and D is the specific data point being considered.

3.3 Utilizing principal component analysis for feature extraction

Principal component analysis (PCA) is a feature extraction technique aimed at reducing the dimensionality of data while preserving variance information. Its primary objective is to identify correlations between data points and eliminate those with strong correlations, thereby reducing dimensionality. This process ultimately decreases the number of input features, leading to a reduction in model parameters and improved computational efficiency. PCA was particularly chosen for this study due to its ability to enhance the training speed of the DL model and reduce overfitting by eliminating redundant features. PCA involves several key stages, starting with data standardization. This stage ensures that all data points fall within the same range to prevent significant errors caused by outliers. The standardization formula, represented by equation (2), is as follows:

$$W_{new} = \frac{W_j - \mu}{\sigma} \tag{2}$$

The next stage in PCA is the calculation of the covariance matrix, which helps determine the correlations between data points. Equation (3) represents the covariance matrix.

$$Cov = \begin{bmatrix} Cov_{11} & Cov_{12} & \dots & Cov_{1N} \\ Cov_{21} & Cov_{22} & \dots & Cov_{1N} \\ \vdots & \vdots & \dots & \vdots \\ Cov_{N1} & Cov_{N1} & \dots & Cov_{NN} \end{bmatrix} \tag{3}$$

3.4 Classification using multi-objective pigeon-inspired optimal long short-term memory

The objective of this study is to devise a model aimed at safeguarding sensor-level WSN in data security, facilitating both sensor authentication during communication and the protection of gathered information from cyber threats. The researchers focused on WSN cybersecurity, identifying prevalent WSN attacks and establishing cybersecurity requirements tailored for WSN to achieve their objective. They specifically examined WSN applications in agricultural contexts and explored the utilization of public key infrastructure alongside symmetric and asymmetric cryptography in constructing their model. Through the integration of MPI-OLSTM, they aimed to enhance WSN cybersecurity while ensuring robust data protection and efficient network performance.

Optimal long short-term memory. In the fundamental process of DL, the aim is to minimize the error function between the computed value and the actual value. This involves deeply training the weight parameter matrix and bias parameter across numerous neural networks. Each parameter's loss function requires computation, incurring significant computational costs. The gradient descent approach is commonly employed to address the gradient issue, simplifying the computation process by converting the global gradient solution into a local gradient solution. Figure 3 depicts the optimal structure of OLSTM. OLSTM technology has led to substantial advancements in various domains such as natural language processing, image description, and speech recognition.

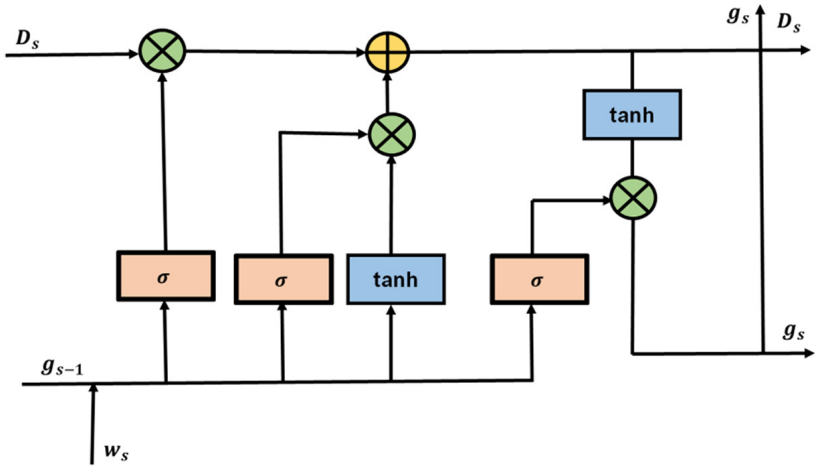

Fig. 3. Optimal long short term structure

The primary function of the forgetting gate is to control the weight of the internal self-recurrent connection. Its activation function, typically a tanh function, ensures that the weight parameter remains between 0 and 1, maintaining the same output shape for the previous internal state Ct–1. The input gate, also referred to as the memory gate, is responsible for identifying the current memory state. It is utilized to pointwise multiply with the output of the forgetting gate to obtain the previous memory state. By combining the forgetting gate and the memory gate, the subsequent hidden state value, represented by the output gate, is determined. The update technique for the internal recurrent state in an OLSTM is expressed through equations (4), (5), (6), (7), and (8).

$$e_s = \sigma\left(a_e + \sum V_e w_s + \sum X_e g_{s-1}\right) \tag{4}$$

$$h_s = \sigma\left(a_h + \sum V_h w_s + \sum X_h g_{s-1}\right) \tag{5}$$

$$r_s = \sigma\left(a_p + \sum V_p w_s + \sum X_p g_{s-1}\right) \tag{6}$$

$$D_s = e_s D_{s-1} + \tanh\left(a + \sum V_j w_s + \sum X_j g_{s-1}\right) h_s \tag{7}$$

$$g_s = \tanh\left(D_s\right) r_s \tag{8}$$

Equation (4) represents the relationships between various variables in the OLSTM model. Specifically, it denotes the current input as w_s , while the hidden states at time t and (S–1) are denoted by g_s and g_{s-1} respectively. The forgetting gate is represented by e_s, the input gate by h_s, and the output gate by r_s. The weight variables in the self-recurrent connection are denoted by V, X, and A. The hyperbolic tangent activation function is represented by tanh(.), while the sigmoid activation function is denoted by σ(.).

Algorithm 1: OLSTM

Import library
Load dataset
Dataset should be normalized to values between 0 and 1
Configure the optimization, lstm units, input and output units.
For *epochs and batch_size* ***do***
    Train the LSTM network
End for
Make security
Calculate root mean squared error

Multi-objective pigeon-inspired optimization. The program is constructed based on the distinct homing behavior of pigeon flocks, aiming to simulate their navigational patterns to discover optimal solutions to optimization problems. Pigeons rely on three key reference variables for their navigation: (1) the sun's position, influencing their ability to navigate and determine homing direction; (2) the geomagnetic field, detected through a magnetic induction architecture in their upper beaks, guiding their flight direction; and (3) topographical landmarks, which expedite homing when present in the terrain.

Algorithm 2: MPI

1. ***Input:*** *OLSTM Model Parameters*
2. ***Output:*** *Optimized Model Parameters*
3. ***Steps:***
   - *Initialize a population of pigeons with random positions and velocities.*
   - *Apply geomagnetic field and landmark navigation rules as defined by equations (9) to (14).*
   - *Evaluate the fitness of each pigeon based on the model performance.*
   - *Update pigeons' positions and velocities iteratively to converge towards optimal parameters.*
   - *Return the optimized model parameters.*

Pigeon flocks utilize two primary methods for homing navigation, employing various navigational aids depending on flying conditions. They rely on the geomagnetic field to determine direction and utilize prominent landmarks as indicators when nearing their destination. Equations (9), (10), (11), (12), (13), and (14) represent these navigational principles.

$$U_j^M = U_j^{M-1} * f^{-RN} + rand\left(W_H - W_j^{M-1}\right) \tag{9}$$

$$W_j^M = W_j^{M-1} + U_j^M \tag{10}$$

$$W_D^M = \frac{\sum_{j=1}^{N^{(M)}} W_j^M E\left(W_j^M\right)}{N^{(M)} \sum_{j=1}^{N^{(M)}} E\left(W_j^M\right)} \tag{11}$$

$$W_j^M = W_J^{M-1} + rand\left(W_D^{M-1} - W_j^{M-1}\right) \tag{12}$$

$$E(W_j^M) = \begin{cases} \dfrac{1}{fitness\left(W_j^M\right) + \varepsilon}, min - os \\ fitness\left(W_j^M\right), \max - os \end{cases} \tag{13}$$

$$N^{(M)} = \frac{N^{(M-1)}}{2} \tag{14}$$

Establish a pigeon group in D-dimensional space with M individuals; $X_i = \left(X_i^1, X_i^2, X_i^3, \ldots, X_i^N\right)$ XiN represents the location of the ith ($i = 1, 2, 3, \ldots, M$) bird in the population; the function fitness X_i^N represents the pigeon's fitness, whereas NMAX1 and NMAX2 denote the geomagnetic compass and landmark operators, respectively, and $V_i = \left(V_i^1, V_i^2, V_i^3, \ldots, V_i^N\right)$ represent the ith pigeon's speed. The geomagnetic compass operator is fundamental for every pigeon in the system. It relies on a center point, denoted as a landmark, which follows the Nth iteration and is represented by the parameter XNC. The fitness function is denoted by A. The number of remaining pigeons

after the Nth iteration is denoted by B. There are two distinct approaches for solving the problem: Max-os (maximum ideal solution) and Min-os (minimum optimal solution). When the NMAX2 iteration is reached in the loop, the landmark operator ceases operation and reports the most effective solution that has been modified up to that point.

4 RESULT AND DISCUSSION

In the experimental setup, the evaluation of the proposed MPI-OLSTM algorithm was conducted on Windows 10, which serves as the operating system, while MATLAB R2017b is executed on an Intel i5 CPU with 16 GB of RAM. The evaluation involves comparing the MPI-OLSTM algorithm with existing methods such as support vector machine (SVM) [20] and decision tree (DT) [20]. Parameters under consideration include accuracy, precision, and recall concerning the quantity of active and inactive nodes, as outlined in Table 2.

Table 2. Numerical outcomes of classification methods

Methods	Accuracy (%)	Precision (%)	Recall (%)
SVM [20]	65.95	67.50	69.85
DT [20]	77.89	75.37	78.59
MPI-OLSTM [Proposed]	96.5	92.3	90.4

Accuracy is a measure of how well a measurement reflects the true, known value. It quantifies the agreement between multiple measurements of the same object. It is calculated by dividing the number of accurate predictions by the total number of predictions made. Figure 4 displays the accuracy rates for both the suggested and existing methods. The proposed classifier achieved the highest classification accuracy at 96.5%, surpassing the performance of the two existing algorithms, SVM (65.95%) and DT (77.89%). This demonstrates the superior accuracy of the MPI-OLSTM method.

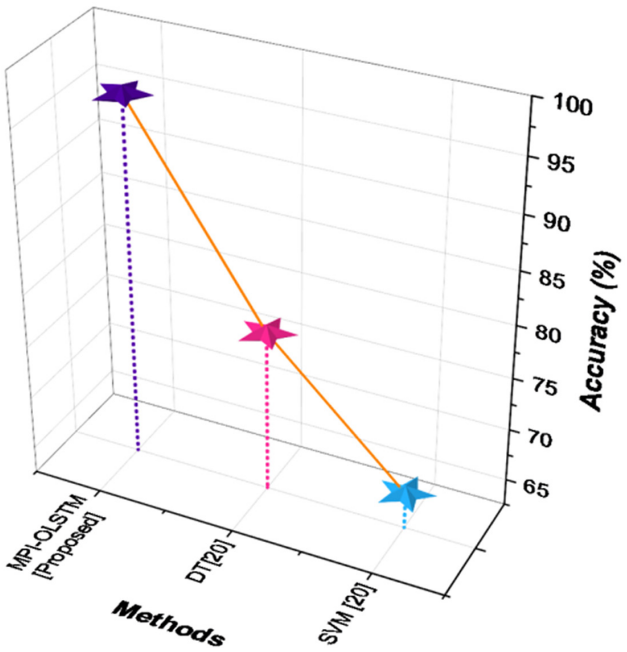

Fig. 4. Comparison of the accuracy

Precision refers to the ability of a value to convey information based on its digits, indicating the degree of agreement between multiple measurements. Figure 5 compares the precision analysis of the suggested and existing approaches. The MPI-OLSTM method proposed achieved a precision of 92.3%, outperforming the SVM and DT methods, which achieved 67.50% and 75.37% respectively.

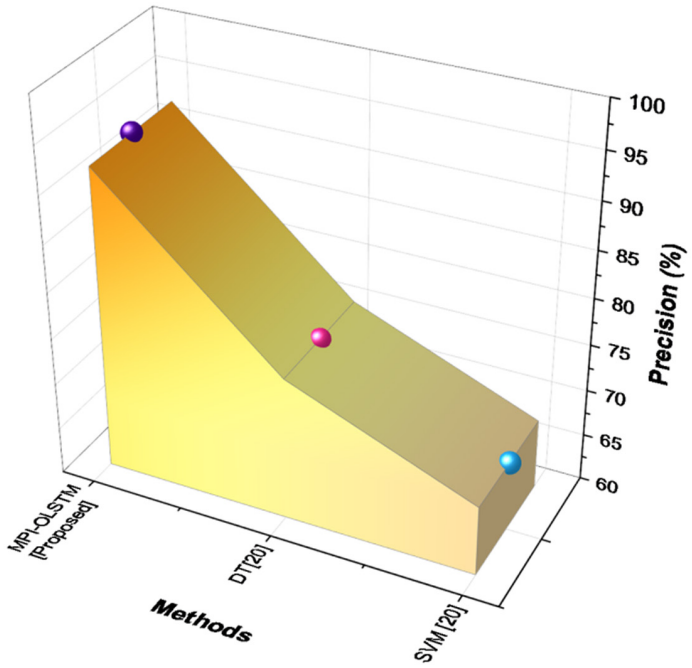

Fig. 5. Comparison of the precision

Recall, also known as the positive predictive coefficient, represents the ratio between the total number of positive predictions and the true positive (TP) values. Figure 6 presents a comparison of recall between the recommended and existing techniques. The MPI-OLSTM method proposed achieved a recall of 90.4%, surpassing the recall values of other existing methods. Specifically, the SVM and DT methods obtained recall values of 69.85% and 78.59%, respectively.

The algorithm's capability to predict correctly depends on high accuracy. The high precision reflects how MPI-OLSTM efficiently minimizes false positives by improvising the reliability of the detection system. MPI-OLSTM effectively identifies attacks due to a high recall rate.

The improved performance of MPI-OLSTM has shown major implications wherein it proposes improved performance in cybersecurity by facilitating a more reliable solution for detecting and mitigating cyber insider attacks in WSNs, hence improving network security and decreasing cyberattack risks. The operational efficiency is achieved due to high precision and recall by reducing false positives, improving detection in critical attacks, which speeds up threat response.

MPI-OLSTM overcomes existing methods such as SVM and DT in several ways. While SVMs struggle with complex, high-dimensional data and large datasets. MPI-OLSTM, which utilizes DL and optimization techniques, handles these challenges more effectively. DTs often suffer from overfitting and may not perform well with large, complex datasets. In contrast, MPI-OLSTM's capability to learn complicated patterns and optimized parameters offers a more robust and adaptable solution.

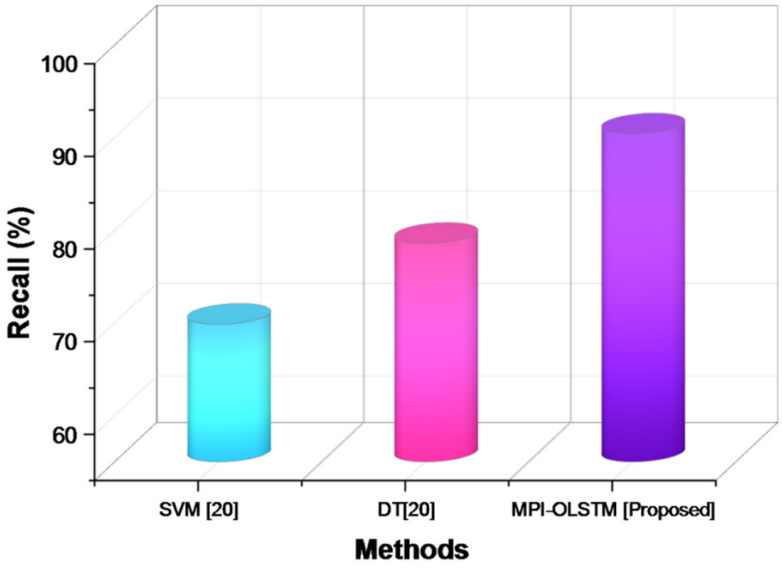

Fig. 6. Comparison of the recall

5 CONCLUSION

This paper has suggested a unique data cybersecurity method called MPI-OLSTM to protect data aggregation in WSNs. The suggested method makes use of MPI-OLSTM to provide more data in less time. The suggested system performs comparably to other comparable systems in terms of processing time and energy consumption, indicating its applicability for safeguarding information aggregation. The outcomes of MPI-OLSTM included achieving accuracy (96.5%), precision (92.3%), and recall (90.4%). The created secure protocol has applications in the military, including border cybersecurity, enemy line surveillance, and WSNs that are made up of several sensor nodes that are utilized in vital infrastructures such as the electricity, water, and communication industries. The outcomes demonstrate the approach's potential and show improvements in WSN lifetime, dependability, and efficiency. Future research could extend MPI-OLSTM to IoT and smart city applications, enhance real-time detection, and improve scalability. Integrating technologies such as blockchain and optimizing efficiency will further strengthen the model.

6 REFERENCES

[1] A. S. Sadeq, A. Hafizah Mohd Aman, R. Hassan, and H. Sallehudin, "Quantitative evaluation of IEEE 802.15.4 and ISA 100.11a for large scale wireless sensor network," in *2021 3rd International Cyber Resilience Conference (CRC)*, 2021, pp. 1–5. https://doi.org/10.1109/CRC50527.2021.9392403

[2] C. Khosa, T. Mathonsi, D. D. Plessis, and T. Tshilongamulenzhe, "Improved encryption algorithm for public wireless network," *Journal of Advances in Information Technology (JAIT)*, vol. 15, no. 2, pp. 233–244, 2024. https://doi.org/10.12720/jait.15.2.233-244

[3] G. Latif, J. Alghazo, and Z. Kazmi, "Security enabling for IoT and wireless sensor network-based data communication," in *Advanced Wireless Communication and Sensor Networks*, 2023, pp. 181–195. https://doi.org/10.1201/9781003326205-16

[4] P. Kaur, K. Kaur, K. Singh, and S. Kim, "Early Forest fire detection using a protocol for energy-efficient clustering with weighted-based optimization in wireless sensor networks," *Applied Sciences*, vol. 13, no. 5, p. 3048, 2023. https://doi.org/10.3390/app13053048

[5] Y. Rajkumar and S. V. N. S. Kumar, "A lightweight privacy preserving distributed certificate-less aggregate based mutual authentication scheme for vehicular adhoc networks," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 1442–1466, 2024. https://doi.org/10.1007/s12083-024-01636-8

[6] F. A. Al-zubidi, A. K. Farhan, and M. E. El-Kenawy, "Surveying machine learning in cyberattack datasets: A comprehensive analysis," *Journal of Soft Computing and Computer*, vol. 1, no. 1, 2024. https://doi.org/10.70403/3008-1084.1000

[7] A. F. Al-zubidi, A. K. Farhan, and S. M. Towfek, "Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model," *Journal of Intelligent Systems*, vol. 33, no. 1, p. 20230195, 2024. https://doi.org/10.1515/jisys-2023-0195

[8] Z. M. Saadi, A. T. Sadiq, Z. O. Akif, and A. K. Farhan, "A survey: Security vulnerabilities and protective strategies for graphical passwords," *Electronics*, vol. 13, no. 15, p. 3042, 2024. https://doi.org/10.3390/electronics13153042

[9] S. Subramani and M. Selvi, "Comprehensive review on distributed denial of service attacks in wireless sensor networks," *International Journal of Information and Computer Security*, vol. 20, nos. 3–4, pp. 414–438, 2023. https://doi.org/10.1504/IJICS.2023.128828

[10] A. J. Varma *et al.*, "A roadmap for SMEs to adopt an AI based cyber threat intelligence," in *The Effect of Information Technology on Business and Marketing Intelligence Systems*, M. Alshurideh, B. H. Al Kurdi, R. Masa'deh, H. M. Alzoubi, and S. Salloum, Eds., Cham: Springer, 2023, vol. 1056, pp. 1903–1926. https://doi.org/10.1007/978-3-031-12382-5_105

[11] H. Wang, "Machine learning-based centralized link coding attack detection in software-defined network," *Wireless Networks*, vol. 30, pp. 6641–6655, 2024. https://doi.org/10.1007/s11276-023-03483-6

[12] Y. Yang, Y. Wu, H. Yuan, M. Khishe, and M. Mohammadi, "Nodes clustering and multi-hop routing protocol optimization using hybrid chimp optimization and hunger games search algorithms for sustainable energy efficient underwater wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 35, p. 100731, 2022. https://doi.org/10.1016/j.suscom.2022.100731

[13] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for intelligent IoT-enabled WSNs," *Computers and Electrical Engineering*, vol. 105, p. 108495, 2023. https://doi.org/10.1016/j.compeleceng.2022.108495

[14] R. Soundararajan, M. Rajagopal, A. Muthuramalingam, E. Hossain, and J. Lloret, "Interleaved honeypot-framing model with secure MAC policies for wireless sensor networks," *Sensors*, vol. 22, no. 20, p. 8046, 2022. https://doi.org/10.3390/s22208046

[15] R. Liang, S. Zhang, W. Zhang, G. Zhang, and J. Tang, "Nonlocal hybrid network for long-tailed image classification," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 20, no. 4, pp. 1–22, 2024. https://doi.org/10.1145/3630256

[16] S. Mehrotra, A. Sharan, and N. Varish, "Improving search result clustering using nature inspired approach," *Multimedia Tools and Applications*, vol. 83, pp. 62971–62988, 2024. https://doi.org/10.1007/s11042-023-18067-x

[17] S. Hariharasitaraman, R. Yadav, and P. Agrawal, "Some insights of cyber physical systems in the context of the tourism and travel industry," in *Handbook of Research on Data Science and Cybersecurity Innovations in Industry 4.0 Technologies*, T. Murugan and E. Nirmala, Eds., IGI Global Scientific Publishing, 2023, pp. 357–379. https://doi.org/10.4018/978-1-6684-8145-5.ch018

[18] S. Tayyaba *et al.*, "Skin insertion analysis of microneedle using ANSYS and fuzzy logic," *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 5, pp. 5885–5895, 2020. https://doi.org/10.3233/JIFS-179676

[19] N. Chandnani and C. N. Khairnar, "Quality of service (QoS) enhancement of IoT WSNs using an efficient hybrid protocol for data aggregation and routing," *SN Computer Science*, vol. 4, 2023. https://doi.org/10.1007/s42979-023-02165-6

[20] R. Shakila and B. Paramasivan, "Retraction note to: An improved range-based localization using whale optimization algorithm in underwater wireless sensor network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. S1, p. 3, 2023. https://doi.org/10.1007/s12652-022-03913-x

[21] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment," *Computer Networks*, vol. 195, p. 108219, 2021. https://doi.org/10.1016/j.comnet.2021.108219

[22] N. C. Gowda, S. S. Manvi, and A. Bharathi Malakreddy, "Blockchain-based access control model with privacy preservation in a fog computing environment," in *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2022, pp. 1–6. https://doi.org/10.1109/CONECCT55679.2022.9865845

[23] L. Shalini, S. S. Manvi, B. Gardiner, and N. C. Gowda, "Image based classification of COVID-19 infection using ensemble of machine learning classifiers and deep learning techniques," in *2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 2022, pp. 1–6. https://doi.org/10.1109/ICDSAAI55433.2022.10028859

[24] N. C. Gowda *et al.*, "TAKM-FC: Two-way authentication with efficient key management in Fog Computing Environments," in *The Journal of Supercomputing*, vol. 80, pp. 6855–6890, 2024. https://doi.org/10.1007/s11227-023-05712-3

[25] S. S. Manvi and N. C. Gowda, "Trust management in fog computing," in *Applying Integration Techniques and Methods in Distributed Systems and Technologies*, G. Kecskemeti, Ed., IGI Global, 2019, pp. 34–48. https://doi.org/10.4018/978-1-5225-8295-3.ch002

[26] N. C. Gowda and A. Bharathi Malakreddy, "A trust prediction mechanism in edge communications using optimized support vector regression," in *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023, pp. 784–789. https://doi.org/10.1109/ICCMC56507.2023.10083686

[27] A. A. Ka'Bi, "Enhancement of energy harvesting efficiency in mobile wireless sensor networks," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2021, pp. 0137–0142. https://doi.org/10.1109/UEMCON53757.2021.9666602

[28] G. Vembu and D. Ramasamy, "Optimized deep learning-based intrusion detection for wireless sensor networks," *International Journal of Communication Systems*, vol. 36, no. 13, p. e5254, 2023. https://doi.org/10.1002/dac.5254

7 AUTHORS

Dr. Rakesh Kumar Godi received the B.E., MTech. and Ph.D. degrees from the VTU University, Karnataka. He is currently associated with the Department of Computer Science, Central University of Karnataka, Kalaburgi, Karnataka, India. He has teaching experience of more than twelve years. He has been published more than 30 research papers in international and national journals/conferences. His research interests include wireless networks, biomedical signal processing, simulation modelling, ensemble machine learning and artificial intelligence. He is a reviewer of many international journals and conferences (E-mail: rakeshgodi@cuk.ac.in).

Vikranth Bhoothpur is currently working as Professor, Department of Computer Science and Engineering, at CVR College of Engineering, Hyderabad, India. His research interests include parallel computing run-times, deep learning and cyber security (E-mail: b.vikranth@cvr.ac.in).

Dr. Bhanushree K J received the B.E., M Tech. and Ph.D. degrees from the VTU University, Karnataka. She is currently working as an Associate Professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India. She has teaching experience of more than 15 years. She has been published more than 16 research papers in international and national journals/conferences. Her research interests include digital image processing, machine learning and artificial intelligence. She is a reviewer of many international journals and conferences (E-mail: kjbhanushree@bit-bangalore.edu.in).

Ambika B J is an Assistant Professor in the Senior Scale at the Department of Computer Science and Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India. With 13 years of teaching experience across various institutions and universities in Karnataka, India, she has established herself as a dedicated educator and researcher in the field of computer science. Her research interests span a broad spectrum of contemporary topics including computer networks, big data, cloud computing, artificial intelligence (AI), and machine learning (ML). Her passion for advancing knowledge in these areas is reflected in her prolific academic output, having published more than 16 articles in reputed journals and conferences. She is a Life Member of ISTE, CSI (E-mail: ambika.bj@manipal.edu).

Naveen Chandra Gowda received his Doctorate in Computer and Information Sciences from Vishveswaraya Technological University, Belgaum, and Karnataka. He is currently working as an assistant professor in the School of CSE, REVA University, Bengaluru. He has more than 14 years of experience in teaching and research. He has published around 30 papers in National and International journals and presented at national conferences. He is also the reviewer for six International Journals and National and International conferences. He has presented various keynote talks in workshops organized around India. He is a Life Member of ISTE, CSI and ACM (E-mail: ncgowdru@gmail.com).