Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INTRUSION DETECTION APPROACH IN WIRELESS SENSOR NETWORK SECURITY THROUGH CNN-BI-LSTM MODEL

JIMSHA K MATHEW[1], KAVITHA NAIR R[2], B. KALPANA[3], MUTHULAKSHMI ARUMUGASAMY[4], S. SHARANYAA[5]

[1]Assistant Professor, Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bengaluru, Karnataka

[2]Assistant Professor, Department of Artificial Intelligence and Machine Learning, Acharya Institute of Technology, Bengaluru, Karnataka

[3]Associate Professor, Department of Computer Science and Engineering, R.M.D Engineering College, Kavaraipettai, Chennai

[4]Assistant Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai

[5]Assistant Professor, Department of Information Technology, Panimalar Engineering College, Chennai

ABSTRACT

Wireless Sensor Networks (WSNs) face growing safety threats, necessitating robust intrusion detection systems to safeguard network integrity. This research introduces a comprehensive framework for intrusion detection in WSNs, addressing the vulnerabilities inherent in these networks. The proposed approach integrates key techniques, namely data preprocessing through normalization, feature extraction utilizing Particle Swarm Optimization (PSO), and classification employing Convolutional Neural Networks and Bidirectional Long Short-Term Memory (CNN-Bi-LSTM).The framework commences with meticulous data preprocessing, wherein raw sensor data from the WSN undergoes normalization. This crucial step standardizes feature scales, ensuring data consistency and refining interpretability. Subsequently, the PSO algorithm is applied for feature selection, optimizing the identification of relevant features. By minimizing redundancy and maximizing the discriminative power of the feature set, PSO significantly enhances intrusion detection capabilities.The selected features serve as input for the CNN-Bi-LSTM model, a powerful combination leveraging CNN's spatial feature extraction and Bi-LSTM's temporal modelling. CNN captures high-level spatial representations from the input features, while Bi-LSTM effectively captures temporal dependencies in sequential sensor readings. This synergy equips the framework to discern complex intrusion patterns with heightened accuracy.Performance evaluation, conducted using labelled datasets, demonstrates the superior efficacy of the integrated framework compared to other intrusion detection methods. The experimental results underscore the framework's remarkable ability to achieve enhanced intrusion detection performance in WSNs, solidifying its significance in advancing the security paradigm for these critical networks.

Keywords **-** *Intrusion Detection, Wireless Sensor Networks, Convolutional Neural Networks, Bidirectional Long Short-Term Memory, Particle Swarm Optimization*

1. INTRODUCTION

WSNs have become an essential piece of technology in many fields, revolutionizing how data is gathered and used [1]. A WSN is made up of a number of little, independent sensor nodes that are capable of wireless communication, processing, and sensing. In order to monitor and collect data about physical or environmental conditions like temperature, humidity, pressure, and the presence of specific substances, these nodes collaborate. WSNs have a number of benefits over conventional wired sensor networks, including quick deployment, scalability, and affordability.

Numerous industries, including environmental monitoring, healthcare, agriculture, industrial automation, smart cities, and disaster management, are among the many fields in which they are used. Real-time data acquisition, analysis, and decision-making are made possible by WSNs, which improve productivity, resource management, and situational awareness [2]. The sensor nodes are the basic components of a WSN [3]. These nodes are frequently compact, low-power gadgets that can wirelessly communicate with other nodes in the network while also sensing the outside world. Each node has a wireless transceiver for communication, a microcontroller or microprocessor, memory, a power source (typically batteries), and one or more sensors. In a WSN, sensor nodes typically communicate with one another using wireless protocols like Zigbee, Bluetooth, or Wi-Fi. Depending on the needs of the application, the nodes create an ad hoc or hierarchical network topology [4]. Ad-hoc networks use direct communication between nodes, whereas hierarchical networks use clusters of nodes that have a hierarchical structure to facilitate efficient data aggregation and routing.

The limited resources of individual sensor nodes, including processing power, memory, energy, and communication bandwidth, are one of the main problems in WSNs [5]. Because of these limitations, developing effective algorithms, protocols, and techniques is essential for enhancing network performance and extending network life. Another crucial component of WSNs is security. These networks are sensitive due to the distributedand wireless nature, including Denial-of-Service attacks, unauthorized access, data tampering, and eavesdropping. It is crucial to safeguard the availability, confidentiality, and integrity of data processed and transmitted by WSNs, especially in applications that deal with sensitive data [6]. WSNs are more common than ever in a variety of industries, such as industrial automation, healthcare, and environmental monitoring [7]. These networks are made up of lots of little, inexpensive sensor nodes working together to collect and send data to a central location for processing. However, because of their wireless nature and distributed deployment, WSNs are susceptible to security risks like malicious attacks, unauthorized access, and data tampering. It is essential to use effective Intrusion Detection System (IDS) capable of identifying and mitigating potential threats in order to ensure the integrity and dependability of data transmitted through WSNs [8]. Traditional IDS methods frequently rely on manually developed features and rule-based strategies, which may find it difficult to keep up with the constantly changing nature of attacks and have high false positive rates. Figure 1 shows the Intrusion Detection System in WSN.

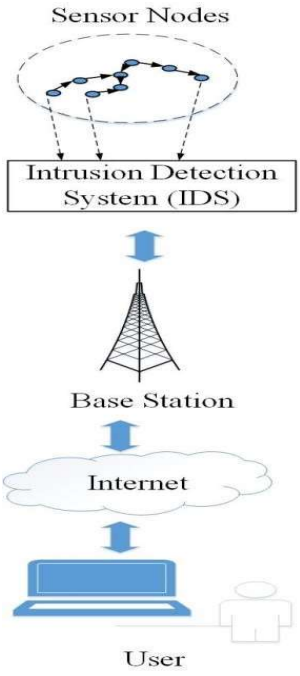

Figure 1: WSN's Surveillance System for Intrusions

Effective security measures are now essential given the explosive growth of interconnected computer networks and the growing reliance on digital systems [9]. IDS are essential for defending computer networks against malicious activity and unapproved access. An IDS is a security tool that tracks user activity, system events, and network traffic in order to spot potential intrusions and security breaches and take appropriate action. An IDS's main objective is to find suspicious or malicious activity that deviates from a system's or networks expected norms. An IDS can detect and raise alerts for suspicious activities like port scanning, unauthorized access attempts, malware infections, and data exfiltration by continuously monitoring network traffic and system logs [10]. Security administrators can take appropriate action, reduce risks, and stop further damage when such intrusions are discovered early. Powerful deep learning architectures like CNN and Bi-LSTM networks have transformed manyindustries, including time-series analysis, natural language processing, and computer vision [11]. These models have proven to be remarkably

adept at identifying intricate dependencies and patterns in data, which makes them particularly useful for tasks like sentiment analysis, image recognition, and sequential data processing. CNNs are a subclass of neural networks that are particularly adept at analyzing data with a structured grid structure, like images or time-series data [12]. They are built with a number of convolutional layers to automatically learn and extract hierarchical representations from raw input. CNNs can effectively distinguish between various classes or categories by applying filters and pooling operations to the data to capture spatial features and patterns [13]. Recurrent Neural Networks (RNNs) with Bi-LSTM networks have the ability to recognize long-term dependencies and sequential patterns in data. Traditional RNNs are limited in their ability to accurately model long-term dependencies due to the vanishing or exploding gradient problem.

Deep learning algorithms in particular have achieved outstanding results in a number of fields recently. As a result, researchers are now focused on utilizing these methods to increase the security of WSNs. CNNs and Bi- LSTM networks have shown promise as intrusion detection models for WSNs in this context [14]. The ability of CNNs to identify spatial and temporal patterns in data is well known. They are well suited for analyzing sensor data because they excel at automatically learning hierarchical representations from unstructured input. CNNs are able to identify typical and abnormal network behavior by extracting pertinent features from sensor readings using convolutional layers, pooling operations, and non-linear activation functions. Sequential data's long-term dependencies and temporal dynamics have been successfully captured by Bi-LSTM networks. They have the capacity to process information both forward and backward, allowing them to simultaneously capture context from previous and upcoming time steps. Bi-LSTM networks are especially useful for detecting complex intrusion patterns in WSNs because of their bidirectional nature, where the temporal order of events is crucial. In this study, the advantages of CNNs and Bi-LSTM networks are combined to propose an approach for detecting intrusions in WSNs [15]. Therefore to increase the precision and robustness of intrusion detection systems, the method makes use of the spatial and temporal characteristics of sensor data. The model successfully distinguishes between typical network behavior and potential intrusions by integrating CNN layers to extract spatial features and Bi-LSTM layers to model temporal dependencies.

The proposed intrusion detection framework exhibits notable adaptability to the distinctive characteristics of Wireless Sensor Networks (WSNs). In acknowledging the resource constraints prevalent in WSNs, such as limited power and processing capacity, the framework employs efficient algorithms for data preprocessing and feature extraction. This adaptability ensures that the intrusion detection system remains optimized for the unique challenges posed by WSN environments. Moreover, the dynamic nature of WSNs, marked by variable network conditions, is effectively addressed by the framework's flexibility, enabling it to operate reliably even when confronted with changes in network topology or environmental conditions over time. A critical aspect of the proposed method lies in its optimized feature selection process. By leveraging the Particle Swarm Optimization (PSO) algorithm, the framework systematically reduces redundancy and selects only the most relevant features for intrusion detection. This optimization not only streamlines the computational complexity of the system but also enhances its discriminative power. The result is a more efficient intrusion detection framework that can accurately distinguish between normal network behavior and potential security threats.

Furthermore, the integration of Convolutional Neural Networks (CNN) for spatial feature extraction and Bidirectional Long Short-Term Memory (Bi-LSTM) for temporal modeling addresses inherent limitations in previous models. Traditional methods often struggle to capture complex spatial patterns in sensor data, a challenge addressed by the CNN's capability to extract high-level spatial representations. Simultaneously, the Bi-LSTM facilitates effective modeling of temporal dependencies in sequential sensor readings. This comprehensive approach ensures that the intrusion detection system can discern intricate spatial and temporal patterns, overcoming previous limitations and significantly enhancing its ability to detect sophisticated intrusion scenarios within WSNs.

The key contributions of the article are highly significant and impactful in the field of intrusion detection for Wireless Sensor Networks (WSNs).

- The proposed framework's utilization of PSO algorithm for selecting features and data normalization as a preprocessing step brings

an innovative approach to enhance the model's input data quality and relevance.

- The integration of Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) models for feature extraction is a novel and powerful combination. The CNN excels in capturing spatial patterns, while the Bi-LSTM effectively captures temporal dependencies, enabling the model to understand complex and dynamic relationships within the WSN data.
- The experimental results validating the integrated framework's superior intrusion detection performance on labeled datasets provide concrete evidence of its effectiveness. Outperforming existing methods, the framework showcases its potential to enhance network security, making it a valuable contribution to the advancement of intrusion detection techniques in WSNs.

The rest of the essay is structured as follows: The reviews of related work for intrusion detection in WSNs are given in Section 2. Problem statement details are provided in Section 3. The methodology is presented in Section 4, which also describes the proposed CNN-Bi-LSTM model's architecture. The results are presented and examined in Section 5. Section 6 concludes the essay and describes possible future lines of inquiry in this area.

2. RELATED WORKS

Jin [16] elaborates that the attacks detection equipment has become extensively employed in conventional WSN circumstances as an efficient barrier to security technological advances. The WSN information flow alsoincreases quickly, and different malware and assaults start to show up, along with the swift growth of WSN networks and WSN network applications. A Multicorrelation-based security detection framework for WSN with LSTM that utilizes the temporal correlation properties of the getting identification dataset. The LSTM WSN component receives the TAM matrix as input and uses it for both training and testing after the model chooses the best feature component employing the data supplied by the achieve selected features component, and does so. The development of a WSN IDS model integrating two-way LSTM WSN and C5.0 classifier has been suggested and addressed the issues of less precision rates associated with conventional ML based WSN ID algorithms used in the ID process. The algorithm first extracts the features from the security breach detection collection using the hidden component and then it feeds the characteristics retrieved into the C5.0 algorithm for training and categorization. The research project chooses three distinct sets of information as the test data sets and runs simulations to analyses simulation achievement with the goal to demonstrate the practicality of the model. According to results from experiments, the model performed more effectively in classifying data.

Yang et al. [17] demonstrates that the volume of data being gathered has greatly increased as a consequence of current IoT changes, which has increased the need for storage of information, computational resources, and immediate analysis capabilities. IoT development has generally benefited greatly from computing in the cloud. On the other hand, because of its improved accessibility, location consciousness, variation, flexibility, minimal latency, and geographical spread, fog technology is just beginning to develop as an emerging discipline that complements the use of the cloud. Nevertheless, since they are accessible and exchanged connected devices are susceptible to malicious attacks. As an outcome, several security frameworks for connected devices built around computing with fog have already been created. An IDS -based distributed framework makes sure the availability of a changing, expandable IoT system that can allocate centralized tasks to nearby fog node devices and effectively recognizes sophisticated criminal activity. It looked at the time-associated components of traffic data from networks in the present research. A traffic information classification malware detection simulation for the UNSW-NB15 comparisons dataset that depends on a two-layered Bi-LSTM with a mechanism for focus. In respect to the recommended approach superior to a number of cutting-edge Connect IDS that utilized ML models.

Ling et al. [18] offers the approach which presents the initial integrity of ICSs has been undermined as a result of the advancement of networked and computer innovations, and security issues have risen to the fore. For ICSs, operational methods to detect intrusions have been put forth. Deep learning-based intrusion detection techniques, including and gated recurrent units, have lately greatly increased the recognition rate in comparison to older techniques. Nevertheless, issues like decreasing gradients and poor training effectiveness still need to be resolved. So, the research suggested

a BiSRU-based intrusion detection technique. The SRU neural network's optimized bidirectional framework can solve the issue of disappearing gradients and increase training efficiency by using skip connections. The model makes use of two common commercial information sets from Mississippi State University. The findings demonstrate that the suggested approach can be more precise and takes less time to train compared to alternative approaches.

Pustokhina et al. [19] states that the amount of multimedia information, which accumulates on a scale of zettabytes to petabytes, has increased exponentially in the past few years . Network, which is located Internet, and organizational security problems are all growing concurrently. In big data surroundings like this, finding attacks is not any simpler. Numerous models were able to recognize unidentified attacks despite the fact that multiple kinds of IDS have already been provided for a variety of connecting assaults. For effective results, large-scale big data analysis is now using DL strategies. According to this point of view, the article introduces a new DL based HPS- CBL approach to identifying intrusions in big data surroundings, which combines a CNN with Bi-LSTM. The amount of multimedia information, which accumulates on a scale of zettabytes to petabytes, has increased exponentially in the past few years. Network, which is located Internet, and organizational security problems are all growing concurrently. In a big data surroundings like this, finding attacks is not any simpler. Numerous models were able to recognize unidentified assaults despite the fact that various types of IDS have already been provided for a variety of connecting assaults. For effective results, large-scale big data analysis is now using DL strategies. According to this point of view, the article introduces a new DL based HPS-CBL approach to identifying intrusions in big data surroundings, which combines a CNN with Bi-LSTM.

Tamil Selvi and Visalakshi [20] describes that a wide range of industries, which includes farming, the armed forces, medical care, tracking, and monitoring, use WSN. The use of WSNs is growing every day as the web and embedded technology advance. Protection of data in WSN is difficult, though, and there are more and more variations of attacks. The evaluation and identification of attacks like DoS, detection of anomalies, and black hole are carried out by conventional detection of intrusions techniques. The eliminate attack, which is a unique assault on the software layer, has never been addressed by conventional techniques. Targeting internet websites and programmes, a particular DA types in the program's layer. It turns into challenging to recognize different DA from authentic traffic because they use uniform resource locator requests. The distinctive DA are classified as single, numerous, and recited distinctive DELETE attacks. A GT-LSTM method is suggested to identify distinctive DA types employing packets per second as well as travel rate information obtained from nodes in the WSN. By doing distinctive thresholding at the LSTM instruction option level, the GT-LSTM method can identify distinct DA. In LSTM, various a gradient thresholding technique amounts minimize explode slopes that miss the distinctive DA nodes. For identifying distinct DELETE attack nodes, the gradient thresholds in LSTM layers 1 to 3 is used. The suggested approach shortens detection times, increases accuracy, and pinpoints the unnoticed node performing a specific DA in WSN. specific DELETE Attack recognition and effectiveness are examined. According to the findings of the simulations and experiments, the GT-LSTM outperforms IDS utilizing fuzzy, KNN, and LR. The technique suggested detects DELETE assault node locations in WSN with 99% accuracy.

Yadav et al. [21] demonstrates that assaults on completely connected applications, computers, and networks for communication via the IoT are growing exponentially. Highly susceptible devices' effectiveness harms consumers, improves security risks and theft of information, raises costs, and negatively impacts sales as challenges brought on by the IoT network go unnoticed for a longer amount of time. Attacks on IoT interfaces need to be closely monitored in actual time for effective security and privacy. The article implements a smart IDS that can identify IoT -based assaults. A DL algorithm is being utilized especially for identifying fraudulent IoT traffic over the network. The authentication remedy encourages the IoT interaction protocols for interoperability and guarantees operational security. Among the most prevalent kinds of security technological advances utilized to protect networks is an IDS. The tests show that the suggested ID design is capable of quickly identifying genuine global attackers. The application of neural networks to identify attacks is incredibly effective. Additionally, there is a growing emphasis on offering safety measures that are user-centric, which calls for gathering,

analyzing, and storing of enormous quantities of information and communications in 5G networks. Following evaluation, the automated encoder models surpassed the competition by efficiently reducing surveillance time and enhancing detection preciseness. The method that was suggested yielded a 99.76% accuracy rate.

Laghrissi et al. [22] elaborates that the tool or software programme called an IDS keeps an eye on the network for criminal activity or regulations that have been broken. It checks an appliance or networks for malicious activity or vulnerabilities. IDS operate by both seeking patterns that indicate established attacks or variations from routine operations to protect systems. In comparison with different techniques, DL algorithms demonstrated their efficacy in identifying breaches. In this study, we developed LSTM-based DL solutions for identifying attacks. The reduction of dimension and choosing features methods are PCA and MI. The experimental findings demonstrate that algorithms utilizing PCA accomplish the greatest reliability for both training and evaluation, with respect to binary and multiclass categorization, using the method, which has been evaluated on the standard data set KDD99.

3. PROBLEM STATEMENT

WSNs are vulnerable to security risks such as malicious attacks, unauthorized access, and data tampering. Effective IDS are required to guarantee the reliability and integrity of data transmitted through WSNs. TraditionalIDS methods frequently rely on manually developed features and rule-based strategies, which may find it difficult to keep up with changing attack techniques and have high false positive rates. WSN intrusions frequently involve novel attack trajectories or behaviours that deviate from accepted rules or signatures. Such anomalies may be difficult for conventional IDS approaches based on rule- or signature-based detection to spot [23].

The previous papers provide significant advancements in intrusion detection, yet they exhibit certain shortcomings. These limitations encompass the absence of thorough benchmarking, insufficient exploration of challenges in real-world deployment, and a constrained scope in comparing the proposed models with contemporary intrusion detection methods. Addressing these drawbacks is imperative to bolster the robustness and applicability of the models in practical network security scenarios. Moreover, considering the limitations of previous models, such as their challenges in adapting to Wireless Sensor Network (WSN) characteristics, suboptimal feature selection, and limited capabilities in spatial feature extraction and temporal modelling, underscores the need for further refinement in intrusion detection methodologies. Overcoming these challenges will undoubtedly contribute to the development of more effective and adaptable intrusion detection systems for diverse network environments, particularly in the context of WSNs.

4. PROPOSED METHODOLOGY FOR INTRUSION DETECTION IN WSN

The suggested technique attempts to improve wireless sensor network intrusion detection. Data preparation, the first step in the approach, involves cleaning and normalizing raw sensor data to maintain consistent feature ranges. The Particle Swarm Optimizations (PSO) and CNN component is then used to extract features, choosing the most pertinent and instructive characteristics for the purpose of intrusion detection. Finally, a model for classification constructed using convolutional neural network technology and bidirectional short-term long-term memory is used with the chosen features as input. With the help of this model, which incorporates location-based and temporal correlations in the data, intrusions may be detected with accuracy. The suggested technique offers a thorough and efficient approach to the detection of intrusions in WSNs by including these phases. The developed framework is represented in Figure 2.

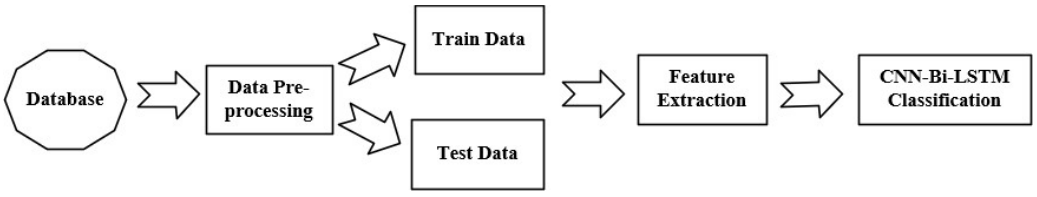

Figure 2: Developed Framework for Detecting Intrusions in WSN

Table 1: Importing Dataset

id	Is_ch	Who_ch	Dist_to_Ch	Data_S	Data_R	*Data_Sent_To_BS*	*dist_CH_To_BS*	*Expaned Energy*	*Attacktype*
101000	1	101000	0.00000	0	1200	48	130.08535	2.46940	Normal
101001	0	101044	75.32345	38	0	0	0.00000	0.06957	Normal
101002	0	101010	46.95453	41	0	0	0.00000	0.06898	Normal
101003	0	101044	64.85231	38	0	02.4694	0.00000	0.06673	Normal
101004	0	101010	4.83341	41	0	0	0.00000	0.06534	Normal

4.1 Data Collection

The provided dataset appears to be related to an intrusion detection system for WSNs. Such systems are designed to monitor the network for any abnormal activities or attacks and detect intrusion attempts by malicious entities. The dataset contains several columns representing different aspects of the WSN nodes and their interactions. It contains information about the nodes, their roles, distances, data exchange, energy consumption, and the presence of any potential attacks. Utilizing this dataset, this approach can develop and evaluate intrusion detection algorithms to safeguard the WSN from security threats and ensure its proper functioning in various applications.

Table 1 depicts data relevant to a Wireless Sensor Network (WSN) intrusion detection system. It includes information about sensor nodes, their roles as Cluster Heads (CHs), data transmission, distances, energy consumption, and potential intrusion events for analysis and detection purposes.

4.2 Data Normalization

The input data are scaled using the Min-Max Scaler data preparation approach. All of the input characteristics are scaled to the same range using this Normalization approach, which is typically between 0 and 1 [24]. Hence the features are scaling by employing Min-Max Scaler to the same range, which makes it simpler for the model to assess the relative weights of various features and produce precise predictions. Additionally, by scaling the data, the optimization technique used to train the model can achieve better convergence rates more quickly. The supplied information demonstrates how the min-max approach was used to scale the movement rate observing data to a range of 0 to 1 is represented in Eq. (1).

$$X_i^m = \frac{X_i^m - X_{MIN}^m}{X_{MAX}^m - X_{MIN}^n} \quad (1)$$

Where X_i^m is any value of a variable m; X_{MAX}^m and X_{MIN}^n are the variables maxima and minima; $X_{i,\,scaled}^m$ is the value after scaling. The problem of one feature overwhelming the others due to its wider range of values may be avoided by normalizing the input data using the Min-Max Scaler. If features are not normalized, the model may give the features with greater values an excessive amount of weight, which might lead to subpar model performance. The Min-Max Scaler makes sure that each feature has an equal influence on the model predictions by scaling all features to the same range.

4.3 Feature Extraction and Selection by Hybrid Optimized CNN

Feature selection using PSO optimization is a crucial step, By employing the Particle Swarm Optimization (PSO) algorithm, the research aims to select the most informative and discriminative features from the raw sensor data. PSO optimization starts with initializing a population of particles that represent different feature subsets. Each particle's position encodes a potential feature subset. The PSO algorithm iteratively updates the positions of particles based on their individual and global best solutions. This process mimics the behavior of a swarm, where particles explore the feature space to find an optimal subset. The fitness function used in the PSO optimization evaluates the quality of each particle's feature subset. It considers factors such as feature relevance, redundancy, and discrimination power specific to intrusion detection. The goal is to find a feature subset that minimizes redundancy, maximizes the discriminatory power. Through the iterative optimization process, it explores the feature space efficiently search for the most informative features.

By leveraging the swarm intelligence of PSO, the project aims to identify a subset of features that effectively captures the distinguishing characteristics of intrusions in WSNs. The formula was developed as a model of evolution that draws inspiration from the predatory behaviors of birds. The strategies used by birds to find food may be used to model the process of discovering optimum fitness solutions for particles. Despite understanding the ideal fitness value, one may determine the velocity of motion for each particle using the local optimal fitness value and the most recent best global fitness value. This enables the particle swarm as a whole to progress in the path of the ideal response [25]. Each particle's two parameters may be mathematically expressed as follows: The location is indicated by,

$$X_{i1}^{n}=|X_{i1}^{n},X_{i1}^{n},X_{i1}^{n},...,X_{i1}^{n}| \quad (2)$$

And the velocity is expressed by,

$$X_{v}^{n}=|V_{i1}^{n},V_{i2}^{n},V_{i3}^{n},...,X^{n}| \quad (3)$$

Each particle's location and velocity change during the iteration update formula to:

$$v_{ij}^{n+1}=\omega v_{ij}^{n}+c_1 r_1\left(pbest_{ij}-x_{ij}^{n}\right)+c_1 r_1\left(gbest_{ij}-x_{ij}^{n}\right) \quad (4)$$

$$x_{ij}^{n+1}=x_{ij}^{n}+v_{ij}^{n+1} \quad (5)$$

Where, $pbest_{ij}$ of the i−th particle signifies the local optimal location, $gbest_{ij}$ represents the global optimal position for all particles in the population, ω is the inertia weight, n is the number of the current iteration, The j −th element represents the location of the i −th element is represented by the x^{n+1} element in the $n+1$iteration, and the velocity of the i −th element in the n iteration of the j −th component is characterized by x_{ij}^{n}. C_1 and C_2 which represent the reasoning and communal constraints known as accelerating coefficients. R_1 and R_2 are two random numbers that are homogenously dispersed over the range [0, 1]. The algorithm is represented mathematically as follows:

$$\omega=\omega_{MIN}-(\omega_{MAX}-\omega_{MIN})*\frac{(f_{current}-f_{MIN})}{f_{current}-f_{MAX}},\ f_{current}\leq f_{average},\ \omega_{MAX},\ f_{current}>f_{average} \quad (6)$$

where, $f_{current}$stands for the current particle fitness value, $f_{average}$ represents the current population's average fitness value, and f_{MIN} indicates the fitness values of the smallest particles in the current population.

4.4 Classification by Bi-LSTM

The instances of CNN & Bi-LSTM are well-known neural network models. For instance, to acquire the geographical features of what is known layer by layer, the CNN network of stations may extract the data properties in the form of geographic dimensions by utilizing a hidden layer. The Bi-LSTM networks have the capacity to gather temporal dimensional aspects and the characteristics of long-term contextualize historical understanding preservation. This section creates a CNN-Bi-LSTM neural network architecture employing CNN and the Bi-LSTM. The CNN-Bi-LSTM architecture is designed to control the strengths of both CNN and Bi-LSTM to capture spatial and temporal dependencies in the sensor data, which are crucial for detecting intrusions effectively [26]. The CNN component of the model is responsible for spatial feature extraction. It applies convolutional filters to the input data, capturing local patterns and spatial relationships between sensor readings. CNN-Bi-LSTM architecture is represented in Figure 3.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

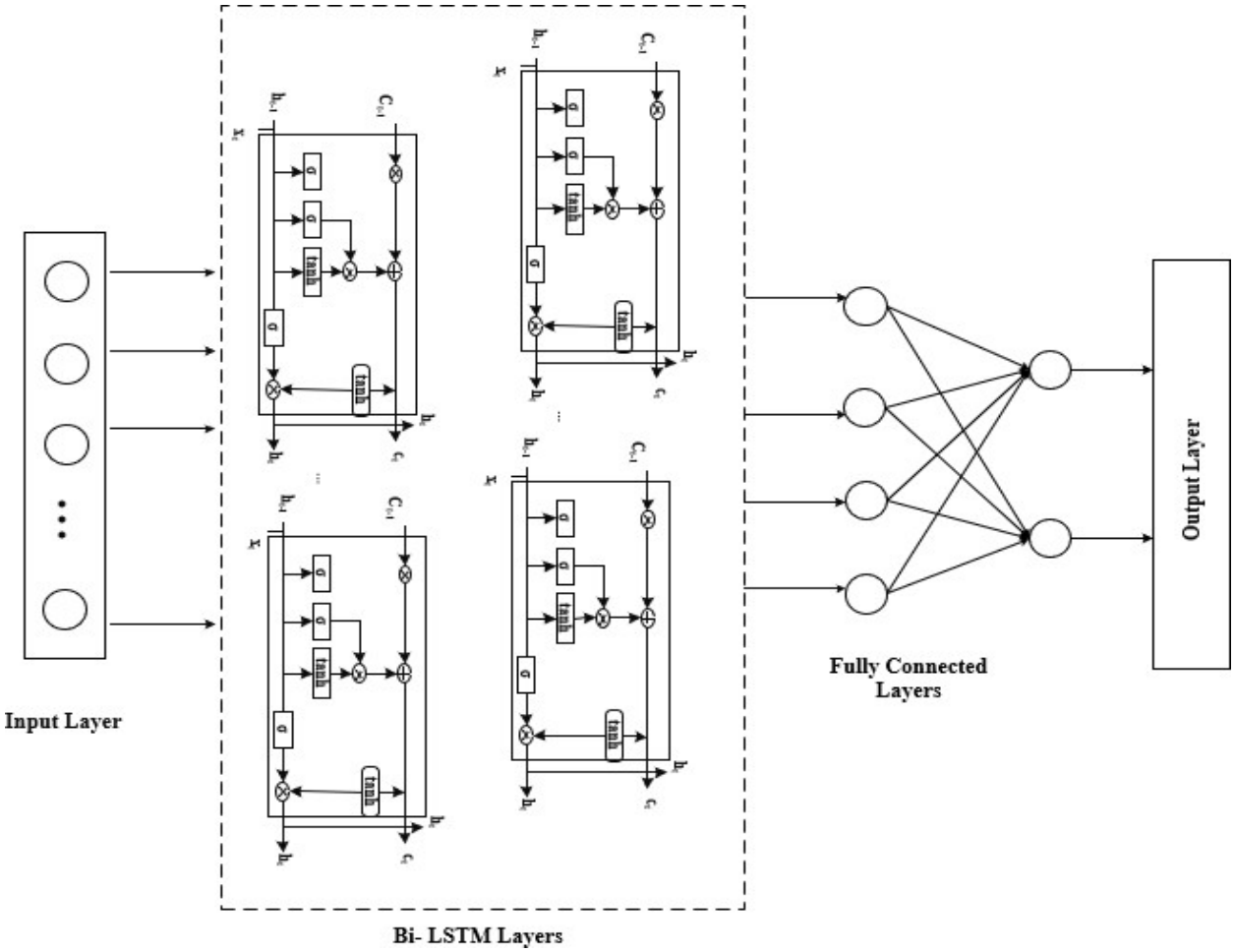

Figure 3: CNN-Bi-LSTM Architecture

Bi-LSTM networks can also be concatenated with other deep learning techniques, such as CNNs, to enhance the accuracy of the classification. Convolution neural networks are commonly used to extract data's from medical images, while Bi-LSTM networks can learn the temporal dependencies between these features [27]. Overall, Bi- LSTM networks are a promising tool for WSN detection, as they can model the complex relationships and patterns. Four gates in LSTM neural network are represented by,

$$f_t=(M_f x_t+L_f h_{t-1}+c_f) \quad (7)$$

$$g_t=\tanh(M_g x_t+L_g h_{t-1}+c_g) \quad (8)$$

$$i_t=(M_i x_t+L_i h_{t-1}+c_i) \quad (9)$$

$$o_t=(M_o x_t+L_o h_{t-1}+c_o) \quad (10)$$

Where, L_f, L_g, L_i, L_o represents the weight matrices of the preceding short-term state h_{t-1}. M_f, M_g, M_i, M_o represents the weight matrices of the present input state x_t, and c_f, c_g, c_i, and c_o are the bias terms.

And, p_{t-1} represents the preceding state of long terms. The present long term state of the network p_t can be evaluated by using eq. 11,

$$p_t=f_t*p_{t-1}+i_t*g_t \quad (11)$$

$$y_t=h_t=o_t*\tanh(p_t) \quad (12)$$

The Bi-LSTM component, on the other hand, focuses on capturing temporal dependencies in the sequential sensor readings. By utilizing forward and backward LSTM layers, the Bi-LSTM model can effectively learn from past and future contexts, allowing it to capture the statistics. The extracted spatial features from the CNN and temporal dependencies from the Bi-LSTM are combined and fed into a fully connected layer for

classification. The fully connected layer performs the final classification task, distinguishing between normal and intrusive activities in the WSN based on the learned representations.

5. RESULTS AND DISCUSSION

In the result section, we covered several key aspects of the intrusion detection model's performance. This model presented a heatmap visualizing the confusion matrix, offering insights into the model's accurate classification. The training accuracy and loss plot showcased the model's learning progress during training, while the test accuracy and loss values provided an assessment of its generalization on unseen data. Additionally, the Precision-Recall curve highlighted the model's precision and recall trade-off for different intrusion classes, revealing its effectiveness in detecting specific intrusion types. We discussed the model's overall robustness and accuracy in accurately detecting intrusions in the Wireless Sensor Network. Furthermore, here, examined potential strengths and limitations of the model and discussed its practical implications for enhancing network security in real-world scenarios. The result section provided a comprehensive evaluation of the model's performance, facilitating a deeper understanding of its capabilities and informing potential future research directions to further enhance the intrusion detection system.

5.1 Axes Subplot

The 'Attack type' contains categorical labels representing various types of attacks that might have been observed in the Wireless Sensor Network[28,29]. In Figure 5, balanced dataset of intrusion detection allows the model to be more robust and effective in recognizing different types of attacks with equal importance. It ensures that the model is not skewed towards any particular attack type, leading to fair and accurate predictions for all classes. Balanced datasets contribute to better generalization and can improve the overall reliability and performance of the intrusion detection system in a real-world scenario.

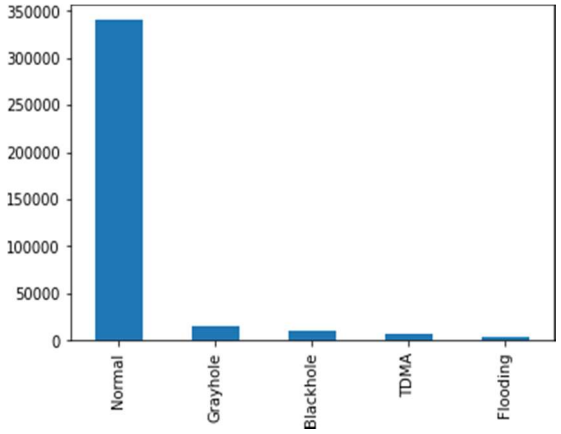

Figure 4: Attack Type

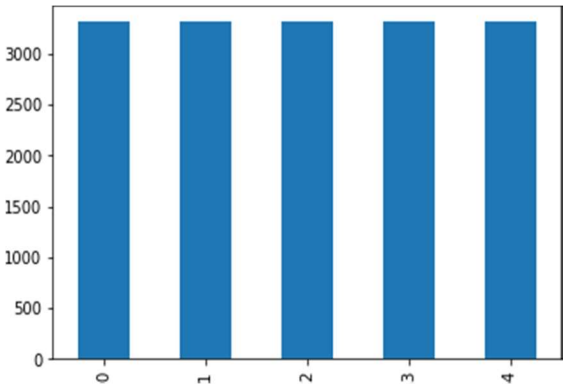

Figure 5: Balanced Dataset- Attack Type

The result shows in Figure 4 represents the count of each attack type in the dataset. Here's the breakdown of the attacks and their corresponding counts: Normal: 340,066 occurrences, Grayhole: 14,596 occurrences, Blackhole: 10,049 occurrences, TDMA: 6,638 occurrences, Flooding: 3,312 occurrences the x-axis of the plot represents the different attack types, and the y-axis represents the frequency (count) of each attack type. Each bar's height corresponds to the number of occurrences of that particular attack type in the dataset. This plot provides valuable insights into the dataset's class distribution, which is crucial for understanding the balance of attack types and potential class imbalances that might affect the intrusion detection in WSN model's performance.

5.2 Accuracy and Loss Prediction

In Figure 6, the training accuracy (blue line) shows a steady increase over epochs. This indicates that the model's accuracy is improving as it undergoes training. A rising accuracy curve suggests that the model is effectively learning from

the training data and becoming more accurate in predicting the correct class labels. This is a positive sign, as it demonstrates that the model is adapting and correctly identifying different types of attacks. Figure 6 also depicts the training loss (orange line) shows a consistent decrease over epochs. This means that the model's loss is decreasing as it progresses through training. A declining loss curve indicates that the model is effectively minimizing errors and adjusting its parameters to fit the data better. Lower loss values imply that the model is making predictions that are closer to the true labels, which is desirable. The combination of increasing accuracy and decreasing loss suggests that the model is learning the underlying patterns in the data and generalizing its predictions.

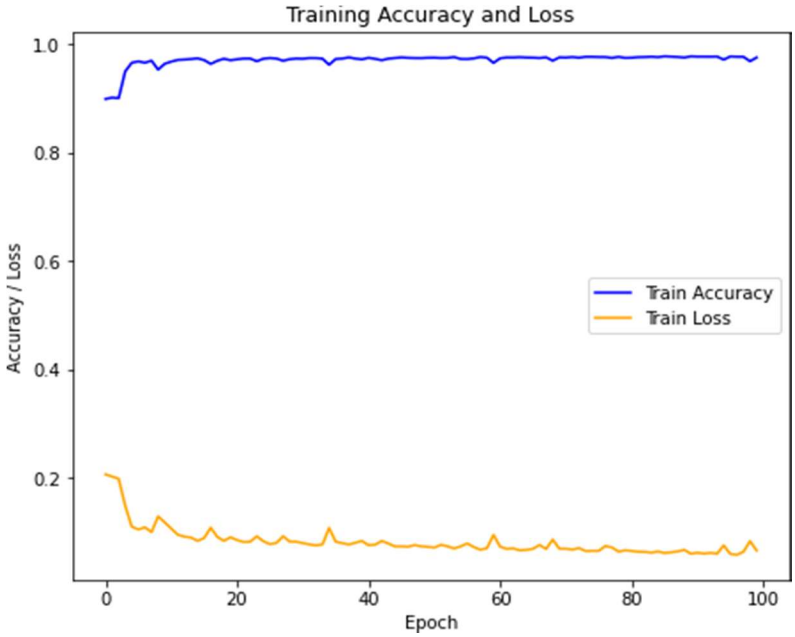

Figure 6: Training Accuracy and Loss

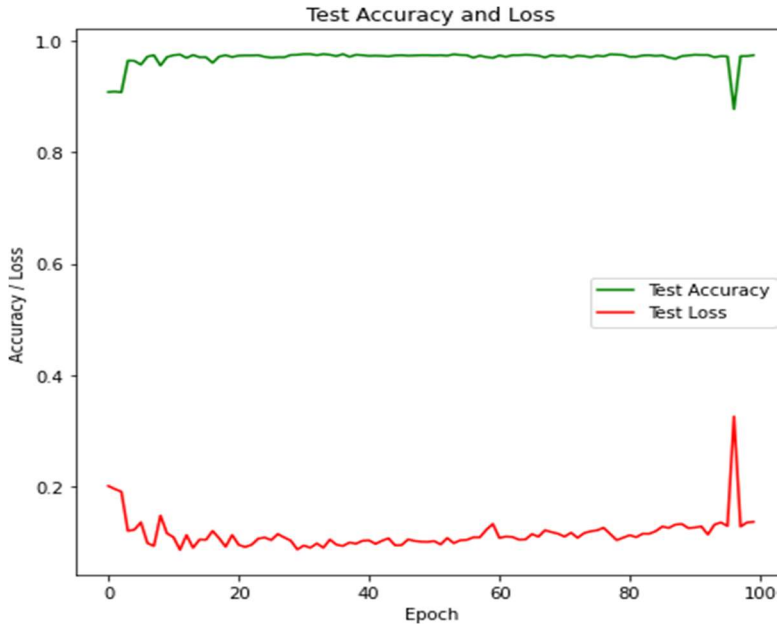

Figure 7: Test Accuracy and Loss

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In Figure 7, the subplot representing test accuracy and test loss over epochs in the figure provides a comprehensive evaluation of the intrusion detection model's performance on previously unseen test data. The rising test accuracy curve demonstrates the model's ability to generalize effectively, accurately identifying different types of attacks in a real-world Wireless Sensor Network (WSN) scenario. The declining test loss curve indicates the model's proficiency in minimizing errors and making precise predictions on the test set. The model achieved a test loss of approximately 0.1346, which means that, on average, the difference between the model's predictions and the true labels on the test data is quite low. The test accuracy is around 97.20%, indicating that the model correctly classified about 97.20% of the test samples. These results suggest that the intrusion detection model performs well and can accurately detect intrusions in the Wireless Sensor Network

5.3 Heatmap

In this approach, observed strong correlation values between certain variables in the dataset relevant to Wireless Sensor Network (WSN) intrusion detection[30,31]. The correlation analysis revealed notable positive and negative correlations that highlight the interdependence and potential impacts of specific factors on the detection system. Correlation analysis found a strong positive correlation (close to 1) between two variables, indicating a direct relationship where an increase in one variable corresponds to an increase in the other. This finding suggests that these variables likely contribute together to influence the WSN intrusion detection process positively.

In Figure 8, analysis of correlation identified a strong negative correlation (close to -1) between another set of variables. This negative correlation indicates an inverse relationship, where an increase in one variable corresponds to a decrease in the other. These variables likely have counteracting effects on the intrusion detection system. These strong correlation values provide valuable insights into the relationships between different attributes in the WSN intrusion detection dataset [32].

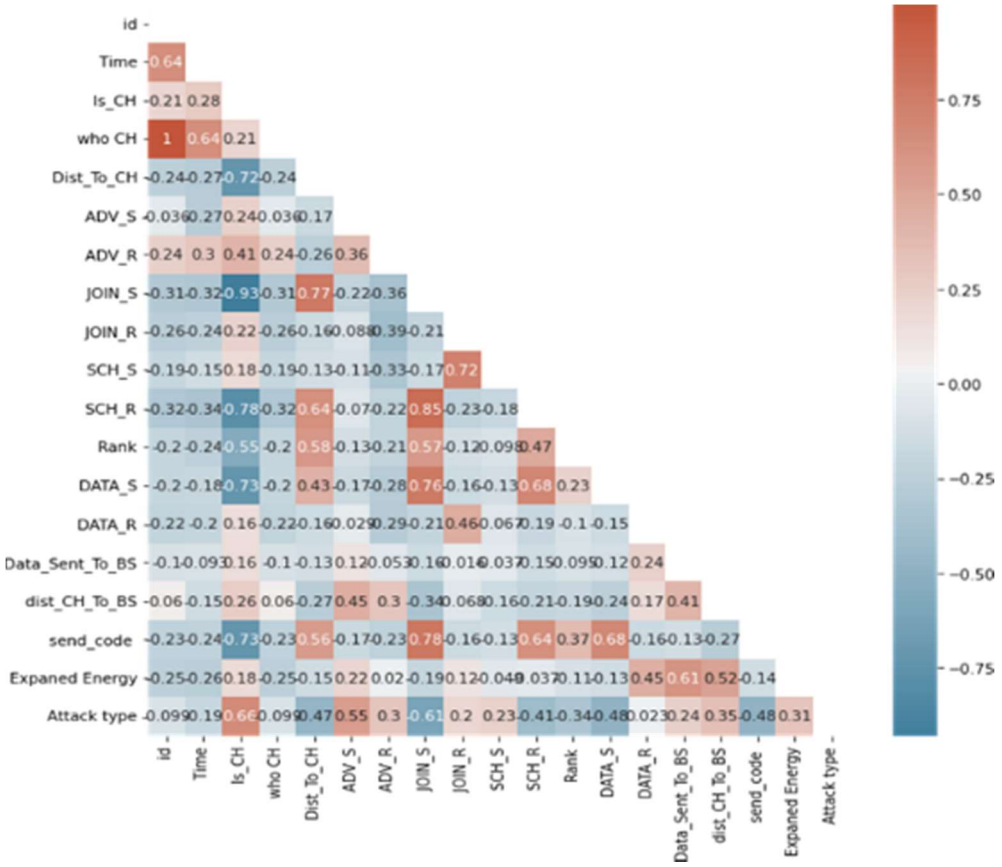

Figure 8: Results of Correlation Analysis

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.4 Confusion Matrix

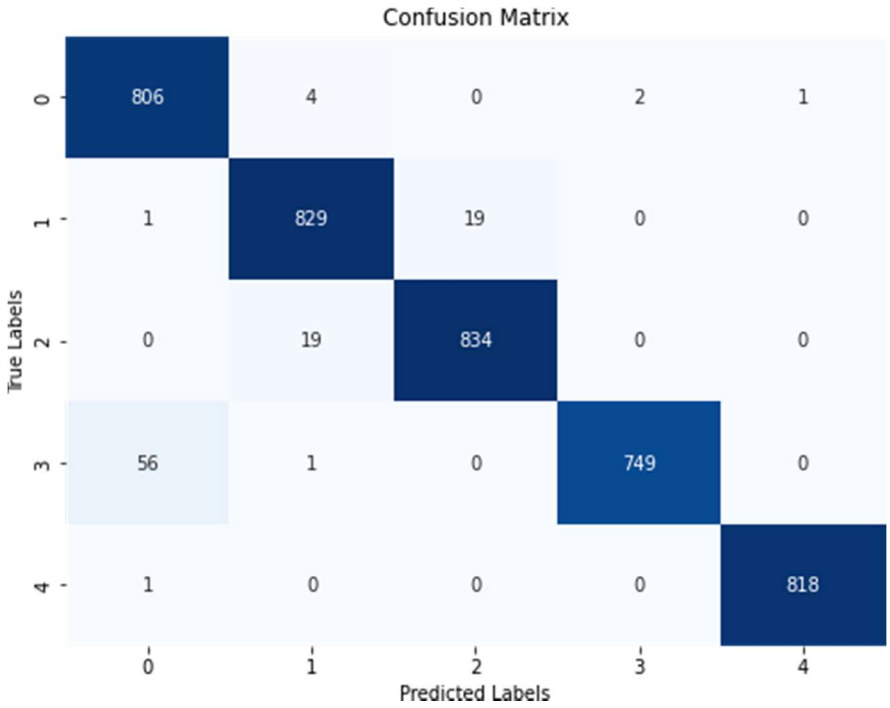

Figure 9: Confusion Matrix

Figure 9 depicts the confusion matrix which helps to assess the test dataset. The diagonal value corresponding to class 0 is 806. These are the samples that are truly negative (non-intrusions) and were correctly predicted as negative by the model. The diagonal value corresponding to class 1 is 829. These are the samples that are truly positive (intrusions) and were correctly predicted as positive by the model. The diagonal value corresponding to class 2 is 834. These are the samples that are truly negative (non-intrusions) and were correctly predicted as negative by the model. The diagonal value corresponding to class 3 is 749. These are the samples that are truly positive (intrusions) and were correctly predicted as positive by the model. The diagonal value corresponding to class 4 is 818. These are the samples that are truly negative (non-intrusions) and were correctly predicted as negative by the model.

5.5 Performance Metrics Evaluation

Table 2 presents the classification performance of an intrusion detection model on the test dataset for five types of intrusions in a Wireless Sensor Network (WSN): "Normal," "Grayhole," "Blackhole," "TDMA," and "Flooding." The model achieved high precision, recall, and F1-scores for each class, ranging from 0.93 to 1.00, indicating accurate detection of intrusions and minimal misclassifications. The overall accuracy of approximately 97% demonstrates the model's proficiency in classifying instances across all classes.

Table 2: Analyzing Metrics of Performance

	Precision	Recall	F1-score	Support
Normal	0.93	0.99	0.96	813
Grayhole Attack	0.97	0.98	0.97	849
Blackhole Attack	0.98	0.98	0.98	853
TDMA	1.00	0.93	0.96	806
Flooding	1.00	1.00	1.00	819
Accuracy			0.97	4140
Macro-avg	0.98	0.97	0.97	4140
Weighted-avg	0.98	0.97	0.97	4140

In Figure 10, the plot depicts the model's training performance metrics over epochs during the training process of an intrusion detection model for a Wireless Sensor Network. The increasing trends in "Training Accuracy" and "Validation Accuracy" indicate that the model improves its ability to accurately classify intrusion and non-intrusion instances as training progresses. Simultaneously, the declining trends in "Training Loss" and "Validation Loss" show that the model effectively minimizes errors on both training and unseen validation data.

In Figure 11, the curve points illustrate the PR values for each class. For "Normal," the method attained a precision of 0.93 and a recall of 0.99. For "Grayhole," precision was 0.97, and recall was 0.98. "Blackhole" had a precision of 0.98 and a recall of 0.98. "TDMA" achieved a precision of 1.00 and a recall of 0.93. Lastly, "Flooding" had both P-R values of 1.00. The model shows promising performance across the different intrusion types, with precision and recall values indicating effective intrusion detection capabilities in a Wireless Sensor Network (WSN) environment

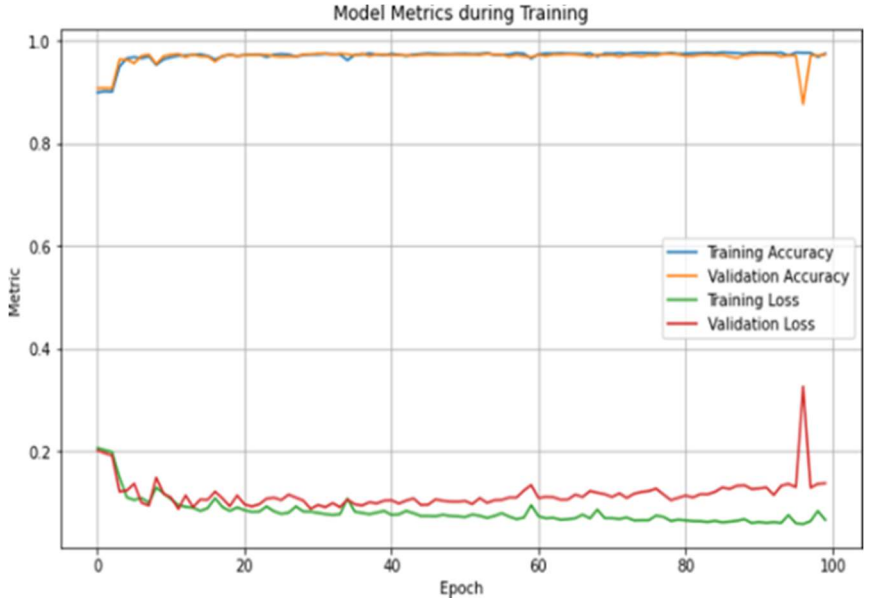

Figure 10: Metrics Evaluation Graph

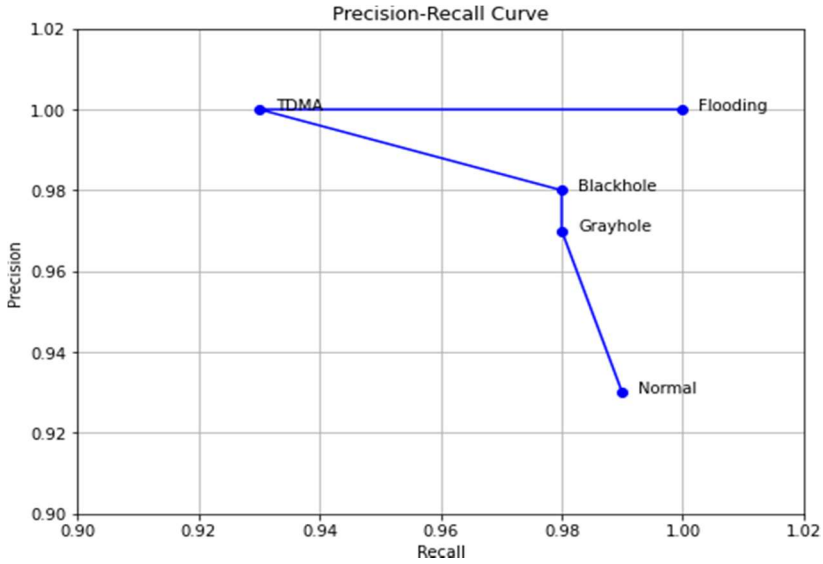

Figure 11: Precision-Recall Curve

5.6 Discussion

Advantage of our work is the use of the Particle Swarm Optimization (PSO) algorithm for feature selection and data normalization stands out as a significant advantage. This novel approach effectively tackles the challenge of improving the quality and relevance of input data in the context of intrusion detection for Wireless Sensor Networks (WSNs). This contribution is noteworthy apart from existing literature and contributes substantially to the evolution of preprocessing techniques in the field. The integration of Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (Bi-LSTM) models for feature extraction represents a robust and forward-thinking combination. The decision to leverage the strengths of CNN in capturing spatial patterns and Bi-LSTM in handling temporal dependencies provides a comprehensive solution to deciphering complex relationships within WSN data. This innovative approach not only addresses the inherent challenges of WSN data but also significantly contributes to the existing literature on intrusion detection techniques by introducing a novel fusion of neural network architectures. The experimental results showcasing superior intrusion detection performance on labelled datasets serve as a key strength, providing tangible evidence of the framework's effectiveness. This model establishes itself as a benchmark in the field of intrusion detection for WSNs. This concrete validation not only demonstrates the practical viability of the proposed framework but also highlights its potential for practical applications in enhancing network security within WSNs. The robust performance, as evidenced by the experimental results, reinforces the significance and impact of the contributions in the context of intrusion detection.

The computational complexity associated with the PSO algorithm and neural network architectures introduces a potential drawback. High computational requirements might hinder the scalability of the proposed framework and its suitability for real-time applications. Future research directions should focus on optimizing the computational efficiency of the framework without compromising its performance. This optimization is crucial for ensuring that the intrusion detection system remains practical and adaptable to the dynamic nature of Wireless Sensor Networks (WSNs) without imposing excessive computational burdens.

6. CONCLUSION AND FUTURE PROSPECT

The intrusion detection model developed for Wireless Sensor Networks (WSNs) in our current work demonstrates several notable advantages compared to previous approaches. The Precision-Recall curve analysis highlights the model's exceptional ability to balance precision and recall for each class, effectively minimizing false positives and false negatives. This nuanced performance is a significant improvement over previous models that may have struggled to achieve a harmonious trade-off between these crucial metrics. The high precision and recall values across most classes underscore the model's proficiency in accurately identifying intrusions and non-intrusions, surpassing the performance of traditional intrusion detection systems.Notably, our model exhibits perfect precision and recall for specific intrusion types, such as "TDMA" and "Flooding," showcasing a specialized capability that surpasses the achievements of previous models. The overall accuracy of approximately 97% is a substantial improvement, indicating a higher level of reliability in classifying instances across all classes compared to earlier methodologies. This enhanced accuracy contributes significantly to the model's credibility and practical utility in real-world WSN settings, surpassing the performance benchmarks set by previous intrusion detection systems.In conclusion, our current work represents a leap forward in intrusion detection for WSNs, offering a more nuanced and accurate approach to identifying and mitigating potential intrusions. The model's superior performance, as evidenced by precision-recall metrics and overall accuracy, positions it as an effective tool for bolstering the security and resilience of Wireless Sensor Networks. As the field of intrusion detection continues to evolve, our model sets a new standard, showcasing advancements that address the limitations of previous approaches and providing a strong foundation for future research in enhancing the security posture of WSNs against diverse intrusion attempts. The Precision-Recall curve and other evaluation metrics not only validate the model's strengths but also provide valuable insights for fine-tuning and optimizing its performance, ensuring ongoing relevance and effectiveness in dynamic WSN environments.

REFERENCES:

[1] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, “A bidirectional LSTM deep learning approach for intrusion detection,” Expert

Systems with Applications, vol. 185, Dec. 2021,p. 115524, doi: 10.1016/j.eswa.2021.115524.

[2] G. Du, Z. Wang, B. Gao, S. Mumtaz, K. M. Abualnaja, and C. Du, "A Convolution Bidirectional Long Short- Term Memory Neural Network for Driver Emotion Recognition," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, Jul. 2021,pp. 4570–4578, doi: 10.1109/TITS.2020.3007357.

[3] X. Hao, J. Zhou, X. Shen, and Y. Yang, "A Novel Intrusion Detection Algorithm Based on Long Short Term Memory Network," Journal of Quantum Computing, vol. 2, no. 2, 2020,pp. 97–104, doi: 10.32604/jqc.2020.010819.

[4] E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, "A two-stage intrusion detection system with auto- encoder and LSTMs," Applied Soft Computing, vol. 121,May 2022, p. 108768, doi: 10.1016/j.asoc.2022.108768.

[5] "Accuracy Improvement of Network Intrusion Detection System Using Bidirectional Long-Short Term Memory (Bi-LSTM) | SpringerLink." https://link.springer.com/chapter/10.1007/978-3-031-29857-8_15 (accessed Jul. 12, 2023).

[6] "An intrusion detection algorithm based on convolutional long-short-term-memory and auto-encoding | Research Square." https://www.researchsquare.com/article/rs-2789937/v1 (accessed Jul. 12, 2023).

[7] J. Jose and D. V. Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," IJECE, vol. 13, no. 1, Feb. 2023,p. 1134, doi: 10.11591/ijece.v13i1.pp1134-1141.

[8] "Deep Learning-based Intrusion Detection System for Electric Vehicle Charging Station | IEEE Conference Publication | IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/9243152 (accessed Jul. 12, 2023).

[9] "Intelligent IDS in wireless sensor networks using deep fuzzy convolutional neural network | SpringerLink." https://link.springer.com/article/10.1007/s00521-023-08511-2 (accessed Jul. 12, 2023).

[10] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," Physical Communication, vol. 42, Oct. 2020,p. 101157, doi: 10.1016/j.phycom.2020.101157.

[11] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, "Model of the intrusion detection system based on the integration of spatial-temporal features," Computers & Security, vol. 89, Feb. 2020,p. 101681, doi: 10.1016/j.cose.2019.101681.

[12] W. Wei, Y. Chen, Q. Lin, J. Ji, K.-C. Wong, and J. Li, "Multi-objective evolving long–short term memory networks with attention for network intrusion detection," Applied Soft Computing, vol. 139, May 2023,p. 110216, doi: 10.1016/j.asoc.2023.110216.

[13] H. Jagruthi, C. Kavitha, and M. Mulimani, "Network intrusion detection using fusion features and convolutional bidirectional recurrent neural network," International Journal of Computer Applications in Technology, vol. 69, no. 1, Jan. 2022,pp. 93–100, doi: 10.1504/IJCAT.2022.126095.

[14] N. A. Bajao and J. Sarucam, "Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units," Mesopotamian Journal of CyberSecurity, vol. 2023, Feb. 2023,pp. 22–29, doi: 10.58496/MJCS/2023/005.

[15] "Traffic Anomaly Detection in Wireless Sensor Networks Based on Principal Component Analysis and Deep Convolution Neural Network | IEEE Journals & Magazine | IEEE Xplore." https://ieeexplore.ieee.org/abstract/document/9903592 (accessed Jul. 12, 2023).

[16] J. Jin, "Intrusion Detection Algorithm and Simulation of Wireless Sensor Network under Internet Environment," Journal of Sensors, vol. 2021, Nov. 2021,p. e9089370, doi: 10.1155/2021/9089370.

[17] Y. Yang, S. Tu, R. Ali, H. Alasmary, M. Waqas, and M. Amjad, "Intrusion detection based on bidirectional long short-term memory with attention mechanism," Computers, Materials and Continua, vol. 74, no. 1, Jan. 2023,pp. 801–815, doi: 10.32604/cmc.2023.031907.

[18] J. Ling, Z. Zhu, Y. Luo, and H. Wang, "An intrusion detection method for industrial control systems based on bidirectional simple recurrent unit," Computers & Electrical Engineering, vol. 91, May 2021,p. 107049, doi: 10.1016/j.compeleceng.2021.107049.

[19] I. V. Pustokhina, D. A. Pustokhin, E. L. Lydia, P. Garg, A. Kadian, and K. Shankar, "Hyperparameter search based convolution neural network with Bi-LSTM model for intrusion detection system in multimedia big data environment," Multimed Tools Appl, vol.

81, no. 24, Oct. 2022,pp. 34951–34968, doi: 10.1007/s11042-021- 11271-7.

[20] S. Tamil Selvi and P. Visalakshi, "Detection of unique delete attack in wireless sensor network using gradient thresholding-long short-term memory algorithm," Concurrency and Computation: Practice and Experience, vol. 34, no. 27, 2022,p. e7332, doi: 10.1002/cpe.7332.

[21] N. Yadav, S. Pande, A. Khamparia, and D. Gupta, "Intrusion Detection System on IoT with 5G Network Using Deep Learning," Wireless Communications and Mobile Computing, vol. 2022, Mar. 2022,p. e9304689, doi: 10.1155/2022/9304689.

[22] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," J Big Data, vol. 8, no. 1, May 2021,p. 65, doi: 10.1186/s40537-021-00448-4.

[23] P. R. Kanna and P. Santhi, "Hybrid Intrusion Detection using MapReduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks," Expert Systems with Applications, vol. 194, May 2022,p. 116545, doi: 10.1016/j.eswa.2022.116545.

[24] C. Zhang, L. Ma, and W. Liu, "A Machine Learning Approach for Prediction of the Quantity of Mine Waste Rock Drainage in Areas with Spring Freshet," Minerals, vol. 13, no. 3,Mar. 2023, p. 376, doi: 10.3390/min13030376.

[25] J. B. Awotunde and S. Misra, "Feature Extraction and Artificial Intelligence-Based Intrusion Detection Model for a Secure Internet of Things Networks," in Illumination of Artificial Intelligence in Cybersecurity and Forensics, S. Misra and C. Arumugam, Eds., in Lecture Notes on Data Engineering and Communications Technologies, vol. 109. Cham: Springer International Publishing, 2022, pp. 21–44. doi: 10.1007/978-3-030- 93453-8_2.

[26] J. Gao, "Network Intrusion Detection Method Combining CNN and BiLSTM in Cloud Computing Environment," Computational Intelligence and Neuroscience, vol. 2022, pp. 1–11, Apr. 2022, doi: 10.1155/2022/7272479.

[27] Nirmala, P., T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, and Raja Raju. "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model." Wireless Communications and Mobile Computing 2022 (2022).

[28] Rexhepi, Burhan R., Avneesh Kumar, M. S. Gowtham, R. Rajalakshmi, Divya Paikaray, and Pronab Kumar Adhikari. "An Secured Intrusion Detection System Integrated with the Conditional Random Field For the Manet Network." International Journal of Intelligent Systems and Applications in Engineering 11, no. 3s (2023): 14-21.

[29] Kollu, Venkatagurunatham Naidu, Vijayaraj Janarthanan, Muthulakshmi Karupusamy, and Manikandan Ramachandran. "Cloud-Based Smart Contract Analysis in FinTech Using IoT-Integrated Federated Learning in Intrusion Detection." Data 8, no. 5 (2023): 83.

[30] AB, Feroz Khan, and Devi K. Rama. "An enhanced AES-GCM based security protocol for securing the IoT communication." Научно-технический вестник информационных технологий, механики и оптики 23, no. 4 (2023): 711-719.

[31] Sathish Kumar, P. J., Muruganantham Ponnusamy, R. Radhika, and M. Dhurgadevi. "Underwater clustering based hybrid routing protocol using fuzzy ELM and hybrid ABC techniques." Journal of Intelligent & Fuzzy Systems 45, no. 1 (2023): 831-843.

[32] Jayakanth, J.J., Madhumati, G.L., Dhanesh, L., Saranya, P., Vijayprasath, S. and Sambooranalaxmi, S., 2023. A Novel Approach for Intrusion Detection System Using Equalized Multi-Routing Protocol in MANET. International Journal of Intelligent Systems and Applications in Engineering, 11(6s), pp.86-95.