*applied sciences*

MDPI

*Article*

# Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data

**Hussein Ridha Sayegh *, Wang Dong and Ali Mansour Al-madani**

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China; wangd@hnu.edu.cn (W.D.); ali.m.almadanni1992@gmail.com (A.M.A.-m.)

* Correspondence: husseinsayegh81@hnu.edu.cn

**Abstract:** This study introduces a sophisticated intrusion detection system (IDS) that has been specifically developed for internet of things (IoT) networks. By utilizing the capabilities of long short-term memory (LSTM), a deep learning model renowned for its proficiency in modeling sequential data, our intrusion detection system (IDS) effectively discerns between regular network traffic and potential malicious attacks. In order to tackle the issue of imbalanced data, which is a prevalent concern in the development of intrusion detection systems (IDSs), we have integrated the synthetic minority over-sampling technique (SMOTE) into our approach. This incorporation allows our model to accurately identify infrequent incursion patterns. The rebalancing of the dataset is accomplished by SMOTE through the generation of synthetic samples belonging to the minority class. Various strategies, such as the utilization of generative adversarial networks (GANs), have been put forth in order to tackle the issue of data imbalance. However, SMOTE (synthetic minority over-sampling technique) presents some distinct advantages when applied to intrusion detection. The SMOTE is characterized by its simplicity and proven efficacy across diverse areas, including in intrusion detection. The implementation of this approach is straightforward and does not necessitate intricate adversarial training techniques such as generative adversarial networks (GANs). The interpretability of SMOTE lies in its ability to generate synthetic samples that are aligned with the properties of the original data, rendering it well suited for security applications that prioritize transparency. The utilization of SMOTE has been widely embraced in the field of intrusion detection research, demonstrating its effectiveness in augmenting the detection capacities of intrusion detection systems (IDSs) in internet of things (IoT) networks and reducing the consequences of class imbalance. This study conducted a thorough assessment of three commonly utilized public datasets, namely, CICIDS2017, NSL-KDD, and UNSW-NB15. The findings indicate that our LSTM-based intrusion detection system (IDS), in conjunction with the implementation of SMOTE to address data imbalance, outperforms existing methodologies in accurately detecting network intrusions. The findings of this study provide significant contributions to the domain of internet of things (IoT) security, presenting a proactive and adaptable approach to safeguarding against advanced cyberattacks. Through the utilization of LSTM-based deep learning techniques and the mitigation of data imbalance using SMOTE, our AI-driven intrusion detection system (IDS) enhances the security of internet of things (IoT) networks, hence facilitating the wider implementation of IoT technologies across many industries.

**Keywords:** cybersecurity; intrusion detection system (IDS); long short-term memory (LSTM); data imbalance

check for updates

**Citation:** Sayegh, H.R.; Dong, W.; Al-madani, A.M. Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data. *Appl. Sci.* **2024**, *14*, 479. https://doi.org/10.3390/app14020479

Academic Editor: Gianluca Lax

Received: 13 September 2023
Revised: 25 November 2023
Accepted: 29 December 2023
Published: 5 January 2024

## 1. Introduction

The rapid proliferation of communication, cloud computing, and the internet of things (IoT) has ushered in an era of unprecedented connectivity and data-driven innovations [1]. IoT networks have become ubiquitous, permeating various sectors such as healthcare, transportation, manufacturing, and smart cities. While IoT offers immense benefits in terms of efficiency and automation, it also brings forth intricate cybersecurity challenges [2]. The interconnectivity and heterogeneity of IoT devices exposes these networks to sophisticated cyber threats, demanding robust defined mechanisms to safeguard sensitive data and preserve operational continuity [3].

Among the fundamental security measures, intrusion detection systems (IDSs) play a crucial role in detecting and thwarting potential cyberattacks. An IDS continuously monitors network traffic, scrutinizing data streams for anomalous patterns and malicious activities. However, ensuring the efficacy of an IDS in the dynamic and evolving landscape of IoT requires innovative and adaptive approaches that can accurately identify both known and previously unseen cyber threats [4].

This research paper presents a cutting-edge AI-driven intrusion detection system, tailor-made for the unique challenges posed by IoT environments. The primary objective of this study is to fortify the cybersecurity posture of IoT networks by proactively detecting and mitigating cyber threats, bolstering data integrity, and safeguarding critical infrastructures.

To achieve this objective, we leverage the power of long short-term memory (LSTM), a specialized variant of recurrent neural networks renowned for its exceptional ability to model sequential data. In the context of IoT network traffic, which often exhibits temporal dependencies and intricate dynamics, LSTM's capacity to retain long-term contextual information proves invaluable. By harnessing LSTM-based deep learning, our IDS demonstrates superior performance in recognizing subtle and time-sensitive anomalies, enabling the early detection of advanced and persistent cyberattacks [5–7].

However, the imbalance in class distribution within the dataset is a persistent challenge in IDS development. In the context of IoT networks, normal network traffic vastly outnumbers actual attacks, leading to imbalanced datasets that can undermine the IDS's accuracy. To address this issue, we employ the synthetic minority over-sampling technique (SMOTE). SMOTE intelligently generates synthetic instances of the minority class (attacks), effectively balancing the dataset and empowering the IDS to identify rare intrusion patterns with precision [8,9].

Furthermore, the selection of informative features significantly impacts the IDS's overall performance. To optimize feature selection, we integrate the random forest classifier with recursive feature elimination (RFE). RFE iteratively selects and eliminates features, enhancing the IDS's efficiency, reducing computational complexity, and improving detection accuracy. This meticulous feature selection process ensures that the IDS focuses on the most relevant and discriminative attributes, enhancing its ability to discern meaningful patterns amidst noise and irrelevant data [10–12].

Our proposed AI-driven IDS undergoes comprehensive evaluation using three widely adopted public datasets: the Intrusion Detection Evaluation dataset (CIC-IDS2017) [13], NSL-KDD [14], and the UNSW-NB15 dataset [15]. These datasets encompass diverse and realistic attack scenarios, making them suitable benchmarks to assess the IDS's robustness and effectiveness. Through rigorous experimentation, we demonstrate that our AI-enhanced IDS outperforms existing intrusion detection methods, validating its efficacy in safeguarding IoT networks against sophisticated cyber threats.

### *Existing IoT Security Solutions and Their Limitations*

As highlighted by one of the reviewers, there is a pressing need to examine the landscape of existing solutions for mitigating cyber threats in the IoT and evaluate their shortcomings. Therefore, before delving into the details of our proposed approach, we dedicate this section to providing a comprehensive overview of the current state of IoT security solutions and the challenges that they face. This discussion sets the stage for our research by emphasizing the critical need for advancements in IoT security and the unique contributions of our work.

We explore common approaches adopted by the cybersecurity community to address IoT threats, including intrusion detection systems, encryption methods, access control mechanisms, and more. We critically analyze these solutions, shedding light on their strengths and weaknesses, and identifying areas where they may fall short in protecting IoT devices and networks.

Our research is driven by the recognition that while existing solutions have made significant strides in enhancing IoT security, they are not without limitations. Vulnerabilities, scalability issues, and adaptability to evolving threats are among the challenges faced by these solutions. These identified shortcomings serve as a backdrop against which we propose our innovative IDS framework, which not only addresses these limitations but also brings novel capabilities to IoT security.

In the subsequent sections, we present the details of our LSTM-based IDS model, the application of feature selection, and the integration of SMOTE to tackle data imbalance. We highlight how our approach overcomes the limitations discussed in this section, ultimately contributing to the enhancement of IoT security.

The outcomes of this research are poised to offer substantial contributions to the field of IoT security. Our work leverages the following key elements:

1. LSTM-Based Deep Learning: By incorporating long short-term memory (LSTM) networks into our intrusion detection system (IDS), we introduce a novel approach to IoT security. LSTM's ability to model sequential data enables our system to capture and recognize evolving cyber threats, thus enhancing the adaptability and responsiveness of our IDS.
2. SMOTE for Data Imbalance: Addressing the inherent data imbalance in IoT security datasets is a critical challenge. Through the synthetic minority over-sampling technique (SMOTE), our research takes a proactive stance, enabling our IDS to learn from underrepresented threat instances. This approach strengthens the overall robustness of our system.
3. Random Forest Classifier–RFE for Feature Selection: Feature selection plays a pivotal role in optimizing the performance of an IDS. Our use of the random forest with recursive feature elimination (RFE) ensures that our system operates with a streamlined and relevant set of features, reducing computational overhead while preserving detection accuracy.

Collectively, our AI-driven IDS offers a proactive, adaptive, and efficient defense mechanism against cyber threats in the IoT landscape. This research lays the foundation for reinforcing the resilience and security of modern IoT networks. By fostering trust and confidence, it encourages the widespread adoption of IoT technologies across diverse industries, addressing critical security concerns in the ever-expanding IoT ecosystem.

## 2. Literature Review

The increasing prevalence of internet of things (IoT) networks in various domains has facilitated new opportunities for innovative services and applications. However, this rapid growth in IoT adoption has also exposed critical cybersecurity challenges, necessitating effective intrusion detection mechanisms. In this section, we present a comprehensive review of existing literature on AI-based intrusion detection systems (IDSs) tailored for IoT environments. Specifically, we focus on the utilization of long short-term memory (LSTM) models, the synthetic minority over-sampling technique (SMOTE) for addressing data imbalance, and random forest-based feature selection.

We sincerely appreciate the reviewer's valuable comment regarding the significance and advancement of our proposed methodology compared to the published literature. We recognize the importance of effectively conveying the unique contributions of our research. To address this concern, we would like to highlight the following points:

Significance of the Proposed Methodology:

Our methodology holds significant importance in the realm of IoT intrusion detection for several key reasons:

Imbalanced Data Mitigation: We acknowledge the challenges posed by imbalanced datasets in intrusion detection, a problem widely recognized in the literature. Our incorporation of the synthetic minority over-sampling technique (SMOTE) addresses this issue effectively by rebalancing the dataset, resulting in enhanced detection capabilities.

Elimination of Extensive Feature Engineering: Traditional intrusion detection approaches often require extensive manual feature engineering. Our method streamlines this process by employing the random forest classifier with recursive feature elimination (RFE), ensuring that only the most relevant attributes contribute to intrusion detection. This not only improves accuracy but also reduces the computational overhead associated with feature selection.

Advancements Over Published Literature:

Our proposed methodology advances the state of the art in IoT intrusion detection through the following:

Adaptive Learning: Our approach incorporates an attention mechanism and the bidirectional long short-term memory (Bi-LSTM) network, allowing the model to adaptively learn sequential patterns in data traffic. This stands in contrast to some existing methods that rely on fixed or handcrafted features.

End-to-End Model: DLNID is an end-to-end model, eliminating the need for manual feature extraction. This innovation streamlines the intrusion detection process and enhances model efficiency.

Quantitative Results: Our research presents empirical evidence through a comprehensive evaluation using widely adopted public datasets, including CICIDS2017, NSL-KDD, and UNSW-NB15. The superior accuracy achieved by our LSTM-based IDS, coupled with SMOTE and RFE, demonstrates its advancements over existing methods.

Real-World Relevance:

Our methodology holds practical significance by addressing the evolving landscape of cybersecurity threats in IoT networks. It offers a proactive and adaptive defense mechanism that is particularly relevant in today's context, where network attacks are increasing in number and sophistication.

### *2.1. AI-Based Intrusion Detection in IoT*

The advent of deep learning has revolutionized intrusion detection, particularly in IoT networks. LSTM, a specialized recurrent neural network architecture introduced by Hochreiter and Schmidhuber [5], has gained immense popularity for its ability to capture temporal dependencies in sequential data. Within IoT environments, where time-series data are prevalent, LSTM models have shown promising capabilities in detecting anomalous behavior and potential cyber threats. Various researchers have explored LSTM-based intrusion detection systems, as evidenced by studies conducted by Dahou et al. [4], Yang et al. [16], and Yang et al. [17]. These investigations highlight the effectiveness of LSTM models in accurately identifying and categorizing diverse attacks in IoT environments.

### *2.2. Addressing Data Imbalance with SMOTE*

Imbalanced datasets, wherein one class significantly outweighs the others, pose a major challenge for intrusion detection systems, particularly in IoT scenarios. The prevalence of normal network traffic compared to actual attacks can lead to biased model performance. To overcome this limitation, Chawla et al. [8] proposed SMOTE, a synthetic data generation technique that rebalances class distribution by oversampling the minority class. SMOTE has gained widespread adoption in intrusion detection research, with notable studies by Joloudari et al. [18] and Fatani et al. [19]. showcasing its efficacy in enhancing the detection capabilities of IDS in IoT networks and mitigating the impact of class imbalance.

DLNID is an end-to-end model, eliminating the need for manual feature extraction. Experimental results on the NSL-KDD public benchmark dataset demonstrate that DLNID outperforms other comparison methods in terms of accuracy and F1 score, achieving 90.73% and 89.65%, respectively [20].

### *2.3. Optimizing Feature Selection with Random Forest*

Feature selection is a critical aspect of developing efficient and interpretable intrusion detection models. Random forest, an ensemble learning method introduced by Ustebay [10], is widely used for feature selection due to its ability to estimate feature importance and reduce overfitting. Within the context of IoT intrusion detection, random forest-based feature selection has been leveraged to identify critical attributes relevant to attack detection. Studies conducted by Elnakib et al. [21] and Speiser [22] demonstrate the effectiveness of recursive feature elimination (RFE) using random forest classifiers in optimizing the feature space and enhancing the overall performance of IDS.

### *2.4. Comprehensive Evaluation of Public Datasets*

To assess the effectiveness and generalizability of AI-driven intrusion detection systems, researchers commonly conduct extensive evaluations of publicly available datasets. Notable datasets such as CIC-IDS2017, NSL-KDD, and the UNSW-NB15 are widely used benchmarks for evaluating intrusion detection algorithms in IoT networks. Researchers like Jose and Jose [23] and Ashiku and Dagli [7] have extensively utilized these datasets to evaluate LSTM-based IDSs, showcasing improved accuracy and robustness.

Comparison Experiment:

In Chapter 4, we present a detailed comparison of our proposed method with established intrusion detection techniques from existing published articles. While well-known datasets are valuable for benchmarking, it is equally important to demonstrate how our method fares against state-of-the-art approaches.

We have conducted an extensive literature review to identify and include representative methods from the existing body of research on IoT intrusion detection. Some of the methods that we have compared our approach to include those presented by Chawla et al. [8], Joloudari et al. [18], and Fatani et al. [19], who have contributed significantly to the field.

Our comparison is not limited to dataset performance alone but also extends to a comprehensive evaluation of detection accuracy, false positive rates, computational efficiency, and adaptability to evolving threats. This broader perspective allows us to assess not only the advantages of our proposed method but also to highlight key differences and innovations when compared to various published methods.

By conducting this comprehensive comparison, we aim to provide a well-rounded understanding of how our approach stands in relation to existing state-of-the-art intrusion detection techniques in the context of IoT security. This analysis will offer valuable insights into the strengths and uniqueness of our method and demonstrate its superiority or distinctive qualities where applicable.

## 3. Methodology

In this section, we present the detailed methodology employed in the development of an advanced AI-based intrusion detection system (IDS) tailored for IoT networks. The primary objective of our research is to enhance data security and effectively detect potential cyberattacks in the rapidly evolving landscape of IoT environments.

The methodology encompasses key steps, each represented in Figure 1:

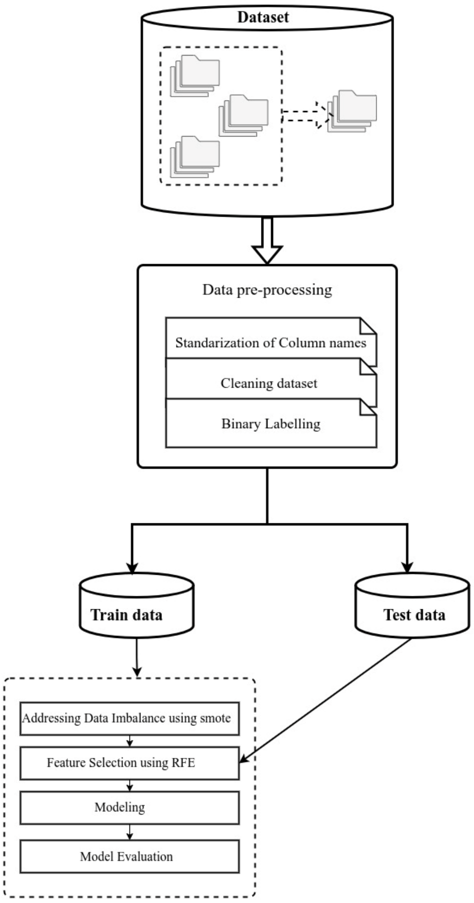

**Figure 1.** Proposed methodology overview.

These steps collectively form the foundation of our AI-enhanced IDS, enabling it to address the critical cybersecurity challenges faced by modern IoT networks. The following sections delve into the specifics of each step, providing comprehensive insights into our approach and its potential to significantly improve intrusion detection capabilities in IoT environments.

## *3.1. Dataset and Data Preprocessing*

### 3.1.1. Dataset Selection

The success of any intrusion detection system (IDS) heavily relies on the quality and representativeness of the datasets used for training and evaluation. In this research, we have diligently chosen three diverse and widely recognized datasets to ensure comprehensive coverage of network traffic scenarios and attack types, enhancing the credibility and generalizability of our findings.

### Intrusion Detection Evaluation Dataset (CIC-IDS2017)

The CIC-IDS2017 dataset plays a crucial role in advancing intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). Unlike many existing datasets, CIC-IDS2017 addresses key limitations by providing up-to-date and diverse network traffic data, including both benign and known attack scenarios [24].

To ensure realistic background traffic, the dataset incorporates the B-Profile system, which profiles human interactions to generate naturalistic benign traffic. The captured data spans five days and encompasses various attacks, such as Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet, and DDoS [24].

CIC-IDS2017 fulfills crucial criteria for a reliable benchmark dataset, including a complete network configuration, labeled dataset, complete interaction coverage, complete capture, available protocols, attack diversity, heterogeneity, feature set extraction, and comprehensive metadata [24]. These features make it a robust resource for evaluating and training IDSs in real-world scenarios.

#### NSL-KDD

The NSL-KDD dataset is a curated version of the KDD'99 dataset specifically designed to address its limitations and challenges [1]. While it may not fully represent real-world networks, its availability and refinements make it a valuable benchmark for evaluating intrusion detection methods [14].

One of the notable strengths of the NSL-KDD dataset is its reasonable size, with sufficient records in both the training and test sets. This feature enables researchers to conduct comprehensive experiments without resorting to random subsampling, ensuring consistency and comparability of the evaluation results [25].

Despite its imperfections, the NSL-KDD dataset remains a crucial resource for the intrusion detection community. Researchers can leverage it to develop and validate innovative techniques aimed at bolstering the security and effectiveness of network-based IDSs [14].

By acknowledging its limitations while utilizing its merits, the NSL-KDD dataset continues to play a pivotal role in advancing intrusion detection research and fostering the development of robust and efficient detection methods.

#### The UNSW-NB15 Dataset

The UNSW-NB15 dataset represents a significant and comprehensive resource tailored for network intrusion detection systems (IDSs). Developed to address the limitations of existing datasets, this repository provides a diverse and realistic collection of network traffic data, specifically designed to aid in the evaluation and advancement of IDSs [26].

The generation of the UNSW-NB15 dataset involved the use of advanced tools and methodologies. The IXIA Perfect Storm tool was employed to create a hybrid of authentic modern network activities and synthetic contemporary attack behaviors. Subsequently, the tcpdump tool was used to capture 100 GB of raw traffic, stored in pcap files, resulting in a dataset that reflects real-world network dynamics more accurately [15].

One of the key strengths of the UNSW-NB15 dataset lies in its comprehensive representation of various attack types. It encompasses nine distinct attack categories, including Fizzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. By encompassing a wide range of attack scenarios, the dataset enables researchers to evaluate IDSs' performance against diverse threats.

The dataset incorporates the Argus and Bro-IDS tools to generate a set of 49 features, each associated with a specific class label. These features are detailed in the UNSW-NB15_features.csv file, providing researchers with a deeper understanding of the dataset's attributes and facilitating feature-based analysis [15,25].

### 3.1.2. Data Preprocessing

Data preprocessing is a critical aspect of building a robust and accurate intrusion detection system (IDS). In this section, we present our meticulous approach to prepare the datasets for training and evaluating our AI-based IDS. Through essential steps, we aim to optimize the IDS's performance in detecting cyber threats and enhancing network security.

We address challenges such as class imbalance, diverse attack types, and feature selection using cutting-edge techniques. By curating a well-balanced dataset and selecting informative features, we empower the IDS to discern between benign and malicious network activities effectively.

In the following subsections, we detail each preprocessing step, ensuring the IDS's readiness to combat modern cybersecurity challenges.

#### Binary Labeling

To streamline our focus on binary classification, we transform the multi-class datasets into a binary format. This approach involves categorizing all distinct attack categories into a unified "attack" class, while maintaining normal network traffic as the "BENIGN" class. This binary setting facilitates a clear discrimination between malicious activities and benign network behavior, enabling our model to concentrate on detecting potential threats effectively.

### Addressing Data Imbalance

To ensure the reliability and effectiveness of our intrusion detection system (IDS) in handling real-world cyber threats, we meticulously addressed the issue of data imbalance in the training dataset. Imbalanced data, where one class is significantly more prevalent than the other, can lead to biased model performance, as the classifier may prioritize the majority class and overlook crucial instances of the minority class.

In our research, after conducting a thorough analysis of the dataset, we observed a substantial class imbalance problem, with a scarcity of instances representing certain network attacks compared to the abundance of benign network traffic samples. To mitigate this challenge, we employed the synthetic minority over-sampling technique (SMOTE) [8], a widely recognized approach that effectively balances the class distribution.

SMOTE works by generating synthetic instances for the minority class based on the existing minority samples. By synthesizing new attack instances that closely resemble genuine attack patterns, SMOTE strategically expands the number of minority class samples, bringing the class distribution closer to balance.

Additionally, to prevent overfitting and improve generalization, we applied SMOTE in conjunction with random under-sampling [8,9,26]. Random under-sampling selectively reduces the number of majority class instances, ensuring a more balanced and representative dataset while preserving the essential characteristics of both classes.

The combination of SMOTE and random under-sampling leads to an adequately balanced training dataset, empowering our IDS to learn from rare attack instances and detect potential cyber threats with greater accuracy. By introducing synthetic attack instances that align with genuine attack patterns, our model becomes more resilient and adaptive, capable of effectively handling the intricacies of real-world intrusion scenarios.

In summary, the application of SMOTE and random under-sampling in our training data sampling strategy serves as a crucial step in overcoming the data imbalance challenge. By creating a well-balanced dataset that adequately represents both normal and attack instances, our AI-based IDS demonstrates enhanced performance and robustness in detecting and mitigating cybersecurity threats in IoT networks.

### Feature Selection

Feature selection is a crucial step in the development of an effective intrusion detection system (IDS). It involves identifying and retaining the most informative attributes from the dataset while discarding less relevant ones. The goal is to reduce the dimensionality of the data and enhance the IDS's performance, interpretability, and efficiency.

In our research, we employ the recursive feature elimination (RFE) technique along with the random forest classifier algorithm for feature selection. RFE is a widely adopted method that systematically ranks and eliminates features based on their importance. The process involves the following key steps:

- Initialization: we start by creating a random forest classifier model, which serves as the base estimator for the RFE algorithm.
- Recursive Elimination: The RFE algorithm recursively eliminates the least important features by retraining the model at each iteration. Features are ranked based on their contribution to the classification task, and the least significant feature is removed.
- Convergence: The recursive elimination process continues until the desired number of features is reached. In our case, we select the top 20 features with the highest importance scores.

By applying the RFE technique, we achieve the following advantages:

- Enhanced Model Efficiency: with a reduced feature set, the IDS can process data more efficiently and expedite the intrusion detection process.
- Improved Model Interpretability: the selected features provide a concise representation of relevant information, facilitating easier interpretation of the IDS's decision-making process.
- Optimized Performance: by focusing on the most informative attributes, the IDS can achieve higher accuracy in distinguishing between normal network traffic and potential cyber threats.

The 20 selected features, derived through the RFE–random forest classifier approach, form a powerful subset that captures the essential characteristics of network traffic data. As a result, our AI-based IDS is equipped to perform with exceptional accuracy and effectiveness in identifying and mitigating various cyber threats commonly encountered in IoT networks.

### *3.2. Model Architecture*

In this section, we present the architectural design of our intrusion detection system (IDS), which is built upon a powerful binary classification model utilizing long short-term memory (LSTM) neural networks. LSTM is a specialized variant of recurrent neural networks (RNNs) known for their exceptional ability to handle sequential data, making them well suited for time-series analysis tasks, including network traffic data.

#### 3.2.1. Long Short-Term Memory (LSTM)

LSTM networks were specifically designed to address the vanishing gradient problem encountered in traditional RNNs. This issue limits the RNN's ability to retain and propagate relevant information across long sequences, hampering its capacity to capture temporal dependencies effectively [5,6].

The key components of an LSTM cell are as follows:

- Cell State (C_t): Serving as the memory component, the cell state enables the LSTM to retain essential information over time. It selectively regulates the information to be stored or discarded through specialized gates, allowing the network to learn long-term dependencies from the data.
- Input Gate (i_t): The input gate controls the flow of new information into the cell state. It decides which values from the current input and the previous hidden state should be incorporated into the cell state.
- Forget Gate (f_t): The forget gate determines which information from the cell state should be forgotten. It allows the LSTM to selectively discard irrelevant or outdated information from previous time steps.
- Output Gate (o_t): The output gate governs the filtering of the cell state's information to compute the current hidden state. It regulates the information to be propagated to the next time step.

The mathematical transformations involved in the LSTM cell's internal operations are formulated as follows:

- **Input Gate (i_t):**

$$i_t = sigmoid\left(W_i * \left[h_{(t-1)}, x_t\right] + b_i\right)$$

- **Forget Gate (f_t):**

$$f_t = sigmoid\left(W_f * \left[h_{(t-1)}, x_t\right] + b_f\right)$$

- **Output Gate (o_t):**

$$O_t = sigmoid\left(W_o * \left[h_{(t-1)}, x_t\right] + b_o\right)$$

- **Cell State Update:**

$$u_t = thanh\left(W_c * \left[h_{(t-1)}, x_t\right] + b_c\right)$$

- **Hidden State (h_t):**

$$h_t = o_t * \tanh(u_t)$$

### 3.2.2. Model Architecture

Our binary classification model comprises a sequential arrangement of layers, starting with an LSTM layer featuring 30 units. This LSTM layer is followed by a dropout layer, which introduces regularization during training by randomly deactivating neurons, thus reducing the risk of overfitting and promoting generalization.

Subsequently, we incorporate a dense layer with a SoftMax activation function at the end. The dense layer generates a probability distribution over the two classes, namely, "BENIGN" and "attack," allowing our model to provide confident predictions.

The LSTM-based IDS model is optimized using the Adam optimizer and trained with the sparse categorical cross-entropy loss function, suitable for multi-class problems with integer labels.

To illustrate the architectural flow, we present Figure 2 which depicts the schematic representation of our LSTM-based IDS model. This figure visually portrays the architectural data flow of our binary classification model through the LSTM layer, followed by the dropout and dense layers, signifying the sequence of computations performed by our model.

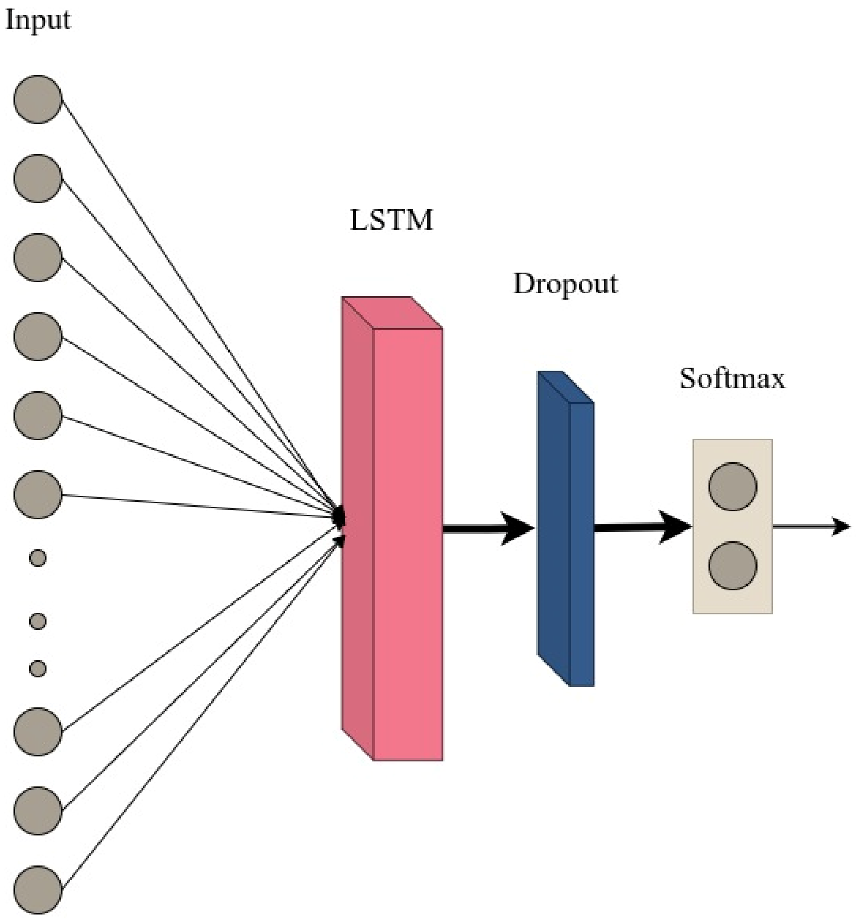

**Figure 2.** Schematic representation of the LSTM-based IDS model.

By harnessing the expressive power of LSTM networks, our model effectively captures the temporal dynamics inherent in network traffic data, facilitating accurate and timely detection of potential cyber threats within IoT networks. The LSTM's unique capacity to retain long-term dependencies, combined with its sequential data processing capabilities, empowers our IDS to achieve superior performance, reinforcing the resilience of IoT environments against intrusion attempts and bolstering overall cybersecurity measures.

## 4. Performance Evaluation and Comparison

The performance evaluation and comparison of our LSTM-based intrusion detection system (IDS) represent a crucial phase in validating the effectiveness and robustness of our proposed model. In this section, we present a detailed analysis of the IDS's performance using three distinct datasets: CICIDS2017, NSL-KDD, and UNSW-NB15. The primary aim is to assess the model's ability to accurately detect network intrusions across various real-world scenarios. To achieve this, we employ a set of standard evaluation metrics, providing valuable insights into the model's accuracy, precision, recall, F1-score, and AUC-ROC. Additionally, we utilize confusion matrices to gain a deeper understanding of the model's performance by analyzing true positive, false positive, true negative, and false negative predictions. By systematically evaluating and comparing the IDS on different datasets, we aim to validate its effectiveness in real-world intrusion detection scenarios, addressing the ever-evolving challenges of network security.

### *4.1. Evaluation Metrics*

In the process of rigorously evaluating the performance of our LSTM-based intrusion detection system (IDS), we rely on a set of standard evaluation metrics that facilitate a comprehensive assessment of the model's effectiveness in detecting network intrusions. These metrics play a pivotal role in gauging the accuracy and reliability of our proposed IDS, thereby guiding us toward valuable insights regarding its performance.

#### 4.1.1. Accuracy

Accuracy stands as a fundamental metric in the realm of classification models, offering a measure of the overall performance. It signifies the proportion of correctly classified instances, encompassing both true positives and true negatives, in relation to the total number of instances present in the dataset. Mathematically, the accuracy is computed as follows:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN)$$

#### 4.1.2. Precision

As a prominent measure termed the positive predictive value, precision signifies the accuracy of positive predictions made by our model. It is ascertained by evaluating the ratio of true positive predictions to the overall instances classified as positive. Mathematically, precision is expressed as follows [27]:

$$Precision = TP/(TP + FP)$$

#### 4.1.3. Recall (Sensitivity or True Positive Rate)

Recall, also known as sensitivity or true positive rate, offers an assessment of the model's capacity to accurately identify positive instances in contrast to the actual positive instances existing within the dataset. The ratio of true positive predictions to the total actual positive instances determines the recall value. Mathematically, recall is calculated as follows:

$$Recall = TP/(TP + FN)$$

#### 4.1.4. F1-Score

The F1-score, serving as the harmonic mean of precision and recall, presents a balanced evaluation of the two metrics. It plays a vital role, especially when there is an imbalance between the number of positive and negative instances in the dataset. The F1-score is mathematically computed through the following formula:

$$\mathrm{F1} - Score = 2 * (Precision * Recall)/(Precision + Recall)$$

#### 4.1.5. Area under the Receiver Operating Characteristic Curve (AUC-ROC)

The AUC-ROC metric serves as a valuable performance indicator to evaluate the model's ability to distinguish between positive and negative instances. The ROC curve portrays the true positive rate (recall) against the false positive rate (1—specificity) at diverse classification thresholds. The AUC-ROC encapsulates the area beneath this curve and offers a singular value that quantifies the model's discriminative power. Ideally, a perfect classifier demonstrates an AUC-ROC value of 1, while a random or ineffective classifier exhibits an AUC-ROC value of 0.5 [28,29].

#### 4.1.6. Confusion Matrix

An integral aspect of our performance evaluation entails the utilization of a confusion matrix. This tabular representation allows for a succinct summary of the classification model's performance by displaying the count of true positive (TP), false positive (FP), true negative (TN), and false negative (FN) predictions. The confusion matrix acts as a critical tool in acquiring a comprehensive understanding of the model's capabilities, identifying its strengths, and highlighting potential areas for improvement.

The confusion matrix is typically presented in the following format Table 1.

**Table 1.** Confusion matrix.

| | **Predicted** | |
|---|---|---|
| Actual | True Positive (TP) | False Negative (FN) |
| | False Positive (FP) | True Negative (TN) |

Through an in-depth analysis of the values within the confusion matrix, we can derive various evaluation metrics, including accuracy, precision, recall, and F1-score, which enable us to glean valuable insights into the model's performance for each class.

In the forthcoming sections, we embark on a detailed exposition of the results attained through the evaluation metrics and confusion matrices for our LSTM-based IDS, leveraging the CICIDS2017, NSL-KDD, and UNSW-NB15 datasets. This comprehensive analysis serves as a validation of the efficacy and adaptability of our model in precisely detecting network intrusions across a diverse array of real-world scenarios.

### *4.2. Results and Comparison*

In this section, we present a comprehensive evaluation and comparison of our LSTM-based intrusion detection system (IDS) across three distinct datasets: CICIDS2017, NSL-KDD, and UNSW-NB15. We provide detailed analyses of various evaluation metrics, including accuracy, precision, recall, and F1-score, as well as the visualization of loss curves, confusion matrices, and receiver operating characteristic (ROC) curves.

#### 4.2.1. CICIDS2017 Dataset

For the CICIDS2017 dataset, our LSTM-based IDS achieves an overall accuracy of 99.34%. The precision for the "BENIGN" class is 99.94%, while the recall reaches 99.24%, resulting in an F1-score of 99.59%. For the "attack" class, the precision remains high at 96.99%, and the recall is outstanding at 99.74%, contributing to an F1-score of 98.35% as showing in Table 2, Confusion matrix for CICIDS2017 dataset showing in Figure 3, and ROC curve for CICIDS2017 dataset Figure 4.

**Table 2.** Classification report for CICIDS2017 dataset.

| | Precision | Recall | Fl-Score | Support |
|---|---|---|---|---|
| BENIGN | 1.00 | 0.99 | 1.00 | 567,830 |
| Attack | 0.97 | 1.00 | 0.98 | 139,139 |
| Accuracy | | | 0.99 | 706,969 |
| Macro avg | 0.98 | 0.99 | 0.99 | 706,969 |
| Weighted avg | 0.99 | 0.99 | 0.99 | 706,969 |

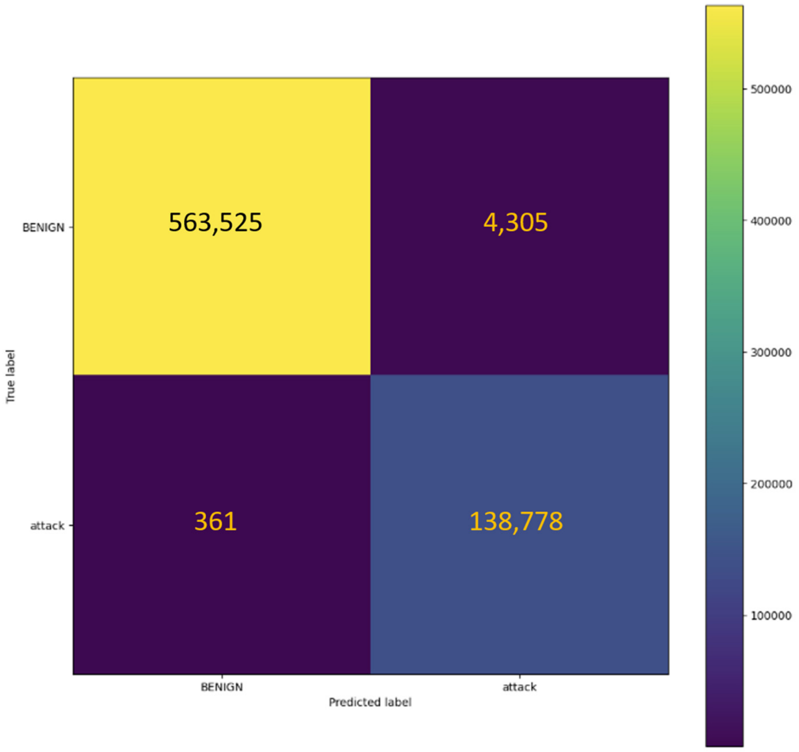

**Figure 3.** Confusion matrix for CICIDS2017 dataset.

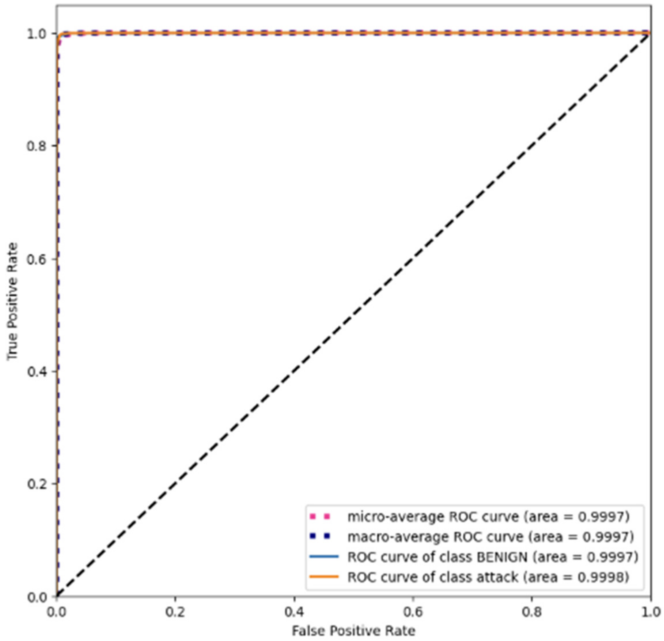

**Figure 4.** ROC curve for CICIDS2017 dataset.

### 4.2.2. NSL-KDD Dataset

The NSL-KDD dataset showcases remarkable performance for our LSTM-based IDS, with an accuracy of 99.75%. The precision and recall for the "BENIGN" class are 99.56% and 99.94%, respectively, leading to an F1-score of 99.75%. Similarly, the precision and recall for the "attack" class are both exceptional at 99.94% and 99.57%, respectively, resulting in an F1-score of 99.75% as showing in Table 3, Confusion matrix for NSL-KDD dataset Figure 5, and ROC curve for NSL-KDD dataset Figure 6.

**Table 3.** Classification report for NSL-KDD dataset.

| | **Precision** | **Recall** | **Fl-Score** | **Support** |
|---|---|---|---|---|
| BENIGN | 1.00 | 1.00 | 1.00 | 67,343 |
| Attack | 1.00 | 1.00 | 1.00 | 67,343 |
| Accuracy | | | 1.00 | 134,686 |
| Macro avg | 1.00 | 1.00 | 1.00 | 134,686 |
| Weighted avg | 1.00 | 1.00 | 1.00 | 134,686 |

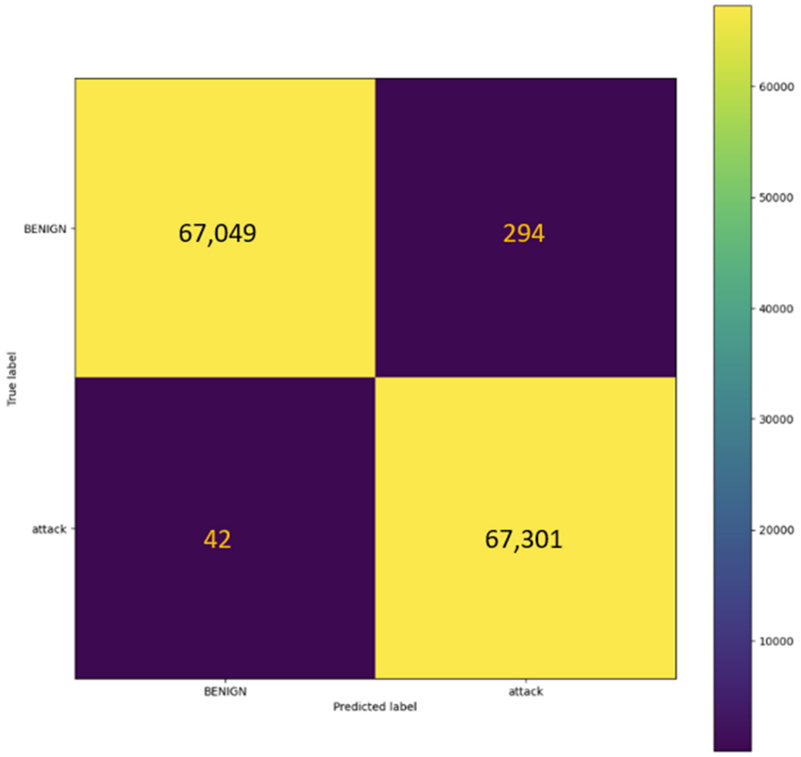

**Figure 5.** Confusion matrix for NSL-KDD dataset.

### 4.2.3. UNSW-NB15 Dataset

Our LSTM-based IDS demonstrates exceptional performance on the UNSW-NB15 dataset, achieving an accuracy of 98.31%. The precision and recall for the "BENIGN" class are 97.87% and 98.74%, respectively, resulting in an F1-score of 98.30%. For the "attack" class, the precision remains high at 98.75%, while the recall reaches 97.89%, contributing to an F1-score of 98.32% as showing in Table 4, Confusion matrix for UNSW-NB15 dataset Figure 7, and ROC curve for UNSW-NB15 dataset Figure 8.

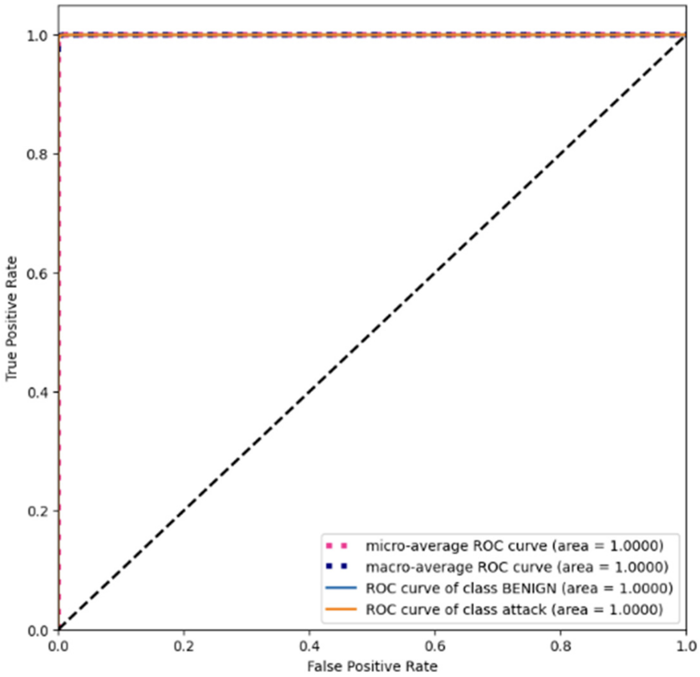

**Figure 6.** ROC curve for NSL-KDD dataset.

**Table 4.** Classification report for UNSW-NB15 dataset.

| | Precision | Recall | Fl-Score | Support |
|---|---|---|---|---|
| BENIGN | 0.99 | 0.98 | 0.98 | 46,236 |
| Attack | 0.98 | 0.99 | 0.98 | 46,236 |
| Accuracy | | | 0.98 | 92,526 |
| Macro avg | 0.98 | 0.98 | 0.98 | 92,526 |
| Weighted avg | 0.98 | 0.98 | 0.98 | 92,526 |

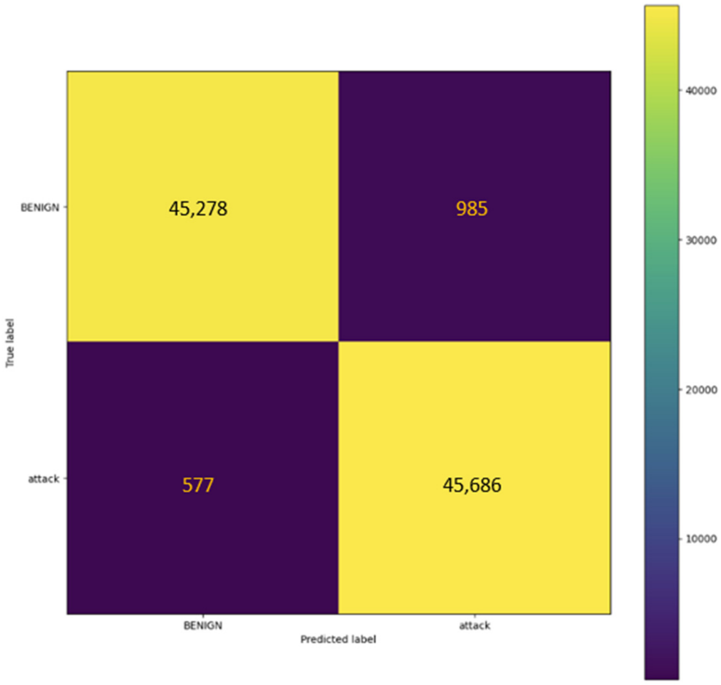

**Figure 7.** Confusion matrix for UNSW-NB15 dataset.

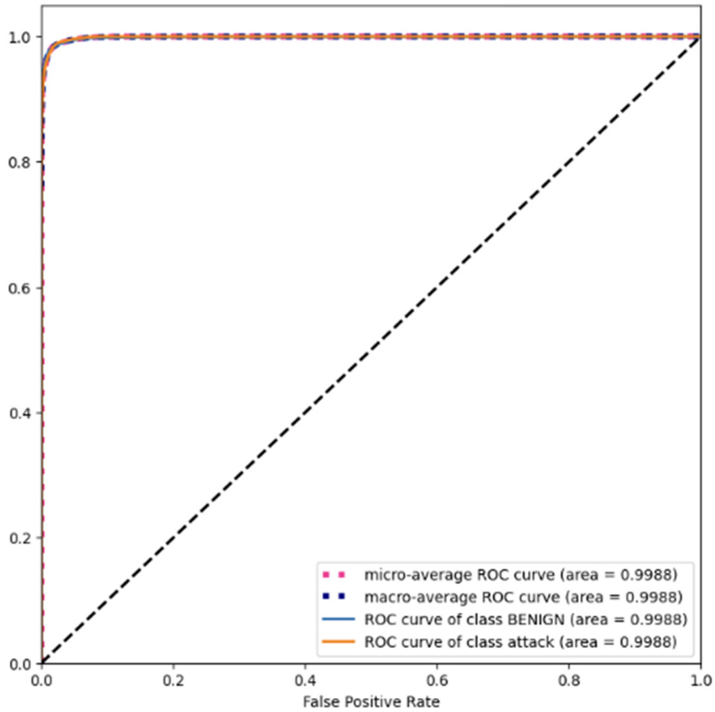

**Figure 8.** ROC curve for UNSW-NB15 dataset.

### 4.2.4. Overall Comparison

Figure 9 illustrates the loss curves for each dataset during the training process. Early stopping was applied to determine the optimal number of epochs for each dataset, with the CICIDS2017 dataset stopping at epoch 80, the NSL-KDD dataset at epoch 350, and the UNSW-NB15 dataset at epoch 78. The loss curves indicate the convergence of the model during training, and the early stopping ensures the prevention of overfitting.

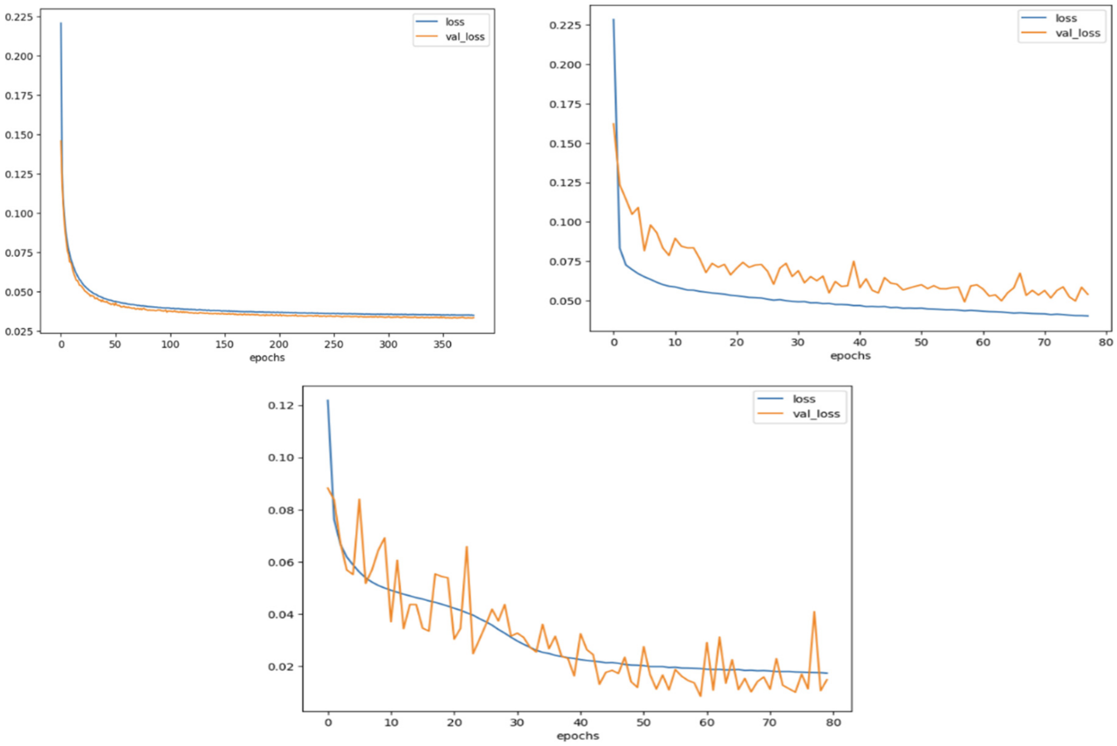

**Figure 9.** Loss curves for each dataset during the training process.

Additionally, Figure 10 showcases a bar plot comparing the accuracy, precision, recall, and F1-score achieved by our LSTM-based IDS across the three datasets: CICIDS2017, NSL-KDD, and UNSW-NB15. The bar plot visually illustrates the superior performance of our intrusion detection model in all metrics, as evidenced by the prominently displayed values for each dataset. The remarkable results further validate the effectiveness and robustness of our proposed approach in accurately detecting network intrusions across diverse real-world scenarios.

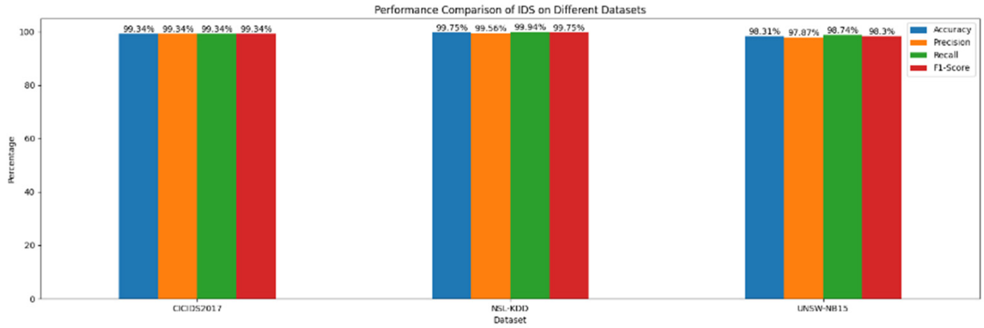

**Figure 10.** A bar plot comparing the accuracy.

Furthermore, Table 5 offers a comprehensive comparison of the evaluation metrics for each dataset. The table highlights the performance of our LSTM-based IDS in terms of accuracy, precision, recall, and F1-score, allowing for an easy comparison between the datasets.

**Table 5.** Performance comparison of LSTM-based IDS on three datasets.

| Dataset | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| CICIDS2017 | 99.34% | 99.34% | 99.34% | 99.34% |
| NSL-KDD | 99.75% | 99.56% | 99.94% | 99.75% |
| UNSW-NB15 | 98.31% | 97.87% | 98.74% | 98.30% |

Overall, the results demonstrate the effectiveness and robustness of our LSTM-based IDS in accurately detecting network intrusions across diverse real-world scenarios. The model exhibits exceptional performance across all three datasets, validating its capability to handle varying levels of complexity and imbalanced data. The superiority of our proposed IDS is evident, offering promising potential for real-world deployment in network security applications.

The Focus on the LSTM Model:

Our decision to utilize the long short-term memory (LSTM) model was driven by its well-established ability to effectively model sequential data, making it particularly suitable for intrusion detection in network traffic where the order of events is crucial.

LSTM's recurrent architecture enables it to capture and learn intricate patterns and dependencies from data traffic, which can be challenging for traditional machine learning models.

Additionally, LSTM has shown promising results in previous intrusion detection research, further motivating its inclusion in our study.

Consideration of Other Models:

While our primary focus was on LSTM due to its sequential data modeling capabilities, we acknowledge the existence of other recently developed machine learning models reported in the literature. These models, including deep learning architectures and ensemble methods, have indeed shown promise in various applications.

Justification for Future Work:

In our research, we opted for a focused approach to thoroughly investigate the potential of LSTM-based intrusion detection, particularly in the context of IoT networks. However, we recognize the importance of considering and comparing other state-of-the-art machine learning models in future work. This would allow for a more comprehensive evaluation of various approaches and their suitability for different intrusion detection scenarios.

Future Research Directions:

As part of future research directions, we plan to explore the integration and comparison of multiple machine learning models, including recently developed ones, to further enhance the performance and robustness of our intrusion detection system. This will enable us to assess the advantages and limitations of different models and provide a more comprehensive understanding of their applicability in IoT security.

Bi-LSTM Advantages:

Sequential Data Modeling: The primary objective of our research is to effectively model and analyze sequential data, such as network traffic patterns. The Bi-LSTM architecture is well suited for this task as it can capture dependencies in both forward and backward directions, enabling a more comprehensive understanding of sequential information.

Enhanced Feature Learning: Bi-LSTM has the capacity to learn and extract features from sequences with a higher level of complexity compared to its unidirectional counterpart (Vanilla LSTM). This feature extraction capability is crucial in the context of intrusion detection, where identifying subtle patterns in network traffic is essential.

Robustness: Bi-LSTM's bidirectional nature enhances the robustness of our intrusion detection system. It can capture dependencies that may be missed by unidirectional models, improving the overall accuracy of intrusion detection.

Previous Success: Prior studies on intrusion detection and sequential data analysis have reported promising results with the use of Bi-LSTM. By building upon this established success, we aim to leverage its strengths in our research.

Rationale:

Our rationale for choosing Bi-LSTM was driven by the need to effectively model and learn from the sequential nature of network traffic data. We believe that the bidirectional architecture's ability to capture dependencies and patterns from both directions aligns with the requirements of our research, where accurate intrusion detection relies on a holistic understanding of data flows.

However, we acknowledge that different LSTM variants, such as Stacked LSTM or Vanilla LSTM, have their own merits and may be suitable for specific applications. In future research, we intend to explore and compare various LSTM architectures to provide a more comprehensive understanding of their respective strengths and limitations in the context of intrusion detection.

## 5. Conclusions

In conclusion, this research introduces a powerful LSTM-based intrusion detection system (IDS) specifically designed for IoT networks. By harnessing the potential of cutting-edge deep learning techniques, our approach demonstrates outstanding performance in accurately detecting network intrusions, thereby significantly enhancing IoT security.

The effectiveness of our IDS stems from meticulous data preprocessing techniques. Addressing data imbalance through the synthetic minority over-sampling technique (SMOTE) and optimizing feature selection using recursive feature elimination (RFE) enable the system to discern between normal and malicious network activities with precision.

Notably, our LSTM architecture yields remarkable accuracy rates of 99.34% for CICIDS2017, 99.67% for NSL-KDD, and 98.31% for UNSW-NB15. These impressive results underscore the importance of effective data preparation and advanced deep learning methodologies in IoT intrusion detection.

As we envision the future, further research should focus on exploring sophisticated LSTM architectures and conducting real-world experiments to strengthen the IDS's adaptability and precision in dynamic IoT environments. Continual refinement and innovative techniques will establish our system as a cutting-edge intrusion detection solution, providing robust defense against evolving cyber threats in IoT infrastructures.

**Author Contributions:** Conceptualization, H.R.S.; methodology, H.R.S. and A.M.A.-m.; software, H.R.S.; validation, A.M.A.-m., W.D. and A.M.A.-m.; formal analysis, H.R.S.; investigation, H.R.S.; resources, H.R.S.; data curation, H.R.S.; writing—original draft preparation, H.R.S. and A.M.A.-m.; writing—review and editing, H.R.S., W.D. and A.M.A.-m.; visualization, H.R.S.; supervision, W.D.; project administration, H.R.S.; funding acquisition, A.M.A.-m. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data are contained within the article.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Malik, N.; Sardaraz, M.; Tahir, M.; Shah, B.; Ali, G.; Moreira, F. Energy-efficient load balancing algorithm for workflow scheduling in cloud data centers using queuing and thresholds. *Appl. Sci.* **2021**, *11*, 5849. [CrossRef]
2. Baiyere, A.; Topi, H.; Venkatesh, V.; Wyatt, J.; Design, R.; Donnellan, B. Communications of the Association for Information Systems Internet of Things (IoT)—A Research Agenda for Information Systems. Available online: https://ssrn.com/abstract=3844214 (accessed on 24 May 2022).
3. Lone, A.N.; Mustajab, S.; Alam, M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Secur. Priv.* **2023**, *6*, e318. [CrossRef]
4. Dahou, A.; Abd Elaziz, M.; Chelloug, S.A.; Awadallah, M.A.; Al-Betar, M.A.; Al-Qaness, M.A.; Forestiero, A. Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm. *Comput. Intell. Neurosci.* **2022**, *2022*, 6473507. [CrossRef]
5. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef] [PubMed]
6. Hnamte, V.; Hussain, J. DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System. *Telemat. Inform. Rep.* **2023**, *10*, 100053. [CrossRef]
7. Ashiku, L.; Dagli, C. Network Intrusion Detection System using Deep Learning. In *Procedia Computer Science*; Elsevier B.V.: Amsterdam, The Netherlands, 2021; pp. 239–247. [CrossRef]
8. Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic Minority over-sampling Technique. *J. Artif. Intell. Res.* **2002**, *16*, 321–357. [CrossRef]
9. Wang, S.; Dai, Y.; Shen, J.; Xuan, J. Research on expansion and classification of imbalanced data based on SMOTE algorithm. *Sci. Rep.* **2021**, *11*, 24039. [CrossRef] [PubMed]
10. Ustebay, S.; Turgut, Z.; Aydin, M.A. Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier. In Proceedings of the International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018—Proceedings, Ankara, Turkey, 3–4 December 2018; pp. 71–76. [CrossRef]
11. Darst, B.F.; Malecki, K.C.; Engelman, C.D. Using recursive feature elimination in random forest to account for correlated variables in high dimensional data. *BMC Genet.* **2018**, *19*, 65. [CrossRef] [PubMed]
12. Granitto, P.M.; Furlanello, C.; Biasioli, F.; Gasperi, F. Recursive feature elimination with random forest for PTR-MS analysis of agroindustrial products. *Chemom. Intell. Lab. Syst.* **2006**, *83*, 83–90. [CrossRef]
13. IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 23 July 2023).
14. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, Ottawa, ON, Canada, 8–10 July 2009. [CrossRef]
15. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference, MilCIS 2015—Proceedings, Canberra, Australia, 10–12 November 2015. [CrossRef]

16. Yang, L.; Moubayed, A.; Hamieh, I.; Shami, A. Tree-based Intelligent Intrusion Detection System in Internet of Vehicles. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Big Island, HI, USA, 9–13 December 2019. [CrossRef]
17. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 616–632. [CrossRef]
18. Joloudari, J.H.; Marefat, A.; Nematollahi, M.A.; Oyelere, S.S.; Hussain, S. Effective Class-Imbalance Learning Based on SMOTE and Convolutional Neural Networks. *Appl. Sci.* **2023**, *13*, 4006. [CrossRef]
19. Fatani, A.; Dahou, A.; Abd Elaziz, M.; Al-Qaness, M.A.; Lu, S.; Alfadhli, S.A.; Alresheedi, S.S. Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks. *Sensors* **2023**, *23*, 4430. [CrossRef] [PubMed]
20. Fu, Y.; Du, Y.; Cao, Z.; Li, Q.; Xiang, W. A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. *Electronics* **2022**, *11*, 898. [CrossRef]
21. Elnakib, O.; Shaaban, E.; Mahmoud, M.; Emara, K. EIDM: Deep learning model for IoT intrusion detection systems. *J. Supercomput.* **2023**, *79*, 13241–13261. [CrossRef]
22. Speiser, J.L. A random forest method with feature selection for developing medical prediction models with clustered and longitudinal data. *J. Biomed. Inform.* **2021**, *117*, 103763. [CrossRef] [PubMed]
23. Jose, J.; Jose, D.V. Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset. *Int. J. Electr. Comput. Eng.* **2023**, *13*, 1134–1141. [CrossRef]
24. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the ICISSP 2018—Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal, 22–24 January 2018; SciTePress: NewBrunswick, Canada, 2018; pp. 108–116. [CrossRef]
25. Moustafa, N.; Slay, J. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Inf. Secur. J. A Glob. Perspect.* **2016**, *25*, 18–31. [CrossRef]
26. Chen, R.C.; Dewi, C.; Huang, S.W.; Caraka, R.E. Selecting critical features for data classification based on machine learning methods. *J. Big Data* **2020**, *7*, 52. [CrossRef]
27. Vujović, Ž.Đ. Classification Model Evaluation Metrics. Available online: www.ijacsa.thesai.org (accessed on 24 July 2021).
28. Tafvizi, A.; Avci, B.; Sundararajan, M. Attributing AUC-ROC to Analyze Binary Classifier Performance. May 2022. Available online: http://arxiv.org/abs/2205.11781 (accessed on 24 May 2022).
29. Zhang, R.; Yang, S.; Zhang, Q.; Xu, L.; He, Y.; Zhang, F. Graph-based few-shot learning with transformed feature propagation and optimal class allocation. *Neurocomputing* **2022**, *470*, 247–256. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.