Performance Evaluation of Intrusion Detection Systems on the TON_IoT Datasets Using a Feature Selection Method

Elijah Mwandata Maseno
Department of Computing and Information Technology
Mama Ngina University College
Gatundu, Nairobi, Kenya
masenoelijah@gmail.com

Zenghui Wang*
Department of Electrical and Smart Systems Engineering & Centre for Augmented Intelligence and Data Science
University of South Africa
Florida, Gauteng, South Africa
wangzengh@gmail.com

Yanxia Sun
Department of Electrical and Electronic Engineering Science
University of Johannesburg
Johannesburg, Gauteng, South Africa
sunyanxia@gmail.com

Abstract

As Internet of Things (IoT) technology develops so quickly, security issues with IoT devices have come to light. IoT is an array of intelligent devices connected via a network to provide various services. The amount of data generated by these devices has an impact on how well the current intrusion detection systems (IDS) function. The generated dataset consists of irrelevant features which reduces the performance of IDS, making IoT ecosystem vulnerable to cyberattacks. The researchers have suggested the feature reduction technique as a potential solution to the current problem. The proposed method seeks to reduce the feature count by removing the redundant feature subset. Several machine learning methods have been successfully implemented in this discipline. This study proposed the application of hybrid feature reduction technique. The research combined Convolutional neural network (CNN) and Long short-term memory (LSTM); CNN extracted local features and decreased dimensionality, while LSTM identified long-term relationships in the data. SVM and Random Forest classifiers models were used to classify the chosen feature subset. This study employed the TON_IoT Datasets, an up-to-date dataset, to evaluate the model. During data preprocessing, the study applied SMOTETomek data pre-processing technique to address class imbalance in the dataset. With the decreased feature subset, the classification models fared reasonably well; RF had a 98% accuracy rate while SVM had a 91% accuracy rate, showcasing the suggested methodology's potential for creating efficient IDS.

CCS Concepts

• **Security and Privacy**; • **Theory of Computation**; • **Computing Methodologies**;

Keywords

IoT, CNN, LSTM, ML, Feature Selection

ACM Reference Format:
Elijah Mwandata Maseno, Zenghui Wang, and Yanxia Sun. 2024. Performance Evaluation of Intrusion Detection Systems on the TON_IoT Datasets Using a Feature Selection Method. In *2024 8th International Conference on Computer Science and Artificial Intelligence (CSAI) (CSAI 2024), December 06–08, 2024, Beijing, China.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3709026.3709048

*Corresponding author.

CSAI 2024, Beijing, China

ACM ISBN 979-8-4007-1818-2/2024/12
https://doi.org/10.1145/3709026.3709048

1 Introduction

Over the past ten years, there has been an increase in interest in the integration of intelligent devices via networks to provide a range of services. The networked gadgets produce enormous amounts of sensitive data [1]. Cybercriminals have become interested in the generated data and are working nonstop to get past the security measures and access this data. Because of the massive amount of data generated in IoT environments, the majority of preventive mechanisms in place are ineffective in efficiently thwarting cyber threats. A study conducted by [2] observed that as the feature space expands, the accuracy of current machine learning-based IDS techniques is significantly impacted. Several studies have proposed feature selection technique as a possible solution to this problem. The idea behind the feature selection method is to reduce the number of features through elimination of the redundant features. The main problem is how well to reduce the number of features while preserving the significant features for efficient and effective intrusion detection systems. Machine learning algorithms have applied in this field with great success. However, most of the existing works use outdate datasets in the evaluation of their models. Because these data sets don't accurately represent the real-world digital environment, they have drawn a lot of criticism [3].

A study by [4] suggested a filter feature reduction technique using XGBoost algorithm. The study reported an increase in detection rate using decision tree (DT) algorithm using the selected feature subset. The application of deep learning algorithms in feature reduction has been on the rise due to their potential in the selection of optimal features in a data set. A study by [5] combined two deep learning algorithms namely Convolutional Neural Network and a Bi-directional LSTM. In this work CNN was used for feature selection on NSL-KDD data set while BiLSTM was used for classification of attacks. The model reported high detection accuracy. In [6] the

authors proposed an intrusion detection system based on CNN and LSTM. This study illustrated CNN's potential for selecting the best feature subsets to enhance intrusion detection.

Due to the demonstrated capacity of deep learning algorithms in the selection of optimal feature subset in the field of IDS, this study aimed to adopt the integration of CNN and LSTM for feature section using a current IoT data set namely the TON_IoT Datasets. The primary contribution of this manuscript can be concise as follows:

- Our approach involved fine-tuning the TON_IoT data sets, through balancing of the data set using SMOTETomek approach, removing redundant features, and selecting only the most distinctive features using CNN-LSTM in order to maximize its performance for accurate attack categorization.
- Application of SVM and RF for classification of attacks.
- Evaluation of the proposed IDS using up to date data sets (the TON_IoT Datasets).

The rest of the study is organized as follows: Section 2 focuses on the related study; Section 3 gives a synopsis of machine learning techniques used is this work; Section 4 focuses on the IoT_ToN data set description and pre-processing; Section 5 gives the proposed research methodology of this study; Section 6 describes the experimental results and discussion and lastly the conclusion of this work is given in Section 7.

2 Related Study

With the huge amount volume of data in IoT, research show that is difficult to detect network attacks with high degree of accuracy [7]. The authors indicated that with feature selection we can learn the behaviour of network attacks with more precision. In addition, the huge volume of data hinders a classifier from making accurate conclusions and slow down the classification process [8]. As outlined earlier in this paper, ML algorithms have the potential of improving the performance of intrusion detection systems through feature selection [9]. This section focuses on some of existing works on feature selection using machine learning.

A study by [2] proposed a filter feature reduction methodology coupled with a deep learning algorithm for intrusion detection system. The first stage of this study perfumed feature selection using Feature Extraction Unit (FEU), a filter-based approach to extract the best feature subset on NSL-KDD dataset. Feed forward deep neural networks (FFDNNs) model had a better accuracy compared with the other models. Deep learning algorithms have shown their effectiveness in feature reduction through their capabilities to investigate every conceivable feature set in the dataset with the least amount of input [10]. A research by [11] used integrated two deep learning algorithms namely CNN and LSTM together with self-attention mechanism (SA) to select the optimal feature subset in NSL-KDD dataset. The proposed methodology reported high possibility of improving the effectiveness of network intrusion detection systems. Following similar approach [12] prosed a CNN-RNN deep learning technique to extract spatial and temporal features in TON_IoT-Datasets. This study deployed SVM to classify the selected feature subset. With an accuracy of 0.9959, the model outperformed other models.

In their work [7] applied the Variance threshold and Chi-square Test feature selection techniques for effective feature selection. The researcher used real world data set known as Advanced security Network Metrics dataset (ASNM) for the model evaluation. Logistic regression and neural networks were used for classification. Tested with the reduced feature subset the NN reported an accuracy of 99%. [13] applied three feature reduction technique namely the ANOVA F-value based method, impurity-based feature selection, and mutual information-based. The DL algorithm applied in this research, namely feed forward neural networks was tested using Kaggle and CICIDS-2017. The model reported an accuracy of 88% and 99.9% respectively. This research demonstrated the potential of integrating deep learning with feature selection for intrusion detection. In a similar manner [14] evaluated the impact of feature selection in the performance of IDS. The researchers applied Anova F-test, Mutual Information, and Chi-square to rate and select the most important features in the UNSW-NB15 dataset. The researchers used classical machine learning algorithms to evaluate their work. The selected algorithms rated differently using varying number of features, show casing the importance of feature selection on the performance of machine learning algorithm. This work can be evaluated further using modern machine learning algorithms.

In this study [15], the authors introduced a hybrid intrusion detection system based on deep learning algorithms. The researchers integrated Convolutional Neural Network (CNN) and bidirectional long short-term memory (BiLSTM) for classification of intrusions. To reduce the number of features in the training data set, random forest classifier and recursive feature selection techniques were adopted. The proposed model had a better detection accuracy with less training time. In [16] presented a novel feature selection technique based on two entropy-based techniques namely Gain Ratio (GR) in addition to Information Gain (IG). The proposed model reduced the number of features in IoTID20 and NSL-KDD datasets significantly. Tested and compared with other existing machine learning algorithms, the proposed model had a better detection accuracy.

The researchers in [17] proposed a feature selection approach based on Extreme Gradient Boosting (XGBoost). The model reduced the number of features in N-BaIoT dataset from the original 115 features to 30 features, an outstanding score. To teste the importance of the selected features, the researchers combined Convolutional Neural Networks (CNN) with Gated Recurrent Units the evaluation for classification of IoT data set. The model reported low processing time with high accuracy compared to CNN-LSTM and other IoT intrusion detection models. Further investigation can be performed using other IoT data sets as per the authors recommendations. In a similar manner [18] proposed an intrusion detection system with XGBoost-based feature selection approach. This approach was combined with various type of Recurrent Neural Networks (RNNs) and was evaluated using two types of data set namely NSL-KDD and the UNSW-NB15 benchmark datasets. With reduced data set XGBoost-LSTM reported the best performance, with 88.13% accuracy. On the other hand, XGBoost-Simple-RNN recorded the best outcome using UNSW-NB15 data set, with 87.07%. In future research, the researcher proposes the investigation of how well the suggested framework performs on certain classes found in the datasets under study.

A study by [19] proposed an intrusion detection system based on deep learning algorithms. This work adopted CNN together

with the fusion of an attention mechanism and the bidirectional long short-term memory (Bi-LSTM) network. In the first phase of this study CNN local features, the selected features are a signed weight through attention mechanism and lastly Bi-LSTM learns the network of sequence features. Adaptive synthetic sampling (ADASYN) was employed in this research to solve the data imbalance issue. NSL-KDD data set is used to evaluate the model's performance. The research reported a better accuracy and F1 score of 90.73% and 89.65%, respectively. The proposed model can be evaluated further using an up-to-date data set in future. In [20] fused recursive feature elimination and information gain for feature selection in IoT data set. For effective feature classification, the researchers adopted cascaded long–short-term memory. On the NSL-KDD and UNSW-NB15 datasets, respectively, this method's accuracy for binary classification was 99.30% and 98.96%.

A study by [21] proposed a network intrusion detection system based on genetic algorithm (GA) for feature selection and LSTM-RNN for classification of intrusion. In this work NSL-KDD dataset was used for model evaluation for both binary and multi-class intrusion. The researchers concluded that this approach has a potential of improving efficiency of intrusion detection. In addition, the researchers compared the performance of the model with other intrusion detection model and established that the model outperformed SVM in binary classification but had similar results with RF. On the other hand, the model outperformed both SVM and RF in multi-class classification. The only limitation of this study is that the evaluation was conducted using only one type of data set, it is recommended further investigation to be done using other types of data set. In [22] optimized GA using particle swarm optimization (PSO) for feature selection in IoT environment. For classification of intrusion the researchers employed LSTM-GRU in CICIDS-2017 dataset. The results demonstrate a significant improvement, with 98.86% accuracy in identifying multiple network attacks. Following the same pattern [23] developed a hybrid intrusion detection model based on Enhanced Binary Genetic Algorithms (EBGA) as a wrapper feature selection (FS) algorithm and Long LSTM. EBGA performs feature reduction and LSTM acts as a classification algorithm. The assessed model demonstrates how feature reduction with EBGA can improve the accuracy of LSTM classification. Similar to the majority of previous studies in this area, the researchers used an outdated dataset, the UNSW-NB15 data set.

3 A Synopsis of Machine Learning Techniques

This study adopted several machine learning algorithms to develop an effective intrusion detection system through feature reduction. The supervised machine learning techniques applied in this work are reviewed in the sections that follow.

3.1 Convolutional Neural Network (CNN)

Convolutional Neural Networks (CNNs) are a specialized form of Artificial Neural Networks (ANNs) designed to process and analyze data with a grid-like topology, such as images. CNNs, as opposed to classic ANNs, concentrate on spatial hierarchies in the data through shared weights and local receptive fields. This makes CNNs particularly effective at detecting patterns, such as edges and textures, in visual data by progressively abstracting and combining these features across multiple layers. CNNs are constructed with various essential elements, such as convolutional layers, pooling layers, and fully linked layers [11][16]. Convolutional layers create feature maps that highlight particular components of the input by applying convolutional operations using shared weights. By reducing the spatial dimensions of these feature maps, pooling layers improve the computational efficiency and input sensitivity of the network. Finally, fully connected layers integrate the extracted features to produce the final predictions, while non-linear activation functions enable the network to capture complex patterns in the data.

3.2 Long Short-Term Memory (LSTM)

LSTM is type of recurrent neural networks (RNNs) that was introduced to solve the problem of addressing the vanishing gradient problem encountered in RNNs while modeling sequential and temporal data [16][21]. LSTMs are particularly effective at capturing long-term dependencies in sequential data, such as time series, text, or speech, due to their unique architecture, which includes memory cells and gating mechanisms. These elements enable long-term selective retention or forgetting of information, which makes LSTMs ideal for jobs where context and order are essential. An LSTM network is made up of a sequence of LSTM cells, each of which has the input, forget, and output gates as its three main gates. The forget gate chooses which information should be discarded, the output gate chooses how much of the cell state should be sent to the next time step, and the input gate controls how much new information is added to the cell state. They differ from regular RNNs in that they can successfully manage temporal information and recall long-term dependencies, which makes them an effective tool for modeling complex sequences.

3.3 Support Vector Machine (SVM)

Support Vector Machines (SVM) one of the classical machine learning algorithm, is a powerful and versatile supervised learning algorithm used primarily for classification and regression tasks [24][25]. The core idea behind SVMs is to find the optimal hyperplane that separates data points from different classes with the maximum margin. This margin maximization makes SVMs particularly effective at handling high-dimensional spaces and cases where the number of dimensions exceeds the number of samples. By focusing on the data points closest to the decision boundary, known as support vectors, SVMs aim to enhance the model's generalization capabilities. Using a method called the kernel trick, SVMs convert the initial input space into a higher-dimensional feature space. By transferring the data into a space where a linear separator can be applied, this transformation enables SVMs to handle non-linearly separable data.

3.4 Random Forest (RF)

Random Forest (RF) is an ensemble learning method that combines the predictions of multiple decision trees to improve classification and regression accuracy [26]. Each tree in the forest is trained on a random subset of the data, with random subsets of features selected at each split, making the model robust against overfitting. The final prediction is typically made by aggregating the outputs of all

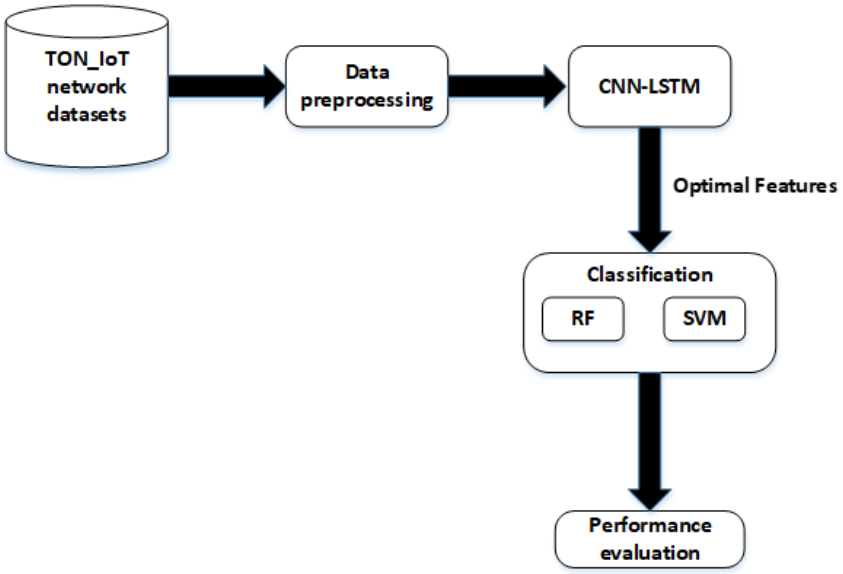

Figure 1: Structure of the proposed model

the trees, either through majority voting in classification tasks or averaging in regression tasks. This approach leverages the diversity of the trees, reducing variance and enhancing generalization. One of the key strengths of Random Forest is its ability to handle large datasets with high-dimensional features, as well as its resilience to noise and missing data. By averaging the predictions of numerous trees, Random Forest reduces the likelihood of overfitting, which is a common problem in individual decision trees.

4 the IoT_ToN DATA SET Description and Preprocessing

The study utilized the IoT_ToN network dataset due to its several advantages over other available datasets. This data set is publicly available and was developed by [27] to handle the lack of distributed architecture for creation of diverse datasets containing complicated cyber threat scenarios and the real-world behaviors of IoT networks, which can be used to assess the legitimacy of the new systems. The dataset consists of 461,043 events which represent the attacks and regular occurrences gathered from the network dataset.

To prepare the data set we followed steps outlined by [27]. Utilizing the Ordinal Encoder technique, this study transformed the categorical dataset into a numerical dataset. To solve the issue of class imbalance, this research applied SMOTETomek. Finally, training and testing datasets was reshaped to make the data set compatible with a Conv1D layer in CNN.

5 Proposed methodology

The model's initial step is data preprocessing, which is followed by the CNN-LSTM integration for optimal feature selection. The final step is using the classification model for intrusion detection, as seen in Figure 1 below.

The study adopted a 1D convolutional layer (50 filters, a kernel size of 5, and sigmoid activation) to capture local patterns in the input sequences, followed by max-pooling, dropout (with a rate of 0.3), and batch normalization to reduce dimensionality and prevent overfitting. An LSTM layer (with 64 units) was applied to learn long-term dependencies within the sequence, and an attention mechanism was applied to focus on the most relevant time steps, enhancing the model's ability to identify important features. The output was flattened and passed through a dense layer (with 512 units and ReLU activation) to transform the extracted features further, with an additional dropout layer (with a rate of 0.5) added to ensure robustness. The model was compiled with the Stochastic Gradient Descent (SGD) optimizer (with a learning rate of 0.001) and binary cross-entropy loss, and trained on a class-balanced dataset, making it well-suited for tasks involving imbalanced data. Finally, the feature extraction model was trained using the fit method on reshaped training data and the class-balanced labels, for 70 epochs with a batch size of 64, and 20% of the training data set aside for validation.

For classification, the extracted data from CNN-LSTM was standardized using Standard Scaler before applied as an input in support vector machine (SVM) classifier with a Radial Basis Function (RBF) kernel. The SVM classifier is configured with a penalty parameter C set to 1, and gamma='scale'.

Finally, RF was initialized using the RandomForestClassifier class, with n_estimators set to 100, to create a forest of 100 decision trees. The parameter random_state=42 was specified to ensure that the results are reproducible, meaning the model will produce the same output each time it's run with the same data and settings.

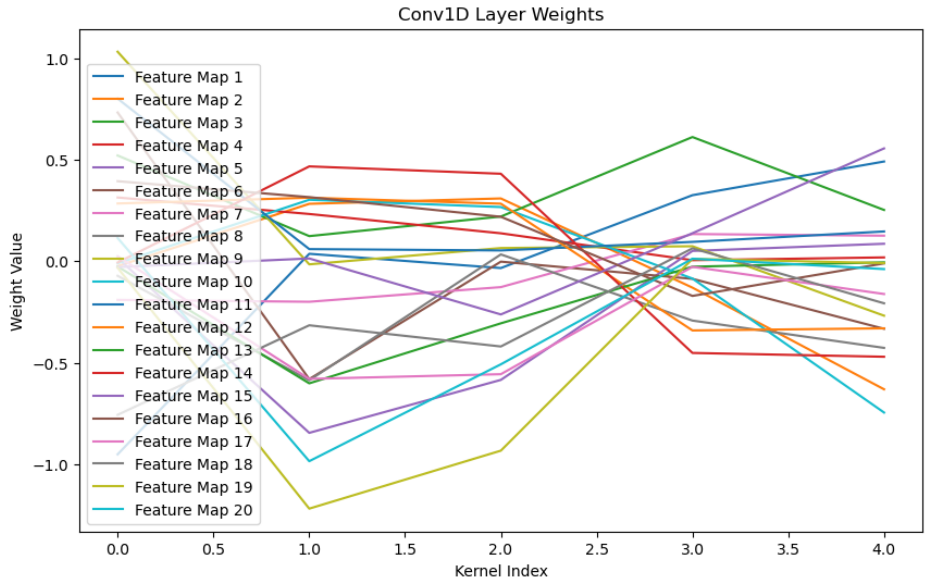

Figure 2: Visualization of Conv1D Filter Weights.

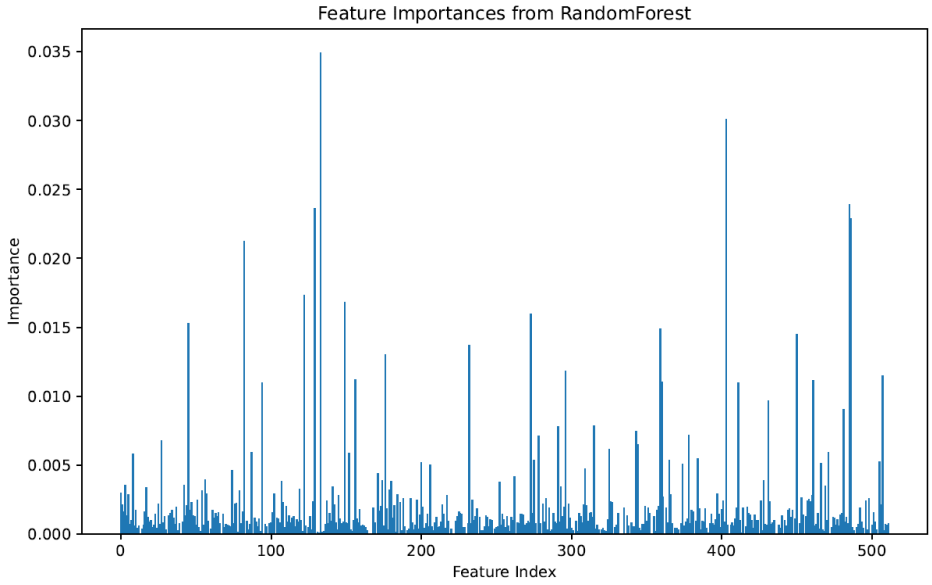

Figure 3: Feature importance from random forest.

6 Experimental Results and Discussion

This section discusses the results obtained from the evaluation of the proposed model.

6.1 Feature Selection

The proposed methodology applied CNN-LSTM together with attention mechanism for optimal feature selection. Figure 2 displays the weights for each output channel (or feature map) in the convolutional layer, demonstrating how the weights are distributed across the kernel and input channels. This study trained RF classifier with the selected feature subset to visualize the importance of each feature in the model. This helped in understanding which features were most influential in making predictions, providing insights into the model's decision-making process. Figure 3 displays features for the TON_IoT dataset that were identified using CNN-LSTM.

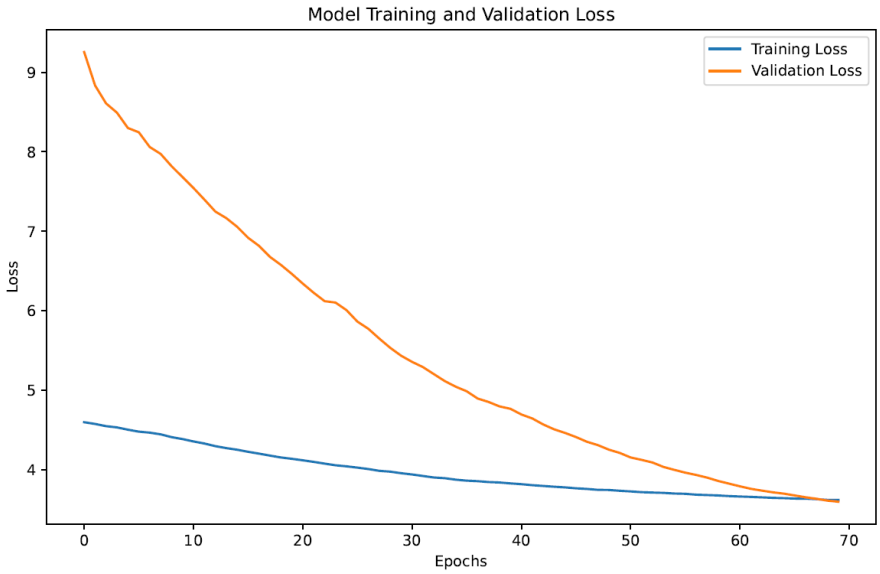

Figure 4: The training and validation loss graph.

Table 1: A summary of the classifiers' output using chosen feature

Classifier	Recall%	Accuracy%	Precision%
SVM	96	91	82
RF	98	98	93

Table 2: A summary of comparison with existing methods

Model	Data set	Classifier	Accuracy%
CNN - Bi-LSTM [28]	UNSW-NB15		94.21
CNN-BiLSTM [29]	UN0SW-NB15		97.09
CNN – LSTM [30]	UNSW-NB15		93.21
LSTM-RNN [31]	Kyoto University Dataset		97.10
BiLSTM-DNN [32]	NSL_KDD	SoftMax	76
Attention and BiLSTM-DNN(ABD) [33]	NSL_KDD	SoftMax	82
Proposed model	IoT_ToN network	SVM	91
Proposed model	IoT_ToN network	RF	98

6.2 Performance Metrics

To evaluate the efficacy of the classifiers, this study used the following metrics: recall, accuracy, and precision.

The selected feature subset is fed as an input to train the model. To visualizes the training and validation loss of the machine learning model over multiple epochs a graph is generated. Figure 4 is a representation of the training and validation loss graph.

Using the training data produced by the informative features chosen by the improved model, SVM and RF classifiers were trained. Testing data was then used to assess trained SVM and RF. SVM generated recall, accuracy, and precision of 96%, 91%, and 82% respectively. On the other hand, RF generated recall, accuracy, and precision of 98%, 98%, and 93% respectively. This was an outstanding performance demonstrating the ability of the proposed model to improve the efficiency of intrusion detection systems in IoT environments. Table 1 summarizes the performance of the classifiers.

As demonstrated in Table 2, the study found that the proposed intrusion detection model outperformed the majority of the other models in terms of accuracy when compared to other comparable

methodologies. To train and test the models, the majority of these models utilized various kinds of data sets. For a more accurate comparison, the model may be exposed to comparable kinds of data sets in the future.

7 Conclusion

In this work, a unique IDS model that combines CNN and LSTM together with attention mechanism for feature selection is presented. This approach's strength is demonstrated by its capacity to efficiently simplify dataset attributes and improve intrusion detection accuracy. Unlike most previous efforts in this sector, which employ outdated data sets incapable of capturing the complex cyber landscape, the model was assessed using the TON_IoT data set, which captures current cyber-attacks. The suggested model significantly improved detection accuracy when compared to similar previous efforts. The necessity for effective IDS, such as the one described in this study, grows as IoT networks expand in scope. In future, this research recommends the model to further evaluated using other type of data set.

Acknowledgments

This work was partly supported by the South African National Research Foundation under Grant nos. KIC240327211160, 141951, 137951, and AJCR230704126719120106.

References

[1] Sithungu, S. P., & Ehlers, E. M. (2022). GAAINet: A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems. 13(5), 456–461. https://doi.org/10.12720/jait.13.5.456-461

[2] Kasongo, S. M., & Sun, Y. (2019). A deep learning method with filter-based feature engineering for wireless intrusion detection system. IEEE Access, 7, 38597–38607. https://doi.org/10.1109/ACCESS.2019.2905633

[3] Ashiku, L., & Dagli, C. (2021). Network Intrusion Detection System using Deep Learning. Procedia Computer Science, 185, 239–247. https://doi.org/10.1016/j.procs.2021.05.025

[4] Kasongo, S. M., & Sun, Y. (2020). Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00379-6

[5] Kumar, L. K. S. (2021). *An Efficient Network Intrusion Detection Model Combining CNN and BiLSTM. 27*(06), 1782–1801. https://doi.org/10.47750/cibg.2021.27.06.140

[6] Du, J., Yang, K., Hu, Y., & Jiang, L. (2023). NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning. *IEEE Access*, *11*(January), 24808–24821. https://doi.org/10.1109/ACCESS.2023.3254915

[7] Desai, R., & Gopalakrishnan, V. T. (2023). Network Intrusion Detection Through Machine Learning With Efficient Feature Selection. *2023 15th International Conference on COMmunication Systems and NETworkS, COMSNETS 2023*, 797–801. https://doi.org/10.1109/COMSNETS56262.2023.10041315

[8] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE Transactions on Computers*, *65*(10), 2986–2998. https://doi.org/10.1109/TC.2016.2519914

[9] Sasikala, K., & Vasuhi, S. (2023). Anomaly Based Intrusion Detection on IOT Devices using Logistic Regression. *Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023*. https://doi.org/10.1109/ICNWC57852.2023.10127375

[10] Qazi, E. U. H., Almorjan, A., & Zia, T. (2022). A One-Dimensional Convolutional Neural Network (1D-CNN) Based Deep Learning System for Network Intrusion Detection. *Applied Sciences (Switzerland)*, *12*(16). https://doi.org/10.3390/app12167986

[11] Hui, B., & Chiew, K. L. (2025). An Improved Network Intrusion Detection Method Based On CNN-LSTM-SA. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *44*(1), 225–238. https://doi.org/10.37934/araset.44.1.225238

[12] Li, S., Chai, G., Wang, Y., Zhou, G., Li, Z., Yu, D., & Gao, R. (2023). CRSF: An Intrusion Detection Framework for Industrial Internet of Things Based on Pretrained CNN2D-RNN and SVM. *IEEE Access*, *11*, 92041–92054. https://doi.org/10.1109/ACCESS.2023.3307429

[13] Lakshmanarao, A., Srisaila, A., & Ravi Kiran, T. S. (2022). Machine Learning and Deep Learning framework with Feature Selection for Intrusion Detection. *2022 International Conference on Communication, Computing and Internet of Things, IC3IoT 2022 - Proceedings*. https://doi.org/10.1109/IC3IOT53935.2022.9767727

[14] Jain, S., Bihani, S., Jaiswal, S., & Arora, A. (2023). Impact of Feature Selection Algorithms on Network Intrusion Detection. *IEEE Symposium on Wireless Technology and Applications, ISWTA*, *2023-August*, 66–71. https://doi.org/10.1109/ISWTA58588.2023.10250134

[15] Ben Said, R., Sabir, Z., & Askerzade, I. (2023). CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection. *IEEE Access*, *11*, 138732–138747. https://doi.org/10.1109/ACCESS.2023.3340142

[16] Natarajan, B., Bose, S., Maheswaran, N., Logeswari, G., & Anitha, T. (2023). A New High-Performance Feature Selection Method for Machine Learning-Based IOT Intrusion Detection. *12th IEEE International Conference on Advanced Computing, ICoAC 2023*. https://doi.org/10.1109/ICoAC59537.2023.10249916

[17] Wang, Z., Huang, H., Du, R., Li, X., & Yuan, G. (2023). Frontiers in Computing and Intelligent Systems IoT Intrusion Detection Model based on CNN-GRU. *Frontiers in Computing and Intelligent Systems* , *4*(2).

[18] Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*(October 2022), 113–125. https://doi.org/10.1016/j.comcom.2022.12.010

[19] Fu, Y., Du, Y., Cao, Z., Li, Q., & Xiang, W. (2022). A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. *Electronics (Switzerland)*, *11*(6), 1–13. https://doi.org/10.3390/electronics11060898

[20] Sundaram, K., Natarajan, Y., Perumalsamy, A., & Yusuf Ali, A. A. (2024). A Novel Hybrid Feature Selection with Cascaded LSTM: Enhancing Security in IoT Networks. *Wireless Communications and Mobile Computing*, *2024*, 1–15. https://doi.org/10.1155/2024/5522431

[21] Muhuri, P. S., Chatterjee, P., Yuan, X., Roy, K., & Esterline, A. (2020). Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks. *Information (Switzerland)*, *11*(5). https://doi.org/10.3390/INFO11050243

[22] Al-Kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & Elaffendi, M. (2023). Intrusion Detection in the Internet of Things Using Fusion of GRU-LSTM Deep Learning Model. *Intelligent Automation and Soft Computing*, *37*(2), 2279–2290. https://doi.org/10.32604/iasc.2023.037673

[23] Azwari, S. Al, & Turabieh, H. (2021). Intrusion Detection using Deep Learning Long Short-term Memory with Wrapper Feature Selection Method. *International Journal of Advanced Computer Science and Applications*, *12*(3), 553–558. https://doi.org/10.14569/IJACSA.2021.0120366

[24] Kumari, A., & Mehta, A. K. (2020). A Hybrid Intrusion Detection System Based on Decision Tree and Support Vector Machine. *2020 IEEE 5th International Conference on Computing Communication and Automation, ICCCA 2020*, 396–400. https://doi.org/10.1109/ICCCA49541.2020.9250753

[25] Chen, C., Song, L., Bo, C., & Shuo, W. (2021). A Support Vector Machine with Particle Swarm Optimization Grey Wolf Optimizer for Network Intrusion Detection. *Proceedings - 2021 International Conference on Big Data Analysis and Computer Science, BDACS 2021*, 199–204. https://doi.org/10.1109/BDACS53596.2021.00051

[26] Liu, Y., Wang, Y., & Zhang, J. (2012). New machine learning algorithm: Random forest. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7473 LNCS, 246–252. https://doi.org/10.1007/978-3-642-34062-8_32

[27] Moustafa, N. (2021). A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society*, *72*, 102994. https://doi.org/10.1016/j.scs.2021.102994

[28] Sinha, J., & Manollas, M. (2020). Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection. *ACM International Conference Proceeding Series*, 223–231. https://doi.org/10.1145/3430199.343022

[29] Yin, J., Hou, B., Dai, J., & Zu, Y. (2024). A CNN-BiLSTM Method Based on Attention Mechanism for Class-imbalanced Abnormal Traffic Detection. ACM International Conference Proceeding Series. https://doi.org/10.1145/3653781.3653807

[30] Can, H., & Albayrak, Z. (2023). A hybrid CNN + LSTM-based intrusion detection system for industrial IoT networks. 38. https://doi.org/10.1016/j.jestch.2022.101322

[31] Patidar, S., Tripathi, M., & Gupta, S. K. (2021). Leveraging LSTM-RNN combined with SVM for Network Intrusion Detection. ACM International Conference Proceeding Series, 26–31. https://doi.org/10.1145/3484824.3484908

[32] Tao, Y., Zhang, J., Wei, L., Gao, Y., & Shi, L. (2023). An Intrusion Detection Model With Attention and BiLSTM-DNN. ACM International Conference Proceeding Series, 78–83. https://doi.org/10.1145/3590003.3590018