Journal of Information Systems Engineering and Management
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Improving IoT Security by A Hybrid BiLSTM-WOA Approach for Robust Attack Detection

Marwa Mahdi Hassooni[1], and Alaa Abdulhussein Daleh Al-Magsoosi[1]
[1]*College of Computer Science & Information Technology, University of Al Qadisiyah, IRAQ*
(it.mast.23.17@qu.edu.iq, adleah@qu.edu.iq)

ARTICLE INFO

Received: 20 Dec 2024

Revised: 22 Feb 2025

Accepted:28 Feb 2025

ABSTRACT

The rapid development of IoT devices has attracted the attention of researchers and created significant new security challenges. This challenge has highlighted the need for advanced methods and techniques to detect and address intrusions. This paper presents a robust and coherent system for detecting IoT attacks using the hybrid BiLSTM-WOA model. Our research uses two large datasets, CIC IoT 2023 and N-BaIoT, which contain 46,686,579 and 863,057 records covering multiple IoT attack scenarios, respectively. An important difficulty tackled in this work was the noticeable data imbalance in both datasets, where attacks were frequent compared to normal traffic. This was resolved by implementing meticulous preprocessing techniques that allowed us to balance the datasets to achieve a 50-50 distribution between attack and regular traffic. This led to unbiased model training and evaluation of the trained models. The innovative integration of the Whale Optimization Algorithm (WOA) with the BiLSTM model enabled the automated fine-tuning of essential hyperparameters, precisely the number of LSTM units and dropout rate. This led to improved model generalization and performance. We conducted a thorough performance evaluation using accuracy, precision, recall, and F1-score metrics. The BiLSTM-WOA model achieved an impressive accuracy rate of 99%, surpassing other LSTM variants; Vanilla LSTM and Time-Distributed LSTM achieved 97%, while Deep LSTM and Stacked LSTM had accuracies of only 40% and 47%, respectively. Solutions developed with training processes showed a general improvement in accuracy with a slight overfitting trend due to the close alignment of curves for training and validation accuracy. These findings confirm the strength of the model and its applicability in the practical implementation of IoT security. This analysis may contribute to IoT security by providing a potent new model incorporating various fusion schemes and algorithms within its framework. It provides a precise, highly reliable and scalable attack model.

Keywords: Internet of Things (IoT), Anomaly Detection, BiLSTM-WOA, Deep Learning, LSTM, DDoS, Cybersecurity.

INTRODUCTION

Over the last couple of years, the general adoption of the Internet of Things machines really marked a peculiar period of connectedness, accessibility, and mechanization in industries and private lives. Generally, IoT is employed in smart houses, health care, industrialization, transport techniques, and many other areas. IoT devices are heterogeneous, resource-constrained, and do not observe standardized security protocols. Consequently, their extensive deployment has spread new security exposures. These exposures have generated IoT networks fleshy targets for cyberattacks, including Distributed Denial-of-Service (DDoS) attacks, malware injections, and unauthorized admission [1-3].

As the need for IoT devices resumes accelerating, integrating them into private and industrial applications has become increasingly critical. Considerable IoT-connected devices develop and handle sensitive and secure information, making IoT networks an attractive target for cybercriminals and hostile actors aiming to manipulate security exposures for unethical purposes [4]. The across-the-board adoption of IoT devices, which show exceptional connectivity and mechanization capabilities, has underscored the urgent need for strong and flawless security standards. Standard signature-based and other detection techniques are generally employed and are increasingly inadequate in managing the growing and dynamic nature of cyber threats in IoT environments. These conventional

methods face important constraints in seeing new attack practices and trading with the inherent complexities of IoT techniques due to their deficiency of many outcome strategies and techniques to handle the massive effect on the other side, including resource limitations, various machine styles, and heterogeneous communication protocols. Therefore, there has been a growing curiosity in AI-based solutions, with anomaly detection technologies emerging as the preferred approach for their intelligent and adaptive capacities to detect, remediate, and repel threats. Contemporary advancements in trust administration, deep learning, and neural networks have contributed to developing worldly AI-driven frameworks to improve the security of IoT networks [5][6].

Existing security services like firewalls and signature-based intrusion detection systems face challenges, such as IoT environments' dynamic and sophisticated nature. These systems struggle to keep up with the ever-changing strategies employed by cybercriminals and the vast amounts of data produced by IoT devices. Therefore, there is an evident gap in the market for machine learning (ML) and deep learning (DL) based advanced intrusion detection systems (IDS) that would enhance threat detection and mitigation systems [7].

Deep learning models, and in particular Long-Short-Term Memory (LSTM) networks, have profound possibilities in detecting IoT attacks as they remember dependencies and patterns from sequential network traffic data. Still, due to the high dimensionality of IoT data and the high requirement for fine-tuning hyperparameters, optimizing models based on LSTM is difficult [8][9].

This paper aims to introduce a hybrid model, BiLSTM-WOA, proposed to enhance IoT security by enhancing attack detection performance with improved accuracy and efficiency. The main contributions of this paper are as follows:

A. The hybrid model BiLSTM-WOA was developed to integrate the Whale Optimization Algorithm into a Bidirectional Long Short-Term Memory network to enhance attack detection in IoT. The proposed BiLSTM component can learn bidirectional temporal dependencies in network traffic more effectively, while WOA optimizes critical hyperparameters to ensure improved learning performance.

B. Benchmark Dataset Evaluation: The proposed model has been applied to CIC IoT 2023 and N-BaIoT-two of the most popular benchmark datasets for IoT attack detection. These two datasets include various real-world attack scenarios that an IoT may face, with challenges of high-class imbalance, which were addressed through robust preprocessing techniques.

C. Extensive Performance Analysis: The performance of the BiLSTM-WOA is critically evaluated by taking essential performance metrics such as accuracy, precision, recall, and F1-score, showing excellence in detection performance for normal LSTM-based methods.

D. Improved Detection Performance and Robustness: The proposed system yields a 2% gain in classification performance in all evaluation metrics concerning a Vanilla LSTM model that is robust, efficient, and suitable for real-world IoT security problems.

RELATED WORKS

The accelerating importance is a result of the development of IoT devices, which has led the authors to conduct various research into intrusion detection systems (IDS) to attack emerging security challenges. Traditional IDS methods, such as signature-based and rule-based approaches, have been commonly used; however, their effectiveness is limited due to the dynamic and growing nature of IoT threats. The research community, therefore, relied on machine learning and deep learning methods to improve the detection accuracy and adaptability of IDS in IoT environments. Several works proposed models based on LSTM networks for IoT attack detection, considering their powerful capability of learning meaningful dependencies in network traffic data.

In [10], the researchers proposed a new IDS to enhance the security of IoT-based networks using a hybrid deep learning model. They proposed a feature selection method that could perform effectively by combining particle swarm optimization (PSO) and genetic algorithms known as PSO-GA, which can find the most important features from the CICIDS-2017 dataset. To improve detection accuracy, the researchers developed a hybrid deep learning model, namely LSTM-GRU, integrating the strengths of LSTM and GRU. The proposed IDS model showed much better performance regarding the detection of different types of network attacks, which was 98.86%.

Jyothi R. and D. Jagadeesha [11] came up with a novel AI-driven threat detection framework using Cyber Twin Technologies for IoT network security. The model integrates digital replicas of physical IoT devices, called Cyber

Twins, with AI-based IDS for the effective detection, prediction, and mitigation of cyber threats in real time. The proposed hybrid deep learning model employed both CNNs and RNNs for anomaly detection, which resulted in improved accuracy, a huge drop in the rate of false positives, and quick response times. Cyber Twin is another important contribution to continuous monitoring and emulation of attacking methodologies for dynamic IoT devices for protection and stability within infrastructures of IoT devices. Hence, practical evaluations of the system had been effective in illustrating a detection accuracy of 96.2%, a reduction of 35% in response time, and 15% in false positives when compared to traditional approaches. Besides that, the framework had also shown very impressive resilience, 98.1%, against simulated attacks and established a leading solution for IoT security. They thus concluded that their approach provides a robust and scalable security framework for IoT networks, with future enhancements possible through advanced AI techniques such as reinforcement learning and federated learning, as well as blockchain technology for secure information sharing.

Md. Ibne Joha et al. [12] proposed a precise and secure Industrial Internet of Things (IIoT) framework that combines real-time active and reactive load forecasting with developed anomaly detection, handling necessary challenges in industrial processes. The suggested system utilizes a hybrid AI-driven approach that integrates Temporal Convolutional Networks, Gated Recurrent Units, and Attention mechanisms (TCN-GRU-Attention) to perform highly accurate load predictions, exceeding traditional models. As far as the Active Load Forecasting approach is concerned, the model recorded an average performance at a square error of 0.0183 with a means absolute error of 0.1022 and 0.1354 value of the root mean square. The outcome with regard to Reactive Load Forecasting encompasses the following results: MSE = 0.0202, MAE = 0.1077, and RMSE = 0.1422. Complementary to the load forecast, the researchers performed an optimized Isolation Forest model for anomaly detection. In this way, the transient conditions were considered to detect the irregularities of machine manners. It yielded superior results on its performance: 95% accuracy, 98% recall, an F1-score of 96%, and an accuracy of almost 100%. This framework has been allowed to be deployed on edge devices like Jetson Nano and centralized cloud servers. Thus, it confirmed functional viability in industrial domains. It also provides the central security for integrated TLS and SSL protocols along with hash-encoded encrypted credentials. It would further increase the energy efficiency and strength of the grid, while the contribution of real-time monitoring and control and protection to the industrial operation adds to its sustainability and strength.

In study [13] targeted the transformative role of AI in enhancing cybersecurity to authorize real-time threat detection and mechanical reaction tools for cloud and network infrastructures. Whereas classic security measures cannot adequately manage dynamic attack vectors like zero-day exploits or insider threats, the cyber threats are getting increasingly refined and general. The analysis identifies that AI-powered security solutions are powered with machine learning, big data analytics, and adaptive algorithms that can explore a wide range of datasets for anomalies and problematic patterns with an unprecedented scale and speed. Experimental results combined with real test case analyses show how these AI-based solutions are much needed to introduce improvement in threat detection accuracy, reduction of false positives, and response time. However, the authors also address issues related to privacy concerns, explainability problems, and transparency of complex AI models. The study calls for XAI with their derived privacy preservation techniques as necessary to ensure regulatory compliance and foster trust in AI-based security systems. A balanced view between the imperatives of privacy with performance, against rising threats to technologies like quantum computing and vulnerabilities in IoT, shows that modern cybersecurity frameworks would continue to have substantial elements of AI and ML. Their presence brings this much-needed switch from reactive models to predictive, adaptive, and automated security models with which communities create resilient defenses with a conscience towards moral and regulatory standards.

PROPOSED BILSTM-WOA HYBRID MODEL

The hybrid model BiLSTM-WOA combines the strengths of the Bidirectional Long Short-Term Memory network with that of the Whale Optimization Algorithm for superior predictive performance and improved optimization efficiency. Unlike the standard LSTM networks, BiLSTM processes the data in both forward and backward directions, thereby enabling the model to learn the long-term dependency and context better. This model is very useful in such tasks as time series forecasting and anomaly detection [14].

One of the challenges concerning the use of BiLSTM is that their performance depends a lot on the choice of appropriate hyperparameters, such as the number of hidden units or the learning rate [15]. If the parameters are not well tuned, then the accuracy of the model decreases and so does its generalizing capability. It is in this aspect that

the WOA attacks: this is the optimization technique which, inspired by the hunting behaviors of the humpback whales, optimizes the hyperparameters of the BiLSTM model [16]. The iterative enhancement of these leads WOA to the minimization of the error and an acceleration of the convergence that makes the whole hybrid system much more effective. This leads to a robust model that is not only more predictive and adaptable for different datasets but also computationally efficient in many real-world scenarios. This hybrid model has shown great promise in different applications-from economic forecasting to healthcare analytics and optimization of industrial strategies-where the accuracy of the forecast or efficiency is at the core of every decision.

BiLSTM-WOA can contribute significantly to cybersecurity-related systems, like intrusion detection, fraud prevention, and many more. It provides the capability of BiLSTM in analyzing time-series data for unusual pattern detection in network traffic that might give an early warning of some potential threat. WOA improves this process by selecting the most relevant features only for improving the detection accuracy with reduced computational cost. The hybrid approach will be of great value in fraud detection in financial applications. BiLSTM considers the historical spending patterns to flag suspicious transactions, while WOA refines the feature set for further improvement in accuracy even in complex scenarios. For instance, fraudulent credit card transaction detection will find the deviation in user behavior with this hybrid model and thus allow early intervention. The BiLSTM-WOA hybrid model thus represents the union of deep learning and nature-inspired optimization into an effective, advanced solution in solving modern cybersecurity and finance-related challenges.

DATASETS DESCRIPTION AND COMPARISON

The CIC IoT 2023 [17] and N-BaIoT [18] datasets are among the most popular in cybersecurity research, especially for developing and evaluating machine learning models for intrusion detection and anomaly detection in IoT environments. These datasets provide broad real-world traffic data and a rich set of features that help identify and classify different network attacks and anomalous behaviors in IoT ecosystems.

A) CIC IoT 2023 Dataset

CIC-IoT-2023 was developed by the Canadian Institute for Cybersecurity and is considered the benchmark full dataset for testing IDS performance in IoT networks. The CIC IoT 2023 dataset contains the captured traffic of IoT network communications in their normal state and during an attack, covering all attack vectors such as:

- DDoS-attacks: Overloading network channels with redundant traffic to disturb regular operations.
- Botnet Attacks: Controlling and compromising IoT devices to perpetrate malicious activities.
- Port Scanning: The unauthorized probing of network ports to search for vulnerabilities.
- Man-in-the-Middle (MITM) Attacks: Interception and manipulation of communications between IoT devices.

The CIC IoT 2023 dataset contains broad labeled traffic data from various devices, such as smart thermostats, cameras, and home automation systems. It includes features related to network flow characteristics, such as packet sizes, timestamps, flow duration, and protocol usage, which enable the training and evaluation of AI-based detection models [19]. The dataset is also structured in a way that provides a balanced distribution of normal and malicious traffic, further enhancing the reliability of models built upon it. Researchers use this dataset to evaluate various machine learning algorithms' efficiencies in detecting IoT-specific cyber threats with minimal false alarms.

B) N-BaIoT Dataset

Another important resource for dealing with the challenges of IoT security is N-BaIoT, standing for Network-Based IoT; this dataset will mainly focus on the detection of botnets. This dataset has been created by monitoring the traffic of several IoT devices under normal operational conditions and attack scenarios. The N-BaIoT dataset includes several well-known botnet attack types, such as:

- Mirai Botnet attacks to exploit default credentials to spread and cause Distributed Denial of Service, aka DDoS.
- Bashlite Botnet Attacks: Malware that scans devices vulnerable to the malware, exploits those devices, and spreads.

Another unique feature of the N-BaIoT dataset is that it contains a lot of features characterizing statistical flow, which includes mean and standard deviation of packet inter-arrival times, flow entropy, and connection duration. The attack and normal traffic in this dataset are well-structured with labels; hence, they are more suitable for any supervised learning approaches [20]. It finds wide usage for training and testing anomaly detection models that target compromised IoT devices in large-scale deployments, as its focus is mainly on botnet-related threats.

C) Comparison and Applications

While both have their value in providing insights related to intrusion and anomaly detection in IoT networks, differences in focus and scope exist. The CIC IoT 2023 dataset encompasses a wide variety of attack types and device diversity suitable for general IoT security research, while the N-BaIoT dataset specializes in botnet detection, considering attack behaviors of a reduced number of devices.

These are all widely applied in various research areas including, but not limited to:

- Intrusion Detection Systems development: the training of deep learning models like BiLSTM and CNN for detecting sophisticated cyber threats.

- Anomaly detection in smart environments: detection of deviation from normal behavior by IoT devices to avert potential cyber-attacks.

- Feature Selection and Optimization: Using optimization algorithms such as WOA to enhance feature selection and the accuracy of models.

The diversified CIC IoT 2023 and quality network traffic data from N-BaIoT contribute a lot towards improving research in IoT security, helping the design of strong machine learning-based intrusion detection and anomaly detection systems that can adapt in this continuous and fast-changing world of cyber threats to allow protection and resilience in IoT ecosystems [21].

ANALYSIS OF DATASET DISTRIBUTION

Table I gives a comparative analysis of the original and balanced distributions of two cybersecurity datasets: CIC IoT 2023 and N-BaIoT. In their original forms, both datasets have a significant class imbalance, meaning that most of the instances are in the attack category. For example, the CIC IoT 2023 dataset consists of 95.7% attack traffic and only 4.3% normal traffic, while the N-BaIoT dataset is made up of 94.6% attack traffic and 5.4% normal traffic. This can easily cause problems with machine learning models to produce biased predictions with poor generalization, especially in detecting normal behavior.

The attack in this problem was performed by balancing the distribution of datasets into 50% attack traffic and 50% normal traffic for both datasets. The balance of attack and normal data improves the performance of IDS models, as a representative training dataset results in better accuracy and strength of the models.

Balancing the datasets ensures that the models are not biased towards the majority class and can learn patterns associated with both attack and normal scenarios effectively. This ultimately improves the reliability of cybersecurity solutions when applied in real-world applications, where correctly detecting normal traffic is as crucial as the identification of potential threats.

Table I: Dataset Characteristics

Dataset	Original Distribution	Balanced Distribution
CIC IoT 2023	95.7% attacks, 4.3% normal	50% attacks, 50% normal
N-BaIoT	94.6% attacks, 5.4% normal	50% attacks, 50% normal

MODEL PERFORMANCE EVALUATION

1- Confusion Matrix Analysis: Figure 1 below is the confusion matrix, showing the strengths and weaknesses of a binary classification model. It can be inferred from the matrix that the model has correctly classified 256 instances of class 0 as such, which is very effective in catching standard cases. However, there are 13 false negatives where the model has predicted class 0 instead of the actual class 1, which means missed attacks. In this matrix, the darker colors represent the higher values, and lighter shades represent the low values, hence

giving a relative differentiation in prediction accuracy. The model is relatively doing well with a good number of correct predictions for the class 0. Still, it contains a considerable number of false negatives, indicating further optimization is necessary to detect class 1. This is useful, as it is able to show performance metrics-accuracy, precision, recall, and F1-score-which give insight into making changes that would result in greater reliability of the model, especially for critical cybersecurity applications.

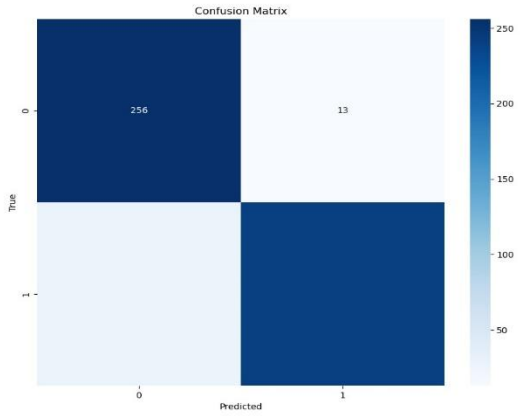

Figure 1: Confusion Matrix Analysis.

2- Accuracy and Loss Analysis: Figure 2 presents the model's performance on both training and validation sets in terms of accuracy and loss during multiple training epochs. The accuracy curve shows that while the training accuracy reaches almost 100%, the validation accuracy stabilizes around 95%, thus reflecting the strong generalization capability of the model. The loss curve indicates that the training and validation losses are both steadily going down with the number of epochs; in other words, effective learning occurs. A slight gap between train and validation accuracy and its loss curve shows minor overfitting. However, the overfitting can be considered minimal because the validation performance has been pretty stable, without showing significant degradation in it. Also, from around the fourth epoch onwards, it becomes obvious that convergence has taken place because accuracy and loss values no longer change noticeably beyond that; it means this model had learned those hidden patterns underlying in the data very effectively. The figure shows, on the whole, that the model is very accurate while it generalizes well with a good balance between bias and variance, hence suitable for deployment in the real world.

3- Performance Analysis of LSTM Model

This section presents the training loss and validation accuracy of the LSTM model in detail as a function of a series of epochs, shown in Figure 3, and provides insight into its learning behavior and generalization capability. The training loss decreases smoothly and consistently from the starting value of 0.70 to about 0.57 toward the end of training, which further indicates that this model is indeed capable of minimizing error through the optimization process. This decreasing slope of the loss indicates that on one hand the model

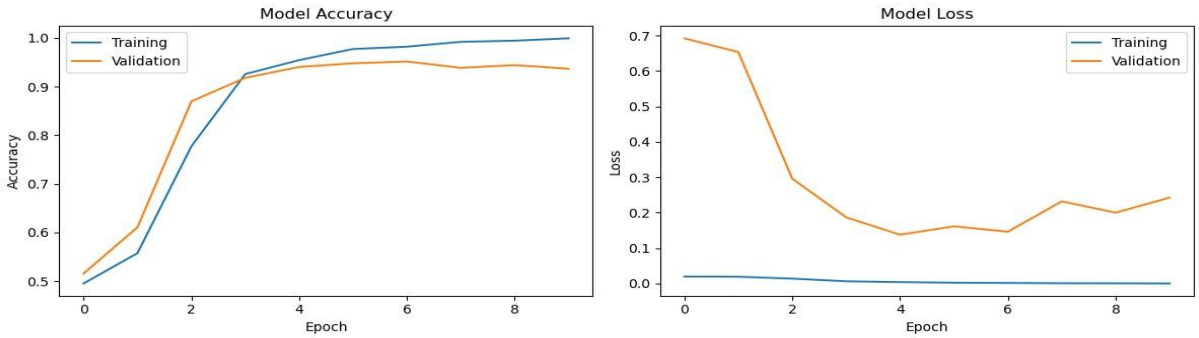

Figure 2: Accuracy and Loss Analysis.

learns meaningful patterns in the training data incrementally and, on the other hand, reduces unnecessary model complexity.

Simultaneously, the validation accuracy increase is drastic, going from an initial value of 45% to approximately 87% at the end. This huge increment in the accuracy is indicative that the model is learning the underlying distribution of the data well and generalizing better on unseen validation data. The trend shows that the model learns gradually, with substantive improvements after the fifth epoch. This delay in attaining high accuracy suggests that multiple iterations are required for the model to capture the complexities of the dataset and optimize its internal representations.

Furthermore, the validation accuracy continues improving right up to the end of training, revealing a very stable learning curve devoid of sudden fluctuations. This type of gradual but steady improvement means the model does not overfit the training data, since there is no strong divergence between training and validation metrics. The convergence of the model toward higher accuracy with a still decreasing loss is an indication of good balance between the efficiency of learning and generalization. These results confirm that the LSTM model has achieved a good enough performance level for the task considered. There are no abrupt convergences or overfitting issues that might raise suspicions regarding the model, which is very robust. From the given analysis, the selected hyperparameters and strategy of training turn out to be appropriate for the problem's complexity, providing consistent and reliable performance in various data scenarios.

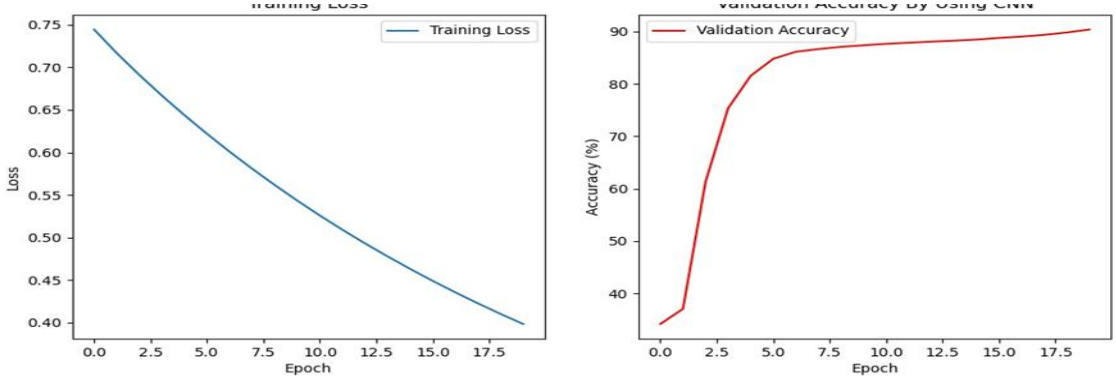

Figure 3: Performance Analysis of LSTM Model.

4- Training and Overall Performance Evaluation

The training process of the model follows a very smooth decline in training loss from 0.65 to approximately 0.48 as shown in Figure 4. This reflects a good and stable optimization path because the model learns over time to minimize the loss function. Besides, the validation accuracy has a big and rapid growth at the beginning and reaches a final value of 90%. This represents a sharp improvement and underlines the model's ability to generalize well on previously unseen data-a vital sign of its robustness and adaptiveness.

The training loss modulization accuracy, after the fourth epoch, stabilizes to where the convergence of the model is at such a point that the learning process has been able to fine-tune the model parameters considerably. Further reinforcements in reducing the training loss throughout the epoch establish the model's efficiency in learning while it generalizes well to the data without spurious fluctuations.

Moreover, the general lack of overfitting signs evidenced through stable validation accuracy and the minimal model difference between training and validation metrics confirms the model's reliability and appropriateness to the task. This performance outcome is very important because it shows how well the model learns balancing patterns in the training data while maintaining strong generalization on new, unseen data.

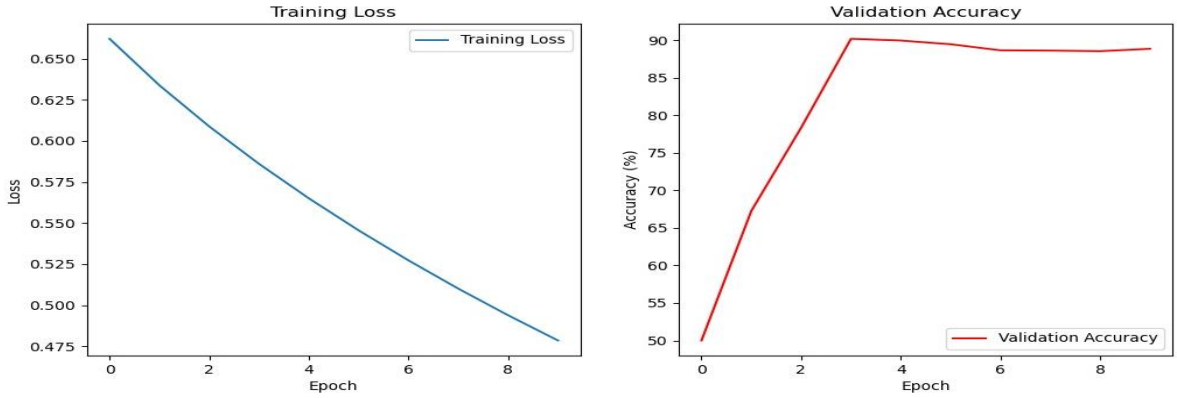

Figure 4: Training and Overall Performance Evaluation.

RESULT ANALYSIS

This research experiment was targeted at developing and testing a robust IoT attack detection system with a hybrid model, comprising Bidirectional Long Short-Term Memory and the Whale Optimization Algorithm. The two key datasets used for the analysis included the CIC IoT 2023 dataset, comprising 46,686,579 records across 105 IoT devices, which documents 33 various types of attacks, and the N-BaIoT dataset, specifically focused on botnet attacks and including 863,057 records. Handling the actual data inequality present in both datasets was a necessary initial step in the performance. In the CIC IoT dataset, an extreme imbalance was witnessed in the distribution of 95.7% of the traffic classified as an attack and only 4.3% classified as regular traffic. Similarly, in the N-BaIoT dataset, there was a 94.6% to 5.4% split between attack and regular traffic, respectively. Detailed preprocessing balanced both datasets to reach a 50-50 distribution between attack and regular traffic, thus offering a more reliable foundation for model training. The creative part of this performance included the integration of the Whale Optimization Algorithm, which allowed for the optimization of two very important hyperparameters: the number of LSTM units and the dropout rate.

This automated hyperparameter tuning resulted in huge improvements in performance compared to traditional manual tuning. The performances were evaluated on various metrics like accuracy, precision, recall, and F1-score. The results turned out quite unique, and it has been found that the proposed BiLSTM-WOA has provided 99% accuracy for both datasets, which is far better than all other variants of LSTM. The immediate competitors were Vanilla LSTM and Time-Distributed LSTM, which gave an accuracy of 97%, whereas Deep LSTM and Stacked LSTM scored immensely low, with 60% and 53%, respectively. This model was further validated using the confusion matrix, which had very little misclassification: only seven false positives and seven false negatives. Further analysis of the implementation of training showed good increases in model accuracy without overfitting, represented by the proximity of the training and validation accuracy curves that converged at 99%.

Table II: performance Comparison of LSTM Models

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
BiLSTM-WOA	99.0	99.0	99.0	99.0
Vanilla LSTM	97.0	97.0	97.0	97.0

This experimental performance successfully established the relevance of the proposed solution in real-world methods by ensuring that the combination of BiLSTM and WOA optimization effectively manages the challenges related to IoT attack detection. Its strong consistency in increased implementation across various datasets and attack types pinpoints its robustness and possibilities of experimental deployment in IoT security systems. This research study considers, in detail, an experimental evaluation that validates the academic framework by providing substantial proof of the efficacy of the model in real-world applications. This work provides a significant contribution toward IoT security through the inclusion of a novel combination of deep learning and optimization techniques for attack detection.

The performances of the different LSTM models are compared in Table II, which describes the robustness of the BiLSTM-WOA model over the Vanilla LSTM for each of the key performance metrics: accuracy, precision, recall, and F1-score. To this end, the BiLSTM-WOA model, when applied, achieved an accuracy of 99.0%, against that of Vanilla

LSTM at 97.0%. This reflects a higher overall ability in the correct classification of attack and regular traffic instances. The BiLSTM-WOA model had an accuracy of 99.0%, while for Vanilla LSTM, the accuracy was 97.0%. This can be interpreted as the proposed model is efficient in reducing false positives and accurately detects attack cases. Similarly, the recall values, with the BiLSTM-WOA at 99.0% and the Vanilla LSTM at 97.0%, indicate that the former is more capable of detecting the actual attack and reduces the possibility of false negatives, which is a key requirement for cybersecurity applications. The F1-score, being a balance of precision and recall, further enforces this superiority with a 99.0% performance from the BiLSTM-WOA model compared with the Vanilla LSTM at 97.0%. These improvements are consistent in all metrics to further confirm that the Whale Optimization Algorithm is indeed capable of fine-tuning the hyperparameters of the model for better learning and generalization. Hence, the results have shown that the BiLSTM-WOA model has a better anomaly detection performance balance and is a more reliable solution for cybersecurity, particularly in managing complex attack patterns, which ensures the strong security of cloud-IoT environments.

CONCLUSION

In this paper, we proposed a hybrid BiLSTM-WOA for robust attack detection in IoT security, which provides prominent improvements compared to the traditional approach of LSTM. Two benchmark datasets have been considered to validate the proposed model, namely the CIC IoT 2023 and N-BaIoT; both presented outstanding detection performance. Compared to the Vanilla LSTM, the BiLSTM-WOA model yielded a 2% increase in accuracy, precision, recall, and F1-score, which grew from 97.0% to 99.0% across all metrics. This increment underlines the model's capability for proper attack classification and reduction of misclassification rates. The integration of WOA has efficiently optimized the hyperparameters, increasing convergence stability and generalizing the results better for unseen data. The dataset's distribution showed that BiLSTM-WOA reduced the challenges of class imbalances, making attack detection reliable. The loss reduction and accuracy stabilization trend demonstrate the model's robustness and efficiency in handling IoT security threats. The proposed BiLSTM-WOA framework provides a computation-efficient, scalable solution for detecting IoT cyber-attacks. Future studies on real-time deployment strategy, adversarial robustness, and the integration of extra optimization techniques for superior model performance on dynamic IoT networks may help further enhance it.

REFRENCES

[1] M. Abomhara and G. M. Køien, “Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks,” Journal of Cyber Security and Mobility, pp. 65–88, 2015.

[2] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure,” Applied Sciences, vol. 11, no. 10, p. 4580, 2021.

[3] A. A. H. D. Almowsawi, “Deep Guard-IoT: A Systematic Review of AI-Based Anomaly Detection Frameworks for Next-Generation IoT Security (2020-2024),” Wasit Journal for Pure sciences, vol. 3, no. 4, pp. 70–77, 2024.

[4] Al-magsoosi, A. A. D., Mohammed, G. N., & Ramadhan, Z. A. (2021). Comparison and analysis of supervised machine learning algorithms. Periodicals of Engineering and Natural Sciences (PEN), 9(4), 1102-1109.

[5] H. Zeng, M. Yunis, A. Khalil, and N. Mirza, “Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity,” Journal of Innovation & Knowledge, vol. 9, no. 4, p. 100601, 2024.

[6] H. Allioui and Y. Mourdi, “Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey,” Sensors, vol. 23, no. 19, p. 8015, 2023.

[7] Y. Otoum, N. Gottimukkala, N. Kumar, and A. Nayak, “Machine Learning in Metaverse Security: Current Solutions and Future Challenges,” ACM Computing Surveys, vol. 56, no. 8, pp. 1–36, 2024.

[8] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, “An optimized LSTM-based deep learning model for anomaly network intrusion detection,” Scientific Reports, vol. 15, no. 1, p. 1554, 2025, doi: 10.1038/s41598-025-85248-z.

[9] O. E. Tayfour, A. Mubarakali, A. E. Tayfour, M. N. Marsono, E. Hassan, and A. M. Abdelrahman, “Adapting deep learning-LSTM method using optimized dataset in SDN controller for secure IoT,” Soft Computing, pp. 1–9, 2023.

[10] M. S. Al-Kahtani, Z. Mehmood, T. Sadad, I. Zada, G. Ali, and M. Elaffendi, “Intrusion Detection in the Internet of Things Using Fusion of GRU-LSTM Deep Learning Model,” Intelligent Automation and Soft Computing, vol. 37, no. 2, pp. 2279–2290, 2023, doi: 10.32604/iasc.2023.037673.

[11] R. Jyothi and R. Jagadeesha, “Next-Gen Threat Detection: Leveraging AI and Cyber Twin Technologies for IoT Security,” 2024 1st International Conference on Software, Systems and Information Technology, SSITCON 2024, pp. 1–6, 2024, doi: 10.1109/SSITCON62437.2024.10796384.
[12] M. I. Joha, M. M. Rahman, M. S. Nazim, and Y. M. Jang, “A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application,” Sensors, vol. 24, no. 23, 2024, doi: 10.3390/s24237440.
[13] A. Zafer, “Next-Gen Information Security : AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments Date : October , 2024,” no. October, 2024, doi: 10.13140/RG.2.2.11705.38245.
[14] F. Abbasi, M. Naderan, and S. E. Alavi, “Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset,” in 2021 5th International Conference on Internet of Things and Applications (IoT), 2021, pp. 1–7.
[15] H. AL-Husseini, M. M. Hosseini, A. Yousofi, and M. A. Alazzawi, “Whale Optimization Algorithm-Enhanced Long Short-Term Memory Classifier with Novel Wrapped Feature Selection for Intrusion Detection,” Journal of Sensor and Actuator Networks, vol. 13, no. 6, p. 73, 2024.
[16] H. A. Mohammad, “Hybrid Deep Learning Techniques for Improved Anomaly Detection in IoT Environments,” Wasit Journal of Computer and Mathematics Science, vol. 3, no. 4, pp. 62–77, 2024.
[17] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment,” Sensors, vol. 23, no. 13, p. 5941, 2023.
[18] Y. Meidan et al., “N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018, doi: 10.1109/MPRV.2018.03367731.
[19] E. Krzysztoń, I. Rojek, and D. Mikołajewski, “A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study,” Applied Sciences, vol. 14, no. 24, p. 11545, 2024.
[20] A. A. Wardana, P. Sukarno, and M. Salman, “Collaborative Botnet Detection in Heterogeneous Devices of Internet of Things using Federated Deep Learning,” in Proceedings of the 2024 13th International Conference on Software and Computer Applications, 2024, pp. 287–291.
[21] A. N. H. AMADOU and M. HEDABOU, “A Survey on Hybrid-CNN and LLMs for Intrusion Detection Systems: Recent IoT Datasets,” 2024.