Enhancing IoT Security: A Deep Learning and Active Learning Approach to Intrusion Detection

Hawraa Fadel Mahdi [1*], Ban Jawad Khadhim [2]
[1, 2] Department of Computers College of Basic Education, University of Diyala, Diyala, Iraq
Email: [1] hawraamahdi@uodiyala.edu.iq, [2] BanJawad@uodiyala.edu.iq
*Corresponding Author

***Abstract*—In response to the escalating demand for robust security solutions in increasingly complex Internet of Things (IoT) networks, this study introduces an advanced Intrusion Detection System (IDS) leveraging both deep learning and active learning techniques. This research addresses the unique challenges posed by IoT environments, such as limited resources and diverse network components, which traditional security measures fail to adequately protect. Employing a BiLSTM model integrated with an active learning strategy, our approach achieved impressive results, including precision, recall, and F1-scores close to 1, and a total accuracy of 0.99. The inclusion of active learning enables the IDS to focus on the most informative data subsets, enhancing processing efficiency and reducing computational demands essential for IoT contexts. This method demonstrates significant promise for detecting sophisticated cyber threats and providing an effective tool for real-world applications. The performance of the proposed model has been rigorously validated on well-established cybersecurity datasets and through simulations in an IoT network environment, confirming its scalability and efficiency. Future work will address potential limitations such as computational demands and adaptability to diverse IoT device architectures, ensuring broader applicability and robustness of the IDS in varied IoT scenarios.**

Keywords—Internet of Things (IoT); Intrusion Detection System; Active Learning; Deep Learning; Bidirectional Long Short-Term Memory.

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) technology across both domestic and industrial sectors underscores the critical importance of robust network security [1]. IoT devices, characterized by their limited memory, low energy capacity, and bandwidth constraints, present unique challenges [3][4]. Furthermore, the expansive and dynamic nature of IoT networks renders traditional security measures ineffective, necessitating innovative solutions [2][3].

Recognizing these challenges, recent academic advancements propose a novel approach to fortifying IoT security through the integration of active learning and deep learning techniques [5][6]. These methods are poised to transform next-generation intrusion protection technologies by addressing the specific vulnerabilities inherent in IoT environments.

IoT networks enable a broad range of functionalities, from simple home automation to intricate industrial systems, significantly increasing the number of connected devices and, consequently, the potential surface for cyber threats [2][3]. Traditional security solutions, designed for more static network environments, fall short in the face of the diverse and evolving nature of IoT ecosystems [2][4]. Moreover, the sophistication of attack vectors employed against IoT networks continues to grow, allowing attackers to exploit vulnerabilities more effectively [3][4].

In response to these challenges, there has been significant progress in machine learning and deep learning. Models such as convolutional neural networks (CNNs) and multi-layer perceptrons (MLPs) have demonstrated their capability to detect patterns and anomalies effectively, which are crucial for identifying security threats [6][8]. However, the practical application of these models in IoT security must take into account their computational complexity and the operational constraints of IoT devices [5][6].

To address these considerations, our methodology employs an active learning mechanism that selectively processes the most informative data points from a given dataset [7][9]. This strategy is particularly effective in IoT settings, where data reduction and minimal system stress are paramount. The integration of active learning with deep learning enables our Intrusion Detection System (IDS) to adapt to evolving threats and anomalous behaviors dynamically, without the need for retraining the entire dataset [9].

At the heart of our approach is a novel hybrid IDS, which combines CNNs and MLPs within an active learning framework [10][11]. This model continuously learns from network traffic and user activities specific to IoT environments, focusing on anomalies so rare they are likely indicative of security threats [11][12]. The active learning component enhances the model's accuracy over time without necessitating frequent retraining on large datasets, thus avoiding system overload [10][12].

Our IDS has been rigorously trained and validated using established cybersecurity datasets like NSL-KDD [13] and BoT-IoT [14], which encompass a variety of attack scenarios. These datasets provide a solid foundation for testing our IDS in controlled, real-world conditions [15][16]. Additionally, we have simulated an IoT network environment to evaluate how the IDS performs in real-time intrusion detection and assess its compatibility with the constraints of IoT devices [10][11][16][17].

We anticipate that our deep learning and active learning-based IDS will significantly improve the detection of advanced cyber threats within IoT networks. By prioritizing the learning and response to rare but critical incidents, our system offers a scalable, efficient, and effective solution tailored for the unique requirements of modern IoT infrastructures [18][20]. This research not only enhances IoT security but also serves as a benchmark for future advancements in cybersecurity for interconnected devices [19][20].

The research contribution in our article is as follows:

- Introduces a novel Intrusion Detection System (IDS) that integrates Bidirectional Long Short-Term Memory (BiLSTM) networks with active learning techniques. This innovative approach addresses the dynamic and resource-constrained nature of IoT environments by enhancing intrusion detection accuracy while minimizing computational demands.
- Presents a thorough evaluation of the proposed IDS using the diverse ToN_IoT dataset, which encompasses a wide range of real-world cyber-attack scenarios. This validation highlights the robustness and scalability of the model in practical IoT settings.
- Demonstrates the effective use of active learning to efficiently manage and label data amidst evolving cyber threats, offering a more adaptable and resource-efficient solution for IoT security.

The structure of the article is designed to provide a comprehensive examination of the proposed IDS and its effectiveness in IoT environments. It begins with a review of relevant literature in the RELATED WORKS section, setting the context and identifying gaps addressed by this study. The METHODOLOGY section details the dataset overview, data preprocessing techniques, and the core components of the BiLSTM model and active learning approach, culminating in the integration of these methods. The EVALUATION METRICS section outlines the criteria used to assess the model's performance. EXPERIMENTAL RESULTS presents the findings from both the standalone BiLSTM model and the combined BiLSTM with active learning. The COMPARATIVE ANALYSIS evaluates the proposed model against existing approaches. The DISCUSSION interprets the results and their implications, while the CONCLUSION summarizes the key contributions and suggests future directions for research.

II. Related Works

This paper [21] explores the integration of active learning strategies in online intrusion detection systems (IDSs) to optimize labeling costs without compromising classification performance. The authors leverage machine learning techniques, particularly focusing on a lightweight Naive Bayes classifier, to distinguish between benign and malicious network flows. They challenge the conventional belief that more data always results in better performance, showing instead that a well-curated subset of data can significantly enhance performance. Employing an active learning approach, they compare the Least Confidence strategy against their proposed method. Both methods begin with 5% of the training set, adapting the inclusion of data based on network flow characteristics. The results indicate their method achieves a maximum AUC score of 90%, outperforming the Least Confidence strategy by 5%. The study demonstrates that optimal performance is achieved when approximately 10% of the training data is used, suggesting a smaller, more precise subset of training data is more effective than a larger, less targeted set.

This paper [22] explores the increasing problem of technology security in the era of the Internet of Things and suggests machine learning as an opportunity for improving the security of the IoT network. The study uses machine learning and deep learning approaches for addressing security gaps in detecting various types of attacks on the IoT network. In particular, the paper investigates the detection of Denial-of-Service attacks using deep learning. The study applies Python with the following packages scikit-learn, TensorFlow, and seaborn to compare algorithm performance in detecting different types of attacks.

The findings indicate that the deep learning model, and especially Convolutional Neural Network, has a high performance across different metrics, including AUC for different types of attacks. For example, the AUC scores for CNN model reach 0.98 and higher for DoS attack type, reconnaissance type, and normal traffic, which means that CNN model detects potential threats with 98% accuracy. The research implication for practice implies that the security of IoT networks can significantly benefit from deep learning's algorithms, which increase performance by detecting potential threats much more precisely, making possible to organize effective attack mitigation strategies.

This paper [23] presents a novel approach to intrusion detection systems in IoT networks. Existing systems have shown to lack Multiview feature fusion and have an inadequate semantic relationship capture. This results in reduced performance or robustness and in addressing real-time attack detection. The method aims to maximize IDS using deep learning and knowledge graph technology. In this process, through knowledge graph and statistical analysis, semantic relationships and key features are extracted to convert IoT network requests into word vectors through Multiview feature fusion and fusion. To identify malicious request attacks, an attention-based CNN-BiLSTM model that can capture long-distance dependencies and context semantics is used. The proposed model's performance is superior to existing ones in terms of robustness, feature selection, accuracy, and the ability to reduce false alarm rates. Thus, the IDS can achieve an accuracy of 90.01%, accurately identify various types of stealthy attacks such as DoS and Probe R2L, U2L, and extract semantic relationships between features. The precision, recall, and F1-score metrics show that proposed approach can accurately identify relationships, normal, and DoS attack patterns. Hence, the proposed work can improve the security of IoT networks.

This paper [24] presents a novel approach to the intrusion detection system that is specialized for IoT networks and utilizes advanced deep learning methodologies to strengthen existing means of cybersecurity protection. More specifically, this approach utilizes Feed Forward Neural Networks, Long Short-Term Memory and Random Neural Networks to detect and reduce the flood of different types of cyberattacks aimed at the IoT. In particular, each of these deep learning models has the following strengths: FFNN is very good at complex patterns of traffic, LSTM has access to long-term dependencies of data in a network, and Random Neural Networks can easily learn new things about every threat that appears due to its dynamic learning. The IDS was tested against the CIC-IoT22 dataset, which resulted in IDS being able to detect the intrusions with 99.93%, 99.85% and 96.42% accuracy for FFNN, LSTM and RandNN, respectively. The importance of these findings is related to the capability of the proposed deep learning-based approach to provide rapid responses to emerging security issues, thereby strengthening the security resilience of IoT networks.

This paper [25] demonstrates a new method for Network Intrusion Detection based on multi-head attention and BiLSTM models. This model is designed to work with intrusion detection data sets with high-dimensional vectors and imbalanced categories. By using different attention weights to each of the vectors inside of the feature vector, based as the encoding of the detection attack type, the relationship is strengthened to achieve a better detection. Use of BiLSTM enables the capture long-range dependency features from BiLSTM and the better detection. When both models were combined, with a drop-out layer to prevent overfitting, the overall detection was significantly improved, while reducing overtraining when learning. As the experiment shows, this method is appropriate as the network intrusion detection model had accuracies of 98.29%, 95.19%, and 99.08% for KDDCUP99, NSLKDD, and CICIDS2017 data set, respectively. In addition to outperforming the existing method, the result can be used to combat security threats and guarantee network security.

This paper [26] proposes a novel IDS for IOT networks based on machine learning, and specifically on deep learning techniques Bi-LSTM and CNN. The BiILSTM-CNN hybrid IDS model Combines the benefits of temporal and spatial character extraction of the Bi-LSTM and CNN methods. An UNSW-NB 15 dataset is used to test the BiLSTM and CNN models individually to compare their performance with the hybrid model in terms of detection performance. Various performance measurement metrics like Sensitivity, Precision, Matthews Correlation Coefficient, and F1-Score indicate that the hybrid model is better than stand-by-alone BiLSTM and CNN models in every aspect.

The hybrid model outperforms the existing state-of-the-art approaches, proving that it can significantly enhance network security and improve IDS against modern intrusion attacks. The paper also shows the statistics of the training in order to determine the improvement in the accuracy and loss function, which further strengthens the validity of the proposed model.

This paper [27] introduces a novel technique for measuring the vulnerability of ML-based Intrusion Detection Systems to adversarial attacks. An adversarial attack is an attack in which the attacker makes minor changes to input characteristics to the point that the model no longer identifies the attacks, essentially bypassing the ML model's binary classification. created a way to assess the susceptibility of ML-based IDS to adversarial attacks using active learning and generative adversarial networks that do not need prior knowledge of the IDS model but its binary classification level. The study found that experimental outcomes of the proposed technique were successful, with a 98.86% success rate in bypassing the IDS model. It is crucial to mention that the paper includes not only a DNN-based IDS but also included a gradient boosted decision tree, which shows that the theory is largely valid. Moreover, reveals training of the Variational

This paper [28] proposes a novel framework to optimize the intrusion detection system in terms of both feature extraction and selection using deep learning and metaheuristic optimization in IoT environments. The framework is designed to enhance the system's ability to distinguish between normal and malicious behavior using a Convolutional Neural Network as the primary feature extractor. CNN is a class of feed forward artificial neural networks that find the meaningful representations of input data in a lower-dimensional space. Feature selection is conducted by the proposed Reptile Search Algorithm (RSA), a metaheuristic algorithm inspired by how a crocodile selects its prey.

The proposed approach is experimentally carried out on four datasets: KDDCup-99, NSL-KDD, CICIDS-2017, and BoT-IoT, as presents in Table I. Comparative results with various optimization techniques as demonstrated in the study confirm that the feature merit of CNN for extraction is very competitive with known methods, as is the feature selection using the RSA algorithm.

TABLE I. SUMMARY OF PREVIOUS WORK

Paper	Models used	Results
[21]	Naive Bayes, active learning (Least Confidence strategy, proposed method)	Maximum AUC score of 90%, outperforming Least Confidence by 5%
[22]	Deep learning (CNN), Python, scikit-learn, TensorFlow, Seaborn	CNN model achieves AUC scores of 0.98 or higher for detecting various attacks
[23]	CNN-BiLSTM with knowledge graphs, multiview feature fusion	Detection accuracy of 90.01%, high precision, recall, and F1-score
[24]	FFNN, LSTM, RandNN	High accuracy rates: FFNN (99.93%), LSTM (99.85%), RandNN (96.42%)
[25]	BiLSTM, multi-head attention, dropout layer	High accuracies on multiple datasets (up to 99.08%)
[26]	BiLSTM-CNN hybrid, using UNSW-NB 15 dataset	Outperforms standalone models and existing approaches in multiple metrics
[27]	Active learning, GANs, VAE	98.86% success rate in bypassing IDS with minimal labeled data
[28]	CNN, Reptile Search Algorithm (RSA)	Effective feature selection and classification across multiple datasets

III. METHODOLOGY

The process of developing a binary classification model using BiLSTM, coupled with an active learning approach, entails several systematic steps [30][31], as shown in Fig. 1. Initially, the methodology begins with data acquisition. This step involves collecting and preparing IoT network traffic data [32][33]. Such preparation helps in understanding both typical and atypical behaviors within the network [32] [34] [35].

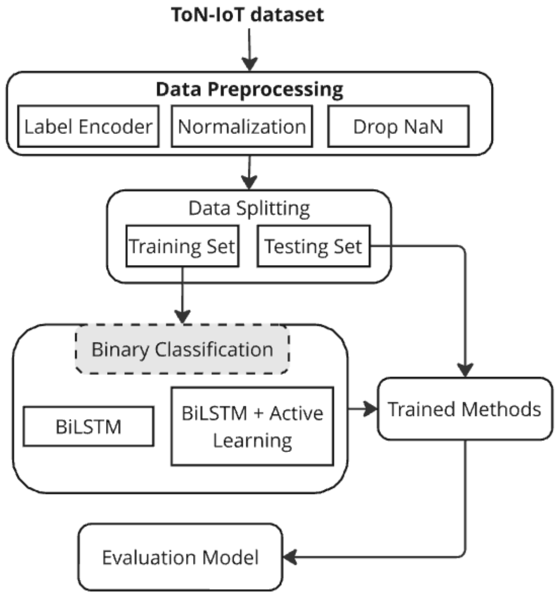


Fig. 1. The proposed methodology

Following data collection, the next step involves scaling the features [36][37]. Feature scaling is crucial as it normalizes the dataset, ensuring that the input data is uniform. This uniformity allows deep learning models to process the data more effectively.

The core of our methodology is the application of the BiLSTM model for binary classification [38][30]. The BiLSTM model is particularly well-suited for time-series data, such as network traffic [38]. Its ability to maintain information over an extended period makes it effective in detecting complex intrusion patterns.

In addition to the BiLSTM model, we integrate an active learning approach [39][40]. This approach involves sorting the instances in a data pool and querying the most informative ones for inclusion in the training set. We implement this strategy through a series of iterations. During these iterations, the model selects the least confident predictions to acquire new labels [39][40]. This selective labeling allows the model to utilize the limited labeled data efficiently and refine its accuracy progressively [40].

The training process includes dividing the data into initial training and test sets. We then make further subdivisions to manage the reserved pool of unlabeled training data effectively [41][42]. The retraining process is iterative. With each iteration, the model incorporates newly labeled data, which enhances its performance [41][42].

The final step in our methodology is the evaluation phase [43]. In this phase, we test the model using the reserved test dataset. We focus on assessing its classification performance and accuracy, particularly through metrics such as precision and recall. We visualize these results using confusion matrices and other reporting tools. These tools help to illustrate the model's effectiveness in detecting and identifying network intrusion attempts [44].

This structured approach merges deep learning and active learning techniques. It provides a robust framework for enhancing IoT security [45].

A. Datset Overview

The ‘ToN_IoT’ dataset comprises a wide range of data sources [46]. Its datasets such as telemetry data from IoT and IIoT sensors, operating systems’ data from Windows 7 and 10 and Ubuntu 14 and 18 TLS, and network traffic were gathered from a highly sophisticated and extensive network purposefully designed at the Cyber Range and IoT Labs at the School of Engineering and Information Technology at UNSW Canberra @ the Australian Defence Force Academy (ADFA) SEIT/UNSW Canberra Specifically, a unique and unprecedented testbed network built based on the industry 4.0 standards consisting of the IoT and IIoT networks were established [29].

The testbed, which utilized a variety of virtual machines and hosts running Windows, Linux, and Kali operating systems, facilitated the interconnected functioning of IoT, Cloud, and Edge/Fog layers. It was employed to simulate a range of cyber-attack scenarios including DoS, DDoS, and ransomware attacks targeting web applications, IoT gateways, and computer systems within the IoT/IIoT network. Data collection occurred in real-time through parallel processing, capturing a wide array of both normal activities and cyber-attack events from network traffic, Windows and Linux audit trails, and IoT service telemetry.

Raw datasets encompassed various formats and sources:

- IoT/IIoT Data: Telemetry data from over 10 types of IoT and IIoT sensors, including weather and Modbus sensors, were recorded in log and CSV files.
- Network Data: This was primarily collected in packet capture (pcap) formats, alongside log files and CSV files generated by the ZEEK (formerly Bro) network monitoring tool.
- Linux Data**: On Ubuntu 14 and 18 systems, a tracing tool known as atop was utilized to log detailed information about disk, process, processor, memory, and network activities. The collected data was stored in TXT and CSV file formats.
- Windows Data: Data collection on Windows 7 and 10 systems was performed using the Performance Monitor Tool. The initial data was captured in a .blg format, which is specific to the Performance Monitor Tool, and subsequently processed into CSV files to document disk, process, processor, memory, and network activities comprehensively.

B. Data Preprocessing Methodology

The preprocessing steps within the provided code given above include essential procedures to prepare IoT device data for a model to detect intrusions [47]. First, one gets rid of irrelevant columns in the dataset, such as “label” and “type” [48], as presents in Fig. 2. Then, the target variable is split into a separate y that contains binary labels to define each traffic instance as a normal connection or an attack.

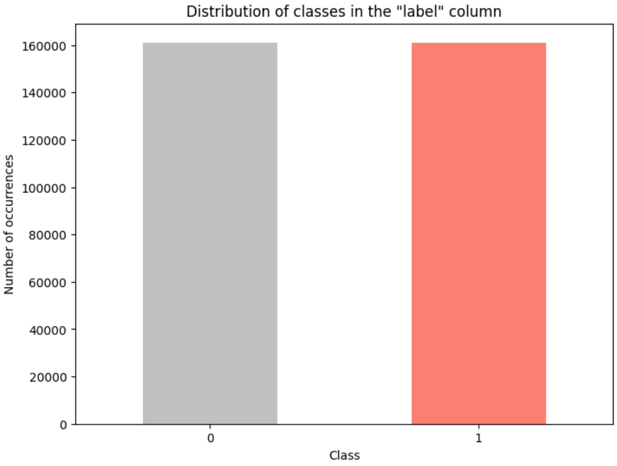


Fig. 2. Label class desctribution

Since there are still columns with object data type in the X columns, one employs the LabelEncoder from sklearn. preprocessing to transform such information into a numerical form that the ML model could better read and analyze adequately. Subsequently, it is easier to start training the model when all the data variables are numbers.

The normalization of feature values is done using MinMaxScaler, which adjusts the values of the features to have a common scale value of between 0 and 1 [49]. Such scaling is important for neural networks and other gradient-based learning algorithms because low-level values in the algorithm may not perform well when the input numerical values vary in a wide range.

The NAN values checking across the dataset ensures the quality and readiness of the data for training, as it implies that the problem has issues with data completeness or problems with the collection and entry of the data [50]. The cleaned and scaled dataset is split into training and test sets [51] where 80% of the data is used to train the model and 20% is withheld for testing purposes. Such a split helps in validating the model by testing it against a set of data it was not trained on to determine its generalization tendencies beyond a set of data.

The code also includes a comprehensive suite for evaluating the performance of the classifier once it has been trained [60]. Several metrics are reported: high-level accuracy and error rates as well as confusion matrix to visualize the types and frequencies of classification errors [65]. Moreover, the more detailed analysis is presented in the classification report, which contains precision, recall, and F1-scores broken down for each class. They are especially useful for verifying the model's strengths and weaknesses for specific types of intrusion. Other calculated metrics are sensitivity and specificity for each class.

Sensitivity or recall is the proportion of actual positives which are correctly identified by the model and is of critical importance for intrusion detection systems since missing an actual intrusion can be very costly. Specificity is the complement of sensitivity and measures the proportion of actual negatives correctly identified, and is important for ensuring that the system does not over-tag normal behavior as intrusive.

In combination, these preprocessing and evaluation procedures create a strong framework for building and testing a machine learning model designed to successfully detect and categorize likely security threats within an IoT network. From the described steps, it is evident that not only the training data, but the trained model should meet a high-quality bar required for applications in cybersecurity.

C. Bi-directional Long Short-Term Memory BILSTM

BiLSTM is a more advanced iteration of LSTM [67][68][69], a recurrent neural network that excels in capturing long-term dependencies in sequence data [54]. The BiLSTM advantage lies in no way in which it is trained as mentioned above, for instead of processing information sequentially, they take in the data both forwards and backwards, meaning they consider the context of the past and future observations on the sequence dataset. Because of this specific feature, BiLSTMs are particularly well-suited to tasks where understanding the entire sequence is essential, such as natural language processing [53], speech recognition, and time-series prediction. By processing each sequence from both directions, they gain a better understanding of the pattern and can predict it more accurately than their standard LSTM counterparts [54]. BiLSTMs are especially beneficial when the previous and upcoming state of an observation is crucial to understand and predict it accurately.

Setup and training of a Bidirectional Long Short-Term Memory network. This model constructed utilizing Keras – an advanced neural networks API. BiLSTM is an improvement of conventional Long Short-Term Memory networks. BiLSTM learns to handle data in both forward and reverse directions, allowing it to carry information about both the future and past to a node. This kind of model, which is beneficial for applications that require considering the whole context where the predictions are reliant is an example of a sequence prediction task.

The BiLSTM network is built in a sequential manner and structured at the end of the configuration with three layers consisting of decreasing units. Paired with each of the hidden layers is a dropout layer set at 0.2 [70]. They function throughout training by randomly deactivating certain nodes, effectively aiding in the prevention of overfitting. The sigmoid activation function [71] is employed in the output layer of the model, making it well-suited for binary classification in this application. suitable for this application domain since an intrusion is either classified as normal or an anomaly.

For optimization, the model uses the Adam optimizer as it consumes very little memory and is very efficient and binary crossentropy for calculating loss [55]. Binary crossentropy is a widely used loss function in binary classification tasks. Furthermore, it uses an early stopping callback to avoid potential overfitting, which stops training the model if validation loss does not decrease in three consecutive epochs.

As a result, the model was trained for 10 epochs with batches of 32 samples. Finally, the model's performance is evaluated on a test dataset with accuracy and confusion matrix and full classification report. The model exhibits high metrics with regard to precision, recall, F1-scores, indicating the high potential of BiLSTM to process sequences enabling its application for the prediction of future data points such as time series, detecting network intrusion as temporal sequence is crucial for precise predictions.

D. Active Learning

Active learning is a type of machine learning in which instead of training the model on all the data, the algorithm queries the user to label the new data points that can maximize learning from the least number of new additional labels [52]. While conventional strategies rely on training a model on a machine-labeled dataset, active learning is a dynamic method through which the model learns from the user's labeling. Whether data with high uncertainty or data that is very unique, the most valuable data is labeled.

They are more beneficial in cases where labeling the entire data is capital intensive on its resources and time that can be expensive to the model. It can be effectively in image classification, natural language processing and any other field where getting additional labeled data can be expensive or unfeasible. They help to achieve the best training throughput by training data that fully influences their learning.

E. BILSTM+Active

The integration of active learning with a Bidirectional Long Short-Term Memory (BiLSTM) model is strategically employed to enhance the training process for binary classification. Initially, the dataset is partitioned into initial training and pool sets. The BiLSTM model's architecture is designed sequentially, incorporating multiple layers and dropout layers to improve regularization and facilitate the differentiation between the two classes using a sigmoid activation function [63].

In terms of optimization and loss calculation, the Adam optimizer and binary cross-entropy loss function are utilized to compile the model, setting an efficient training dynamic. Following this initial training phase, active learning is initiated. Here, the trained model predicts on the unlabeled pool of data to identify the least certain predictions or the model's most uncertain sample regions. These identified samples are then added to the training set, allowing the model to focus on learning from the most informative or challenging samples at that time [64].

This active learning cycle is repeated several times, each cycle aiming to bolster the model's performance. During each iteration, the model may update its weights based on new data. If these updated weights yield higher validation accuracies, they are retained. Ultimately, the model's final performance is assessed on the test set. The high accuracy and detailed classification metrics achieved demonstrate the model's capability to effectively handle complex classification tasks by integrating insights from both past and prospective data.

However, it is crucial to acknowledge the limitations inherent in the BiLSTM and active learning approach, particularly in their application to cybersecurity. The model may not handle specific types of network intrusions or scenarios outside its training data distribution effectively. This could lead to less reliable performance in detecting novel or sophisticated cyber-attacks that deviate from the patterns observed during training. Without a comprehensive discussion on the robustness and generalizability of the model, potential users and researchers might not fully understand the impacts these limitations could have on the deployment and operational effectiveness in diverse cybersecurity environments. Recognizing these limitations is essential for setting realistic expectations about the model's capabilities in real-world applications.

IV. EVALUATION METRICS

To effectively evaluate the model's usefulness in image classification, we will employ several evaluation metrics that are essential for a full understanding of the model's performance. However, the following is a brief of the contribution of every metric to evaluating the model

A. Accuracy

It is one of the central evaluation metrics used to assess the general quality of a model's prediction [56]. It is defined as the ratio of the number of correct classifications of samples including both true positives and true negatives to the total amount of the dataset's observations.

$$ACC = \frac{TN + TP}{TP + TN + FP + FN} \tag{1}$$

B. Precision

This measure is crucial in terms of the model's ability to predict a class accurately [57]. It is measured as the number of accurate positive predictions that are true positives divided by the sum of accurate positive predictions and inaccurate positive predictions.

$$PRE = \frac{TP}{FP + TP} \tag{2}$$

C. Recall

This metric evaluates the ability of the model to accurately capture all cases of a class [58]. The calculation is done by taking the number of True Positives and dividing them by the total of True Positive and the False Negative.

D. F1-Score

The F1-score is a balanced metric which integrates precision and recall by means of their harmonic mean [59]. Thus, the measure integrates both, providing a comprehensive assessment of how the model fares in recognizing relevant instances.

$$F1 - S = 2 \times \frac{PRE \ \times REC}{PRE + REC} \tag{3}$$

In the context of cybersecurity, the implications of these metrics are profound. A high precision rate minimizes the risk of false positives, which are costly and can lead to unnecessary responses. Conversely, a high recall rate ensures that the system is effective at detecting true threats, minimizing the risk of missed detections that could result in undetected intrusions. The F1-Score serves as a critical measure for balancing these aspects, particularly when dealing with imbalanced datasets that could bias the model towards the majority class. Understanding the trade-offs between these metrics and the potential biases introduced by dataset characteristics is essential for validating the model's reliability in detecting diverse and evolving intrusion patterns.

V. Experimental Results

A. BILSTM

The performance of the BiLSTM model used to identify Fake and Real Signatures is highly acceptable as demonstrated in the confusion matrix and classification report presented in Fig. 3 and Fig. 4. The model has accurately predicted a considerably high number of instances. It has predicted 59,379 true positives for class 0 and 31,874 and true negatives for class 1.

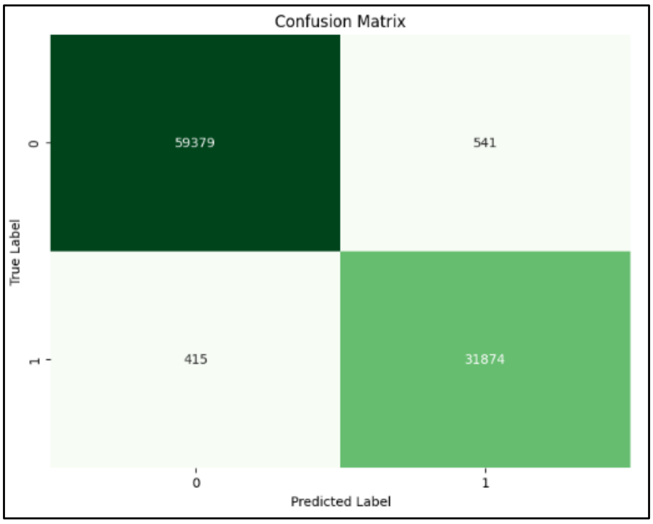
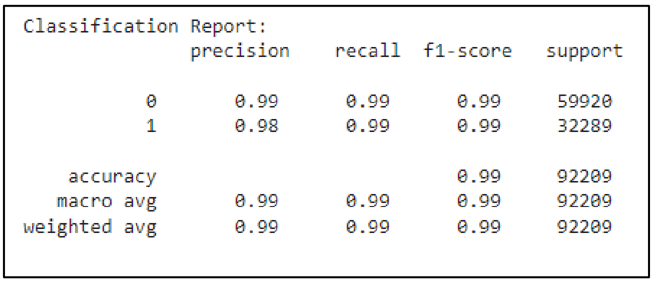


Fig. 3. Confusion matrix of BILSTM



```
Classification Report:
              precision    recall  f1-score   support

           0       0.99      0.99      0.99     59920
           1       0.98      0.99      0.99     32289

    accuracy                           0.99     92209
   macro avg       0.99      0.99      0.99     92209
weighted avg       0.99      0.99      0.99     92209
```

Fig. 4. Classification Report of BILSTM

These values are very high, which means that the model was very sensitive and specific in accurately identifying both classes of the target variable. The misclassified instances are low that is, only 541 false positives and 415 false negatives.

This shows that the model was very knowledgeable of the two classes. The other metric values, which include precision, recall, and F1 score show that the model was extremely successful. All the metric values, which are precision values of 0.99 for class 0 and 0.98 for class 1, recall values, which are 0.99 for both classes, and F1 scores that are 0.99 for both classes, are extremely high.

The accuracy of the model is 0.99, which is very high as well. This means that the model performs as a classifying model, and the BiLSTM model has proved effective in accurately classifying sequential data through exploiting the temporal dynamics present in the dataset.

B. BILSTM with Active Learning

These outstanding classification results are achieved by BiLSTM network combined with active learning, es presents in Fig. 5. The confusion matrix of the predictions of the trained neural network reveals high numbers of true positives and true negatives: there are 38,376 and 71,616, respectively. These numbers demonstrate that the model is able to recognize both classes accurately with a low number of false positives and false negatives: 499 and 160, respectively.

The classification report supports these findings shown in Fig. 6, as it demonstrates that the model has outstanding precision, recall, and F1-scores for both classes: 1.00 precision for class 0 and 0.99 for class 1, and recall of 0.99 and perfect 1.00 for classes 0 and 1, respectively. Furthermore, both classes have the F1-score of 0.99, indicating the model’s ability to perform balanced classification. The accuracy of the model is also high: it is 0.99.

In summary, the above results prove the efficiency of active learning combined with BiLSTM, allowing the model to learn iteratively from the most informative and ambiguous data points and, consequently, to improve predictions in sequential data tasks.

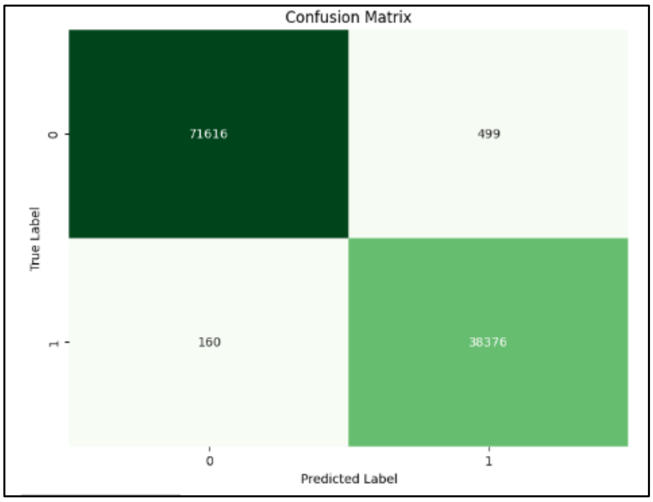
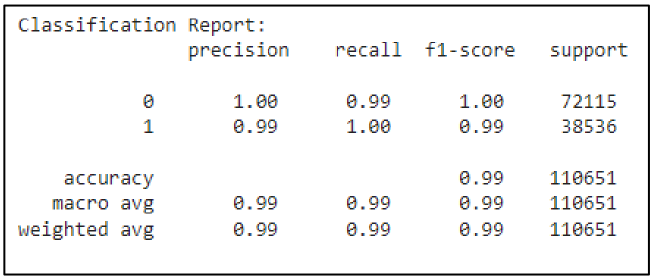


Fig. 5. Confusion matrix of BILSTM+Active



```
Classification Report:
              precision    recall  f1-score   support

           0       1.00      0.99      1.00     72115
           1       0.99      1.00      0.99     38536

    accuracy                           0.99    110651
   macro avg       0.99      0.99      0.99    110651
weighted avg       0.99      0.99      0.99    110651
```

Fig. 6. Classification Report of BILSTM +Active

VI. Comparative Analysis

The comparative analysis outlined in Table II vividly demonstrates the efficacy of both the BiLSTM model and its enhanced version with active learning. The BiLSTM model alone shows excellent performance metrics, with a precision of 0.99, recall of 0.99, F1-score of 0.99, and an overall accuracy of 0.99. These results underscore its robust capability in sequence classification tasks. However, the incorporation of active learning significantly enhances these outcomes, particularly for class 0, where the precision is pushed to a perfect score of 1.00. Despite this increase in precision, the model maintains high recall and F1-score at 0.99 and 1.00, respectively, with the overall accuracy remaining stable at 0.99. This indicates that the addition of active learning to BiLSTM does not compromise its ability to correctly identify true positives and negatives across classes, but rather refines its precision without affecting the overall performance adversely. Such enhancements highlight the strategic benefit of integrating active learning, particularly in scenarios where reducing false positives is critical without losing sensitivity to true positive detections.

The BiLSTM model alone can boast its excellent level of classification of sequenced data, with high precision, recall, and F1-scores bordering on their theoretical maximum of 1.00 for both classes.

Hence, the model demonstrates its strength and capacity in identifying patients for whom the treatment is beneficial or non-beneficial. Introduction of active learning with BiLSTM improves all these levels to perfect or near-perfect conditions. In particular, it enhances the precision for class 0 to the ultimate 1.00.

Thus, the standalone BiLSTM and active BiLSTM approaches are highly efficient for the classification of sequenced data. A more detailed comparison between them shows that they both are extremely effective in identifying the classification patterns.

Second, the active learning [66] approach enhances the level of precision for class 0 to a perfect condition without compromising the high level of recall and F1-score for both classes. Therefore, it allows the model to focus on the most informative data points by sacrificing only the margin of the recall.

This strategic iteration results in a model that not only retains its inherent temporal pattern recognition strength offered by BiLSTM but also gains an incremental improvement in classification acuity, a testament to the synergy between active learning and BiLSTM in complex sequence modeling tasks.

TABLE II. Comparative Analysis Results

Model	Precision	Recall	F1-Score	Accuracy
BILSTM	0.99	0.99	0.99	0.99
BILSTM+ACTIVE	1.00	0.99	1.00	0.99

Based on Table II, the overall accuracy of 0.99 for both models underscore the success of both approaches in handling the intricacies of sequence prediction with great effectiveness.

VII. Discussion

Achieving near-perfect precision for class 0 with the BiLSTM + Active Learning model significantly enhances its practical applications, particularly in domains like signature identification where false positives can have severe consequences. Precision, recall, and F1-score are crucial metrics in such contexts because they provide a comprehensive view of the model's ability to correctly identify true positives (precision) while minimizing the overlook of actual positives (recall). The high F1-score indicates a balanced relationship between precision and recall, essential for applications where both false positives and false negatives carry significant implications.

The comparative table below summarizing the performance of different models from the related work and comparing them with the BiLSTM and BiLSTM with active learning models based on the available results in Table III.

TABLE III. Performance of Related Models to BiLSTM

Paper	Accuracy	Specific Achievements
[21]	90%	Outperformed Least Confidence by 5%
[22]	98%	High AUC scores for detecting various attacks
[23]	90.01%	High precision, recall, and F1-score
[24]	99%	High accuracy rates across models
[25]	99%	High accuracy on multiple datasets
[26]	-	Superior to standalone models
[27]	98%	High success in bypassing IDS
[28]	-	Effective feature selection and classification
Our work	99%	High overall performance
Our work	99%	Perfect precision and high overall performance

The advancements in machine learning and particularly in deep learning models have played a pivotal role in the field of intrusion detection and cybersecurity, as reflected in the array of studies within the related work. The models employed across various papers range from Naive Bayes with active learning strategies to sophisticated hybrids of CNNs and LSTMs, each contributing uniquely to the domain.

Paper [21] reports on the application of a Naive Bayes classifier coupled with active learning, achieving an AUC score of 90%. This approach underlines the efficiency of machine learning complemented by active learning even with fairly simple algorithms. In contrast, the paper [22] uses a sophisticated CNN architecture that provides AUC scores above 0.98, which emphasizes the capability of deep learning for feature extraction and pattern recognition to detect attacks.

The CNN and BiLSTM models presented in paper [23] is a powerful tool that harnesses spatial and temporal features, reaching a 90.01% detection accuracy. Different types of neural network architectures were addressed in paper [21], which show excellent accuracy based on the FFNN model:

99.93%. This implies that the detection architecture should be chosen, aligned with diverse data features.

Finally, as presented in Paper [24] possibly by including attention mechanisms, all models exhibit very high accuracy, that is, up to 99.08%, due to attention mechanisms, which allow focusing on different parts of the data sequence, as required by the complex patterns posed by attacks that can only be discerned by the model by taking under consideration subtleties in data hate are not necessarily prevalent throught the whole session record.

Our trained BiLSTM model only that is on par with these models in terms of accuracy combines its potential acuracy in terms of its accuracy score with active learning to achieve state-of-the-art precision at 1.00, which indicates that active learning algoeritms can be used to further finetune models accuracy where some prediction direction is crucial achieve precision of this kind, as any false positives in differentiation benign and malicious acts around the session data pools are costly.

Furthermore, the recent trend in applying active-learning dynamics with GANs and VAEs discussed in paper [27], and the implementation of metaheuristic algorithms which is used for feature selection in paper [28] is just an additional testimony to the development of sudden intelligence and intelligence insertion into a model. Not only must these models be accurate, but they will have to be elegant, adaptive, and enduring due to the dynamics of the environment they scrutinized. Not only does our BiLSTM model, particularly with active learning, share the high-precision accuracy notes of the past work, but it also suggests an opportunity for precision-based performance change.

The use of active learning, more particularly, suggests a calculated move towards models that are destined to develop on their own, more restructured and evolve only by permissible from the vaguest and most informative data points. Hence, the solution is solid.

The strengths of our models lie in their ability to leverage temporal dynamics (BiLSTM) and enhance precision through iterative refinements (active learning). However, potential biases in the dataset or the experimental setup could limit the generalizability and performance across different types of network intrusions or novel cyber-attack scenarios. Future research could explore enhancing the active learning strategy, adapting the models to different datasets, or incorporating additional machine learning techniques to address these limitations. This could include exploring hybrid models or advanced neural network architectures that could further improve the robustness and adaptability of the system.

Our approach uniquely contributes by achieving exceptional precision without compromising overall performance, which is particularly valuable in applications where distinguishing between benign and malicious actions with high accuracy is crucial. Future directions will aim to extend these capabilities, ensuring that the models not only maintain their high performance but also adapt to the evolving landscapes of cybersecurity threats.

VIII. Conclusion

This study integrates active learning with deep learning within the IoT security domain, successfully developing an Intrusion Detection System (IDS) tailored for IoT environments. The combination of a Bidirectional Long Short-Term Memory (BiLSTM) model with active learning has proven to be a robust framework, enhancing threat detection capabilities significantly. Our findings demonstrate that this combination not only achieves high performance metrics—precision of 1.00 and recall, F1-score, and accuracy of 0.99 for the BiLSTM with active learning model, but also underscores the potential of these methodologies in resource-constrained scenarios.

The precision achieved by the BiLSTM with active learning highlights its efficacy in precisely identifying threats without generating false positives, a crucial attribute in cybersecurity where erroneous alerts can be costly. Comparatively, the BiLSTM model alone also shows commendable results but lacks the enhanced precision of its active learning-enhanced counterpart. However, while these metrics are promising, they must be contextualized within real-world applications. High performance in controlled test conditions does not always directly translate to effectiveness in operational environments, particularly in cases of class imbalance or evolving attack strategies that were not represented in the training data.

Although our models perform well across standard metrics, their robustness against novel or sophisticated cyber threats remains partially speculative without further testing on diverse datasets or real-world deployment scenarios. Furthermore, a detailed error analysis is essential to understand the conditions under which the models might fail or misclassify, providing insights for continuous improvement.

Looking ahead, enhancing the active learning component to better adapt to rapidly changing threat landscapes could significantly improve the model's applicability. Exploring hybrid approaches that incorporate other machine learning paradigms or advanced neural architectures might also yield improvements in scalability and adaptability. Additionally, case studies or deployment in real-world IoT environments would offer invaluable insights into the practical challenges and performance metrics in operational settings.

References

[1] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, and A. V. Vasilakos, "The role of big data analytics in Internet of Things," *Computer Networks*, vol. 129, pp. 459-471, 2017.

[2] H. Aldowah, S. U. Rehman, and I. Umar, "Security in Internet of Things: Issues, Challenges and Solutions," in *Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018)*, pp. 396-405, 2019.

[3] R. Bhatt, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: a survey," *SN Appl. Sci.*, vol. 3, no. 1, pp. 1–14, 2021, doi: 10.1007/s42452-021-04156-9.

[4] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions," *Wireless Pers. Commun.*, vol. 119, no. 3, pp. 2603–2637, 2021, doi: 10.1007/s11277-021-08348-9.

[5] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," *arXiv preprint arXiv:2210.13547*, 2022.

[6] Y. Yue, S. Li, P. Legg, and F. Li, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey," *Secur. Commun. Netw.*, vol. 2021, no. 1, p. 8873195, 2021, doi: 10.1155/2021/8873195.

[7] K. Yang, J. Ren, Y. Zhu, and W. Zhang, "Active Learning for Wireless IoT Intrusion Detection," *arXiv preprint arXiv:1808.01412*, 2018.

[8] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *arXiv preprint arXiv:1904.05735*, 2019.

[9] M. Zakariah and A. S. Almazyad, "Anomaly Detection for IOT Systems Using Active Learning," *Appl. Sci.*, vol. 13, no. 21, pp. 12029, 2023, doi: 10.3390/app132112029.

[10] S. Yin, W. Zhang, Y. Feng, Y. Xiang, and Y. Liu, "Automatic IoT device identification: a deep learning based approach using graphic traffic characteristics," *Telecommun. Syst.*, vol. 83, no. 2, pp. 101–114, 2023, doi: 10.1007/s11235-023-01009-1.

[11] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3211–3243, 2021, doi: 10.1007/s11831-020-09496-0.

[12] R. Alghamdi and M. Bellaiche, "An ensemble deep learning based IDS for IoT using Lambda architecture," *Cybersecurity*, vol. 6, no. 1, pp. 1–17, 2023, doi: 10.1186/s42400-022-00133-w.

[13] S. Revathi and A. Malathi, "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 12, pp. 1848-1853, 2013.

[14] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems*, vol. 100, pp. 779-796, 2019.

[15] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "Toward an intrusion detection model for IoT-based smart environments," *Multimed. Tools Appl.*, pp. 1–22, 2023, doi: 10.1007/s11042-023-16436-0.

[16] S. Sapre, P. Ahmadi, and K. Islam, "A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets Through Various Machine Learning Algorithms," *arXiv preprint arXiv:1912.13204*, 2019.

[17] D. D. Kulkarni and R. K. Jaiswal, "An Intrusion Detection System Using Extended Kalman Filter and Neural Networks for IoT Networks," *J. Netw. Syst. Manage.*, vol. 31, no. 3, pp. 1–40, 2023, doi: 10.1007/s10922-023-09748-x.

[18] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, pp. 1-27, 2021.

[19] A. Rosay, E. Cheval, M. Ghanmi, F. Carlier, and P. Leroux, "Study of Network IDS in IoT devices," *SN Comput. Sci.*, vol. 4, no. 4, pp. 1–25, 2023, doi: 10.1007/s42979-023-01849-3.

[20] L. Arnaboldi and C. Morisset, "A Review of Intrusion Detection Systems and Their Evaluation in the IoT," *arXiv preprint arXiv:2105.08096*, 2021.

[21] Q.-V. Dang, "Active Learning for Intrusion Detection Systems," *2020 RIVF International Conference on Computing and Communication Technologies*, pp. 1-3, 2020, doi: 10.1109/RIVF48685.2020.9140751.

[22] B. Susilo and R. F. Sari, "Intrusion Detection in IoT Networks Using Deep Learning Algorithm," *Information*, vol. 11, no. 5, p. 279, 2020, doi: 10.3390/info11050279.

[23] X. Yang, G. Peng, D. Zhang, and Y. Lv, "An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph," *Secur. Commun. Netw.*, vol. 2022, no. 1, p. 4748528, 2022, doi: 10.1155/2022/4748528.

[24] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered Intrusion Detection System," *Internet of Things*, vol. 24, p. 100936, 2023, doi: 10.1016/j.iot.2023.100936.

[25] J. Zhang, X. Zhang, Z. Liu, F. Fu, Y. Jiao, and F. Xu, "A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism," *Electronics*, vol. 12, no. 19, p. 4170, 2023, doi: 10.3390/electronics12194170.

[26] S. Sadhwani, M. A. H. Khan, R. Muthalagu, and P. M. Pawar, "BiLSTM-CNN Hybrid Intrusion Detection System for IoT Application," 2024, Jan. 03, doi: 10.21203/rs.3.rs-3820775/v1.

[27] D. Shu, N. O. Leslie, C. A. Kamhoua, and C. S. Tucker, "Generative adversarial attacks against intrusion detection systems using active learning," *WiseML '20: Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, Association for Computing Machinery*, pp. 1-6, 2020, doi: 10.1145/3395352.3402618.

[28] A. Dahou, M. Abd Elaziz, S. A. Chelloug, M. A. Awadallah, M. A. Al-Betar, M. A. A. Al-qaness, and A. Forestiero, "Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm," *Comput. Intell. Neurosci.*, vol. 2022, no. 1, p. 6473507, 2022, doi: 10.1155/2022/6473507.

[29] N. Moustafa, M. Keshk, E. Debie, and H. Janicke, "Federated TON_IoT Windows Datasets for Evaluating AI-based Security Applications," *arXiv preprint arXiv:2010.08522*, 2020.

[30] Y. Yan, F. Liu, X. Zhuang, and J. Ju, "An R-Transformer_BiLSTM Model Based on Attention for Multi-label Text Classification," *Neural Process. Lett.*, vol. 55, no. 2, pp. 1293–1316, 2023, doi: 10.1007/s11063-022-10938-y.

[31] A. Mohapatra, N. Thota, and P. Prakasam, "Fake news detection and classification using hybrid BiLSTM and self-attention model," *Multimed. Tools Appl.*, vol. 81, no. 13, pp. 18503–18519, 2022, doi: 10.1007/s11042-022-12764-9.

[32] M. Liu and L. Yang, "IoT Network Traffic Analysis with Deep Learning," *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pp. 184-189, 2024.

[33] Y. Xiong, S. Dong, R. Liu, F. Shi, and X. Jing, "IoT network traffic classification: a deep learning method with Fourier transform-assisted hyperparameter optimization," *Front. Phys.*, vol. 11, p. 1273862, 2023, doi: 10.3389/fphy.2023.1273862.

[34] M. Santos. *A Data Scientist's Essential Guide to EDA | Towards Data Science*. Medium, 2024.

[35] Y. Dodge, "Exploratory Data Analysis," *The Concise Encyclopedia of Statistics*, 2008, doi: 10.1007/978-0-387-32833-1_136.

[36] S. Galli, "Feature scaling in machine learning: Standardization, MinMaxScaling and more...," *Train in Data's Blog*, 2023.

[37] Dr. D. Guggenheim. *The Mystery of Feature Scaling is Finally Solved*. Towards Data Science, Medium, 2022.

[38] J. Kim and N. Moon, "BiLSTM model based on multivariate time series data in multiple field for forecasting trading area," *J. Ambient Intell. Hum. Comput.*, pp. 1–10, 2019, doi: 10.1007/s12652-019-01398-9.

[39] R. Tchoua, A. Ajith, Z. Hong, L. Ward, K. Chard, D. Audus, and I. Foster, "Active learning yields better training data for scientific named entity recognition," in *2019 15th International Conference on eScience (eScience)*, pp. 126-135, 2019.

[40] B. Sayin, E. Krivosheev, J. Yang, A. Passerini, and F. Casati, "A review and experimental analysis of active learning over crowdsourced data," *Artif. Intell. Rev.*, vol. 54, no. 7, pp. 5283–5305, 2021, doi: 10.1007/s10462-021-10021-3.

[41] V. Digalakis Jr, Y. Ma, P. Paschalidis, and D. Bertsimas, "Towards Stable Machine Learning Model Retraining via Slowly Varying Sequences," *arXiv preprint arXiv:2403.19871*, 2024.

[42] I. Prapas, B. Derakhshan, A. R. Mahdiraji, and V. Markl, "Continuous Training and Deployment of Deep Learning Models," *Datenbank. Spektrum.*, vol. 21, no. 3, pp. 203–212, 2021, doi: 10.1007/s13222-021-00386-8.

[43] S. Raschka, "Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning," *arXiv preprint arXiv:1811.12808*, 2018.

[44] A. Panesar, "Evaluating Machine Learning Models," in *Machine Learning and AI for Healthcare*, 2021, doi: 10.1007/978-1-4842-6537-6_7.

[45] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, 2020.

[46] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustainable Cities and Society*, vol. 72, p. 102994, 2021.

[47] N. A. Hikal and M. M. Elgayar, "Enhancing IoT botnets attack detection using machine learning-IDS and ensemble data preprocessing technique," in *Internet of Things—Applications and Future: Proceedings of ITAF 2019*, pp. 89-102, 2020.

[48] A. Tawakuli, D. Kaiser, and T. Engel, "Transforming IoT data preprocessing: A holistic, normalized and distributed approach," in *Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems*, pp. 1083-1088, Nov. 2022.

[49] B. Deepa and K. Ramesh, "Epileptic seizure detection using deep learning through min max scaler normalization," *Int J Health Sci (Qassim)*, pp. 10981-10996, 2022.

[50] V. Păpăluță. *What's the best way to handle NaN values?*. Towards Data Science, Medium, 2021.

[51] A. Rácz, D. Bajusz, and K. Héberger, "Effect of dataset size and train/test split ratios in QSAR/QSPR multiclass classification," *Molecules*, vol. 26, no. 4, p. 1111, 2021.

[52] H. Hino, "Active Learning: Problem Settings and Recent Developments," *arXiv preprint arXiv:2012.04225*, 2020.

[53] R. Ghaeini, S. A. Hasan, V. Datla, J. Liu, K. Lee, A. Qadir, and O. Farri, "DR-BiLSTM: Dependent Reading Bidirectional LSTM for Natural Language Inference," *arXiv preprint arXiv:1802.05577*, 2018.

[54] S. M. Nacer, B. Nadia, R. Abdelghani, and B. Mohamed, "A novel method for bearing fault diagnosis based on BiLSTM neural networks," *Int. J. Adv. Manuf. Technol.*, vol. 125, no. 3, pp. 1477–1492, 2023, doi: 10.1007/s00170-022-10792-1.

[55] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[56] G. Naidu, T. Zuva, and E. M. Sibanda, "A Review of Evaluation Metrics in Machine Learning Algorithms," *Computer Science On-line Conference*, pp. 15-25, 2023.

[57] J. Brownlee, "How to Calculate Precision, Recall, and F-Measure for Imbalanced Classification," *Machine Learning Mastery*, vol. 1, 2020.

[58] "Recall, Precision, F1 Score - Explication Simple Métrique en ML," Oct. 19, 2023.

[59] GeeksforGeeks. *F1 Score in Machine Learning*. GeeksforGeeks, 2023.

[60] M. Grandini, E. Bagli, and G. Visani, "Metrics for Multi-Class Classification: an Overview," *arXiv preprint arXiv:2008.05756*, 2020.

[61] L. Ferrer, "Analysis and Comparison of Classification Metrics," *arXiv preprint arXiv:2209.05355*, 2022.

[62] K. Abdelli, H. Griesser, C. Tropschug, and S. Pachnicke, "A BiLSTM-CNN based Multitask Learning Approach for Fiber Fault Diagnosis," *arXiv preprint arXiv:2202.08034*, 2022.

[63] S. K. Challa, A. Kumar, and V. B. Semwal, "A multibranch CNN-BiLSTM model for human activity recognition using wearable sensor data," *Vis. Comput.*, vol. 38, no. 12, pp. 4095–4109, 2022, doi: 10.1007/s00371-021-02283-3.

[64] D. Yu, L. Wang, X. Chen, and J. Chen, "Using BiLSTM with attention mechanism to automatically detect self-admitted technical debt," *Frontiers of Computer Science*, vol. 15, no. 4, p. 154208, 2021.

[65] R. L. Abduljabbar, H. Dia, and P.-W. Tsai, "Development and evaluation of bidirectional LSTM freeway traffic forecasting models using simulation data," *Sci. Rep.*, vol. 11, p. 23899, 2021, doi: 10.1038/s41598-021-03282-z.

[66] R. Yacouby and D. Axman, "Probabilistic extension of precision, recall, and F1 score for more thorough evaluation of classification models," *Proceedings of the first workshop on evaluation and comparison of NLP* systems, pp. 79-91, 2020.

[67] H. Peng, C. Wu, and Y. Xiao, "CBF-IDS: Addressing Class Imbalance Using CNN-BiLSTM with Focal Loss in Network Intrusion Detection System," *Applied Sciences*, vol. 13, no. 21, p. 11629, 2023.

[68] T. S. Pooja and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 448-454, 2021.

[69] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," *IEEE Access*, vol. 8, pp. 185489-185502, 2020.

[70] B. Ko, H. G. Kim, K. J. Oh, and H. J. Choi, "Controlled dropout: A different approach to using dropout on deep neural network," in *2017 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 358-362, Feb. 2017.

[71] H. Pratiwi, A. P. Windarto, S. Susliansyah, R. R. Aria, S. Susilowati, L. K. Rahayu, and I. R. Rahadjeng, "Sigmoid activation function in selecting the best model of artificial neural networks," in *Journal of Physics: Conference Series*, vol. 1471, no. 1, p. 012010, 2020.