ÉCOLE NATIONALE SUPÉRIEURE D'ARTS ET MÉTIERS
UNIVERSITÉ HASSAN II DE CASABLANCA

Detection of Brute Force Attacks in Cybersecurity Using Hybrid Approaches Combining CNN and LSTM

AGDOUD FATIHA, HARRAG RHADA, CHAABAN HANANE

Master Big Data and Internet Of Things

Abstarct

Brute-force attacks constitute a significant form of a cyber-attack. They are a method of unauthorized access attempts through their brute-force attempts at different credentials of logins. Older detection techniques based on hard-coded rules or static thresholds can no longer be employed due to easy bypass methods by highly sophisticated and continuously evolving forms of brute force attack strategies. In this work, we propose a hybrid solution consisting of CNNs, and LSTMs, to improve the efficiency of brute-force attack detection. The CNN model is used to localize features available from the network traffic data. LSTMs are critical in capturing critical long-term dependencies and sequential patterns instrumental for identifying attack behavior progressively. In addressing the hybrid model's performance assessment, it relies on a labeled dataset of network traffic logs comprising benign samples and brute-force attack samples.

The proposed model provides clear superiority over both traditional and only heterogeneous models-concerning realization with a comparatively high level of accuracy, robustness, and adaptability to changes in dynamic attack patterns. This hence the novel approach becomes a scalable and efficient way of offering detection in real time for brute-force attacks in modern-day cybersecurity systems.

I. Introduction:

Cybersecurity is an extremely important aspect in the current today digital world in which cyber-crimes occur more frequently and in a more sophisticated way. Brute force attacks are just one of the many methods used among various threats for penetrating the secure systems. It involves trying all possible combinations of password or key either by cracking or war pounding weak authentication mechanisms. This increase in such attacks indicates the importance of securing computer systems with more powerful and effective detection methods.

With advancing technology, conventional rules-based and signature-based systems are slowly being replaced by dynamic and flexible systems such as Machine Learning (ML) and Deep Learning (DL). These technologies possess mighty capabilities because their evaluation of large amounts of data detects even the most difficult attack acts. For instance, Machine Learning helps in the model-building for anomalies due to patterns found in data whereas Deep Learning techniques such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory networks (LSTM) help in extracting very complicated features from raw data connection logs.

This paper aims to analyze the application of the hybrid model developed from the combined CNN and LSTM for the detection of brute-force attacks, which are a constant threat to cyber security. This method has been analyzed for performance comparison with traditional methods and against the results obtained using the individual models CNN and LSTM.

II. Related Works:

Brute force attack happens to be among the widely adopted cybersecurity threats in IoT networks. Unauthorized access can be performed through organized trials of usernames and passwords with the use of automated tools. This type of threat attack causes huge destruction in IoT because these will be targeted toward edge devices, which, ultimately, can control all connected devices. Older techniques of brute force attack mitigation and prevention include network-based Intrusion Detection Systems (IDS), rule-based anomaly detection as well as other techniques, such as the blacklist of IP addresses or enforcement of stricter password policies. However, these are usually characterized by limits like high false-positive rates, scalability issues, and delayed detection.

Machine learning and deep learning technologies have brought drastic changes to brute force attack detection. Some popular examples include the Decision Trees, Support Vector Machines (SVMs), and Deep Neural Networks (DNNs), which have adapted considerably to the emerging attack patterns. This was the work done by the authors [1]. They developed a classification model via a deep learning method, using the MQTT-IoT-IDS2020 dataset, to detect brute force attacks across IoT networks. Their construction model achieved an impressive accuracy of 99.6% using bi-flow features and 99.7% using uni-flow features. The results highly proof the robustness and scalability of the approach. It postulates that deep-learning-based techniques are likely to outperform conventional methodologies in being dynamic and intelligent intrusion detection systems specifically created for IoT networks.

In this paper [2], the authors present an efficient methodology for detecting SSH brute force attacks using supervised deep learning via Convolutional Neural Network (CNN). The model outperforms several conventional machine learning classifiers, including Naive Bayes, Logistic Regression, Decision Tree, k-Nearest Neighbors, and Support Vector Machine. The proposed model provides encouraging results with an accuracy value of 94.3%, precision of 92.5%, recall of 97.8%, and an F1

score of 91.8%. It shows that deep-learning, particularly CNNs, holds better potential for detecting and preventing brute-forcing users without altering time-honored techniques. Additionally, the study emphasizes the need for detection mechanisms to keep up with the trends of sophisticated attacks.

Moreover, several studies have combined the features of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) to tackle the problems of brute force attack detection. For example, the authors in [3] developed an Intrusion Detection System (IDS) model that combined CNN and LSTM models enhanced with feature selection techniques and synthetic minority over-sampling technique (SMOTE) for addressing class imbalance. The approach resulted in improved detection accuracy over several network attacks, including brute force attacks. Another research paper [4] has presented a hybrid model based on CNN and LSTM which performed well for detecting network intrusion attacks, particularly brute force attacks. The model uses CNN capabilities in extracting features as well as the abilities of LSTM in understanding and learning from the time dimension of input data, which is very important in understanding and detecting attack behavior patterns within time difference.

Yet another study on IoT security [5] proposed a hybrid CNN-LSTM approach for intrusion detection in general, where brute-forcing attacks were detected through network traffic patterns. This model significantly outperformed the conventional techniques, showing a clear sense of adaptability to the evolving nature of cyber threats, as it uses both CNN and LSTM.

The strength of this combination of methods for brute-force attack detection, employing the CNNs for feature extraction and LSTMs for dynamic time capture of pattern recognition in network traffic, signals a good future for computerized solutions in IoT networks that will be used for cybersecurity.

III. Proposed approach:

This part describes the combined architecture of CNN and LSTM, and also the performance comparison against CNN alone and also with LSTM alone. The data collected for training and validation is the HTTPS Brute-force dataset from Zenodo [6] , which consists of raw network flow data as well as aggregated features.

1. Dataset Description

The HTTPS Brute-force dataset, which is retrieved from Zenodo [6], provides a collection of network flow data that is labeled with a distinction of "attack" and "benign" traffic. This dataset is an indispensable instrument for the study of network behavior and the identification of the patterns of brute force attacks.

To examine the necessary key columns, we performed the following:

- SRC_IP and DST_IP: They represent the IP addresses of the source and the destination, allowing the detection of endpoints of communication.
- SRC_PORT and DST_PORT: These, on the other hand, reveal the source and destination ports that are very important for identifying the services that are under threats.
- DURATION: Is an entity recording the time of the connection, and thus being the basic element of length by which we can measure long or suspicious activities that have an impact.

- BYTES and PACKETS: Account for the total amount of data and the number of packets transferred, respectively, on a binary communication layer, hence giving an estimation about the amount of communication.
- ROUNDTRIPS: It counts up the total number of round trips the vehicle has made, which in turn enables us to catch the non-standard configurations of the vehicle's behavior.
- REQUEST_SIZES_MEDIAN and RESPONSE_SIZES_STD: They contain mean data sizes of requests and responses that support profiling normal and abnormal communication patterns.
- CLASS: A target variable, providing one-hot encoded labels for either "attack" or "benign" attack, is the dependent variable in the supervised classification task.

These columns have been chosen for reasons such as their usefulness in identifying brute force attacks based on the analysis of the network behavior. The dataset was made the research base through pre-processing, computing features along with standardization, and served as a training and testing tool for our model which is a hybrid of LSTM and CNN.

2. Hybrid CNN + LSTM Model:

This hybrid architecture with CNN LSTMs is going to combine the best features of Convolutional Neural Networks (CNN) for local feature extraction and Long Short-Term Memory (LSTM) networks to capture the temporal dependencies. Thus, this model structure shows high promise for handling time-series data such as network traffic logs.

Hyperparameter Tuning:

Using KerasTuner, we conducted a hyperparameter tuning process to optimize the performance of the hybrid CNN + LSTM model.

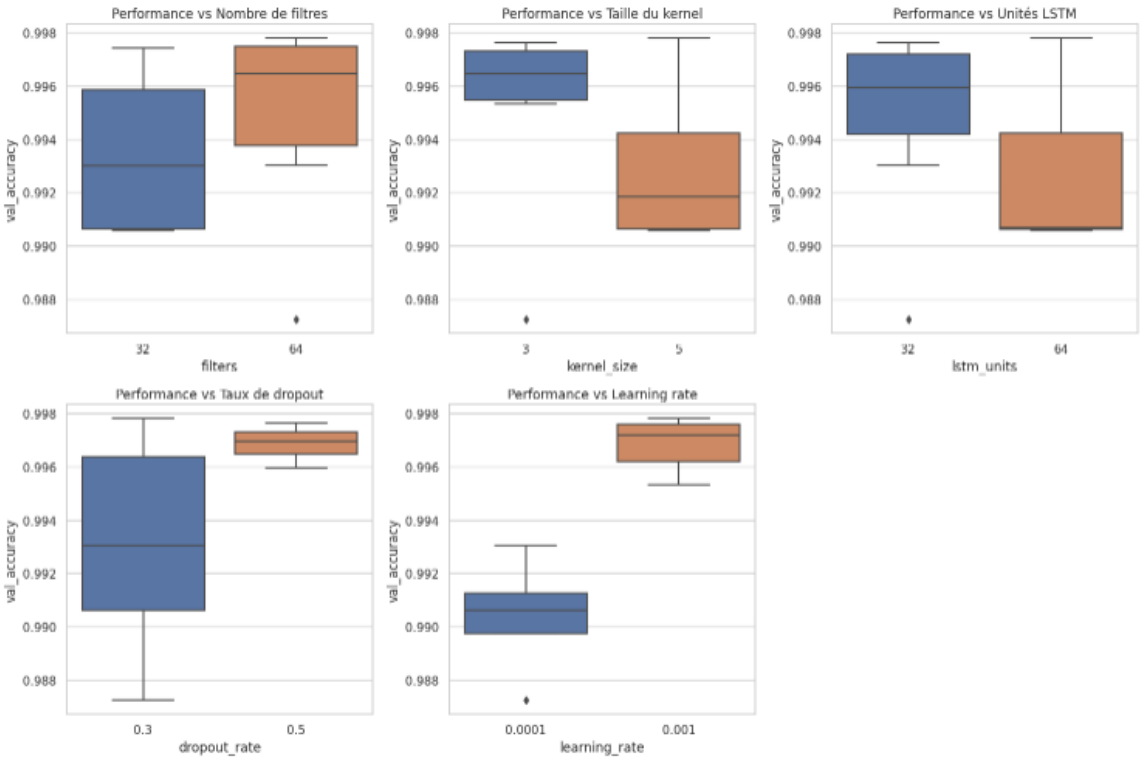

Figure 1 : Tunning Parameters Results

The best hyperparameters after tuning are:

CNN Layer: 64 filters with a kernel size of 5.
Pooling Layer: Pool size of 3.
LSTM Layer: 64 units.
Dense Layer: 64 units.
Dropout: 30% rate.
Optimizer: Adam with a learning rate of 0.001.
Batch Size &: A batch size of 32 and 10 epochs.

The entire architecture is shown as follows:

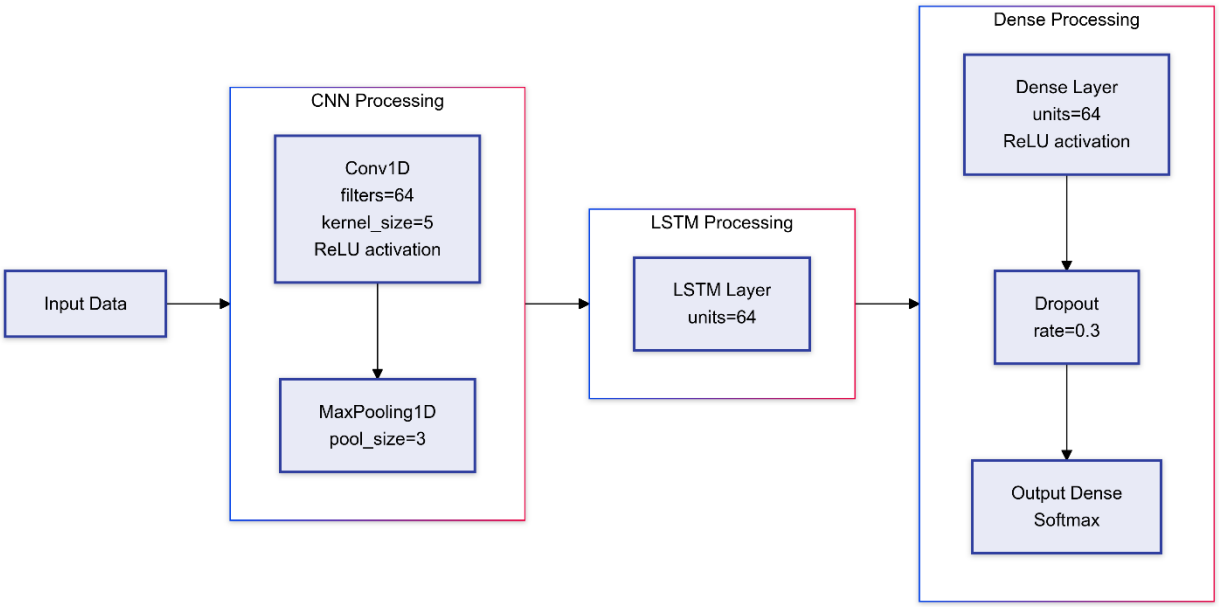

Figure 2 : Diagram Approach

Model Features

Feature standardization: To ensure that all input features are on similar ranges letting the model learn some more efficiently by standardizing the data using StandardScaler.

Sequence Formation: The data is divided into sequences of equal lengths called timesteps and given to feed into the CNN and LSTM layers before being processed.

CNN Layer: Conv1D Layer having 64 filters and kernel size 3 extracts local-level features from the sequences as necessary for identifying complex attack patterns in the network traffic data, the most significant of which follow it MaxPooling1D, as a result, dimensionality reduction.

LSTM Layer: The long-term dependencies depict the presence of LSTM regarding language sequences since time-series data such as network traffic logs allow for such flexibility in associating consecutive data points. The LSTM layer takes up such input to form a compressed representation of its input data.

Final Classification Layer: The output from the LSTM layer is forwarded to the Dense layer with ReLU activation, which contains a set of 128 units. Additionally, a 50% Dropout layer is incorporated to discourage the model from overfitting. Finally, a Dense layer with softmax activation to output classification results segregating data as "attack" or "benign."

3. Methodological Transparency:

We actually looked into the possibility of having a hybrid CNN+BERT model for better feature extraction and sequence learning. Unfortunately, due to some resource constraints, like computational power, we could not successfully implement this hybrid architecture. In addition, we really wanted to leverage the capabilities of BERT to represent texts, but all the required resources to train and optimize such a demanding model were not available. Therefore, we opted for the more practical CNN+LSTM hybrid architecture which gave us good results within the resource threat.

4. CNN Model:

The CNN model is trained using the same training sets, but applies only convolutional models that can be used to automatically extract features. It captures local patterns in the data but lacks an understanding of temporal dependencies, rendering it unsuitable for sequential data.

5. LSTM Model:

It only depends on capturing the temporal dependencies of the data. It would capture better sequences in the data but couldn't extract local patterns like CNN.

IV. Investigation and Discussion

1. Results of CNN + LSTM

The hybrid CNN-LSTM architecture was trained and tested on the HTTPS Brute-force dataset. This architecture nicely marries the pattern recognition abilities of CNN with the sequential analysis strength of LSTM, hence, making it an excellent choice for brute force attack detection.

Performance metrics: Accuracy: 99.79%, Loss: 0.0132

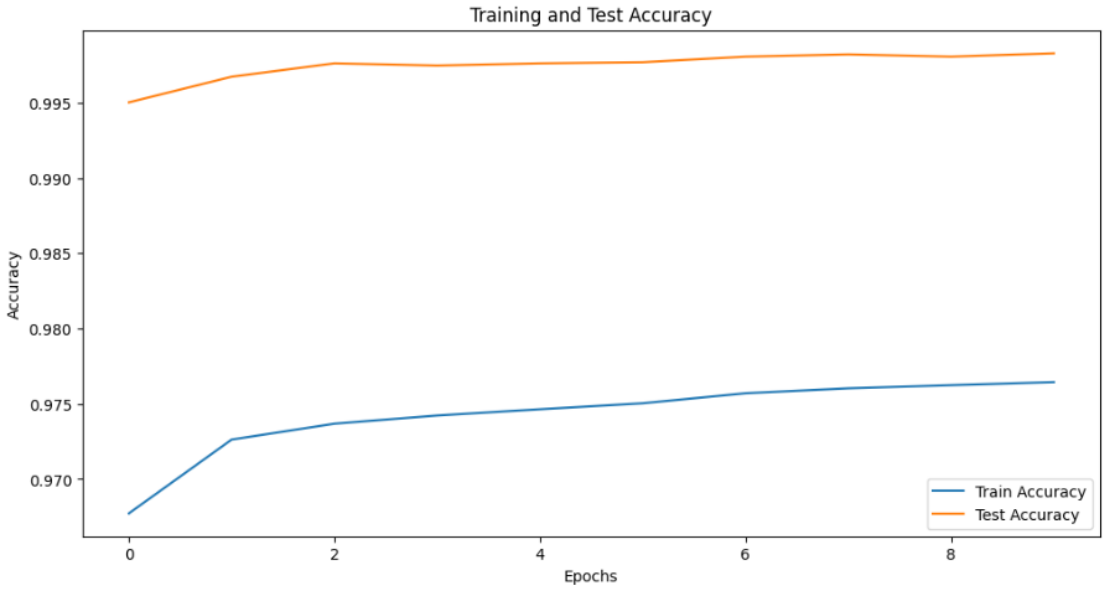

Figure 3: Training and test Accuracy

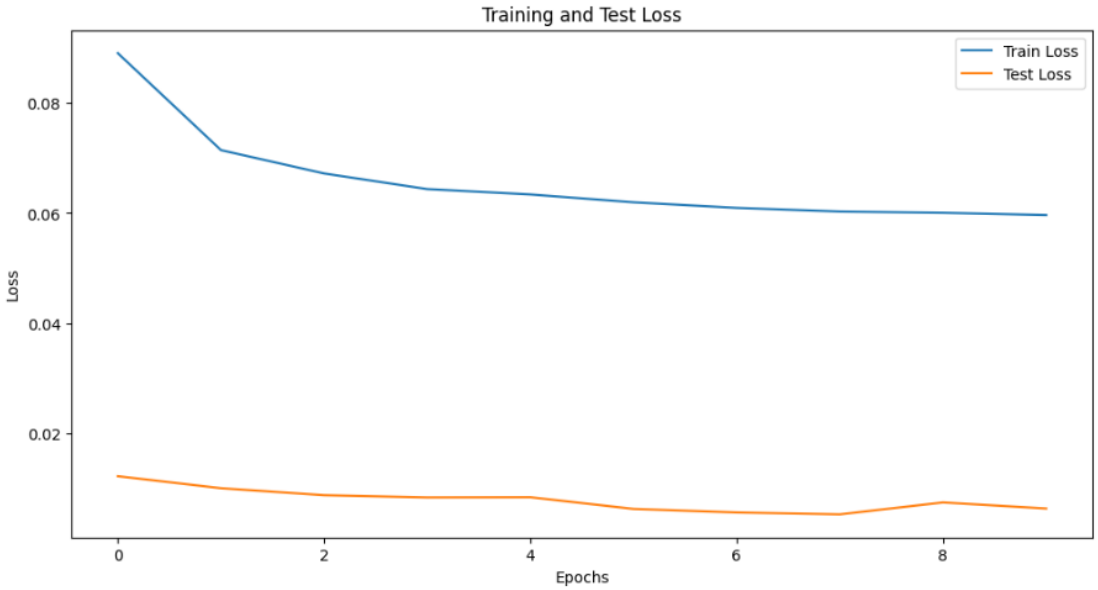

Figure 4: Training and test Loss

Classification Report:

Class	Precision	Recall	F1-Score	Support
Benign	1.00	1.00	1.00	11,150
Attack	0.99	1.00	0.99	2,344

Table1: Classification Report of classification with CNN-LSTM

Confusion Matrix:

	Predicted: Attack	Predicted: Benign
Actual: Attack	11,130	20
Actual: Benign	8	2,336

Table2: Confusion Matrix of classification with CNN-LSTM

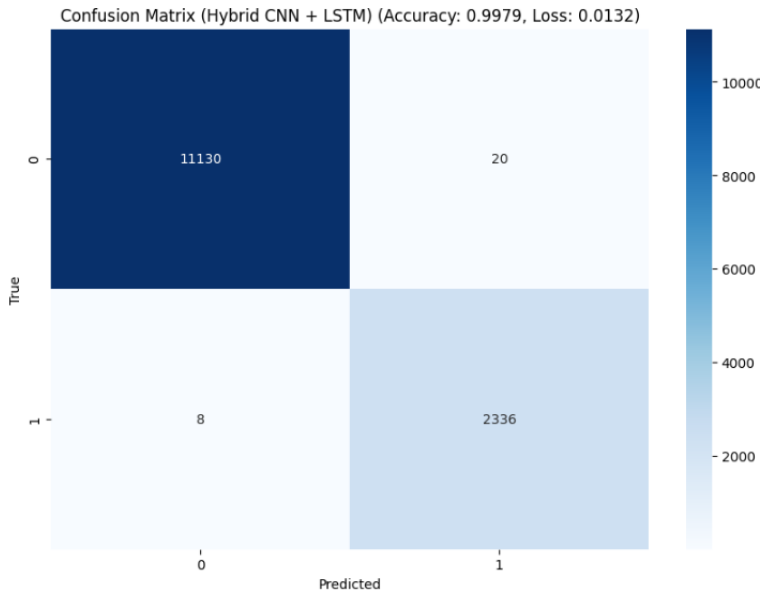

Figure 5: Confusion Matrix

2. Comparison with CNN and LSTM Alone:

Model	Accuracy	Loss
CNN	97.66%	0.0583
LSTM	98.68%	0.0342
Hybrid CNN+LSTM	99.79%	0.0132

Table 3: Comparison of Accuracy and Loss for CNN, LSTM, and the Hybrid Model

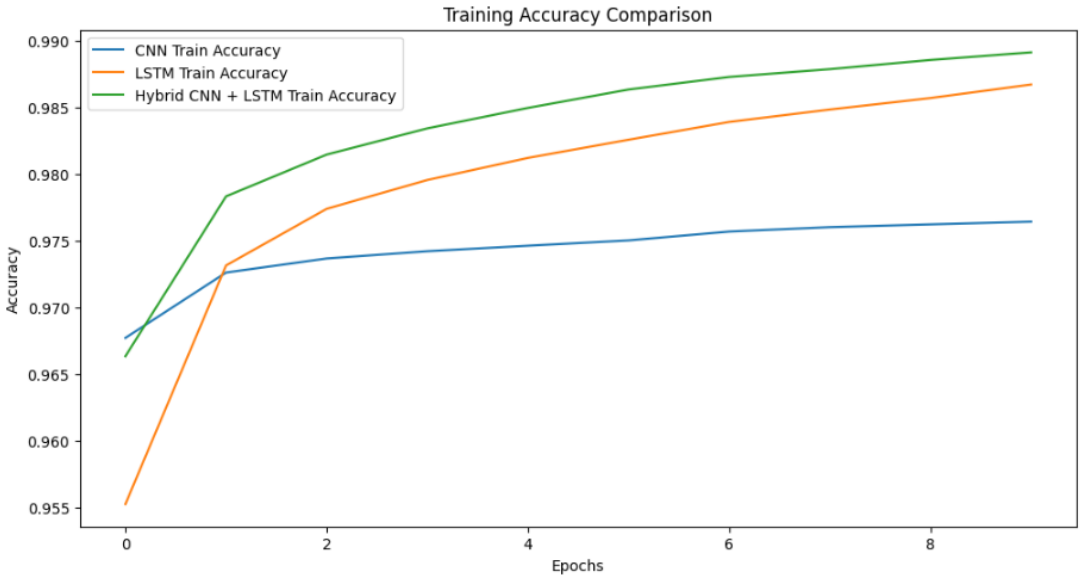

Figure 6: Training Accuracy Comparison

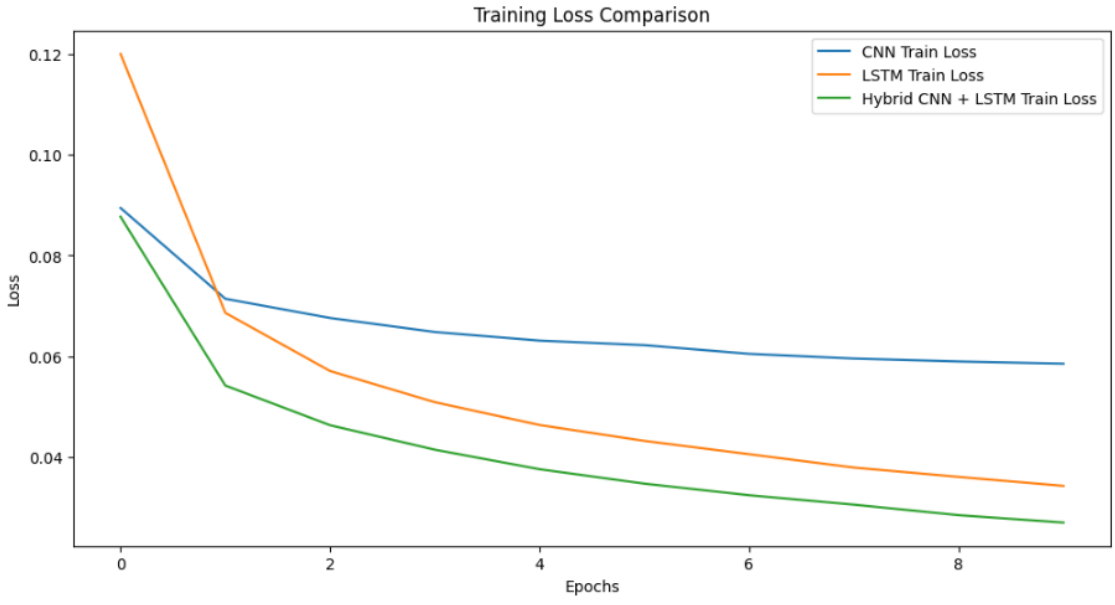

Figure 7: Training Loss Comparison

The hybrid model CNN + LSTM has more strength as they marry each other's complementary features. CNN has an edge over it in extracting and localizing the features from the network flow data, like packet sizes, TCP flags, and inter-packet times, which are so critical while

detecting attack patterns. The only drawback of CNN is that it does not give good features from long-term dependencies in the sequential data.

LSTM is designed to capture the long-dependent and temporal patterns while it is being effective enough analyzing time-series data like the sequence of packets in network traffic. LSTM does not perform with quite as good efficiency, however, in extracting local features.

The combination of local feature extraction by CNN and recognition of a sequence pattern over time by LSTM will therefore have the complementary benefits of both models and make the system more robust and more accurate in detecting brute force attack in HTTPS traffic.

3. Comparison with Other Research Results:

Our hybrid CNN-LSTM architecture attains 99.79% performance accuracy in brute force attack detection. To ascertain the empirical validity of our approach, let us look into other recent works focused on direct brute force attack detection.

Wanjau et al. (2021) [2] did a study focusing on SSH-brute-force attack detection while using a CNN based approach. It achieved 94.3% accuracy, 92.5% precision, and 97.8% recall. Our hybrid model, on the other hand, produced values that were considerably better:

5.49% more accurate (99.79% vs 94.3%)

7.5% more precise for attack detection (99% vs 92.5%)

and Recall rates comparable at 100% vs 97.8%

These improvements are due to the capturing of non-spatial dimension features through the CNN, as well as temporal patterns through the LSTM layers in the model.

The focus of Otoom et al. (2023) [1] is solely the use of brute force attacks on IoT networks by deep learning methods. The work utilized the MQTT-IoT-IDS2020 dataset and achieved accuracies of: 99.6% bi-flow features, 99.7% uni-flow features

And though the results appear close to that of our model, our hybrid method reflects a marginal improvement of 0.09% in accuracy, showing the strength of coupling CNN and LSTM architectures.

The performance metrics across these brute force attacks detection studies are summarized in the following table:

Study	Approach	Accuracy	Precision	Recall	Dataset Type
OurSudy	Hybrid CNN-LSTM	99.79%	99%	100%	HTTPS Brute-force
Wanjau et al. (2021)	CNN	94.3%	92.5%	97.8%	SSH Traffic
Otoom et al. (2023)	Deep Learning	99.7%	Not reported	Not reported	IoT Network Traffic

Table3: Comparison with other Research Results

The reasons why the model showed better quality performance in detecting brute force attacks are:

The complementary advantages of CNN and LSTM: CNN extracts local patterns from network flow data, whereas LSTM implies dependencies in time scales of attack sequences.

The optimized hyperparameters through KerasTuner, the proper optimization for preprocessing of network flows, and the balanced architecture of the model to prevent overfitting made it possible to achieve.

These comparative experimental results showed that the hybrid approach achieves state-of-the-art performance in the specific case of brute force attack detection. All these considerations can be summarized in the assertion that the synergistic combination of features extracted from CNN and their temporal patterns identified through LSTM "makes a stronger case than a single model as a better alternative for automated identification of brute force attacks within network traffic."

IV. Conclusion and Perspective

This paper comes up with a hybrid way to combine Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to detect brute force attacks in cybersecurity. The model has proved to perform far better than conventional approaches and also versus CNN and LSTM taken separately. Accuracy of 99.79 percent, with minimum loss, was obtained by the hybrid architecture, which leverages local features and temporal dependencies, thus outperforming earlier studies in proving how effective are the combined deep learning approaches in the field of cybersecurity applications.

It is shown that the hybrid CNN-LSTM model has clearly demonstrated a capacity to detect brute force attacks even in HTTPS traffic; however, on top of even these sophisticated and evolving attack patterns, it has continued to have strong detection fidelity. It is further evident from comparisons to existing literature that the approach yields quite significant enhancements on accuracy, precision, and recall, which affirms its potential for practical cybersecurity applications.

Perspective: Future extensions of this model may consider adapting the model to specific network attacks and fine-tuning it for more real-time data input, and implementation with automated defense systems to further increase its security factors in IoT and other vital network infrastructures. The model can be tested on other attack data, including more extensive attack databases, diverse and larger-scale attack scenarios to study its adaptability and scalability to different environments. Further endeavors could be taken through other architectures such as BERT combined with CNN in evaluating their performance in this field. The BERT's contextual language processing strength and feature extraction capabilities of CNN could also improve the model's solidity against complex attack patterns. The advancement in transfer learning and unsupervised learning systems would also open up doors to the improvement of this model even in case of inadequate labeled data.

V. References:

[1] Ahmed Fawzi Otoom*, Wafa' Eleisah, Emad E. Abdallah (2023). Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks.

[2] Stephen Kahara Wanjau, Geoffrey Mariga Wambugu, Gabriel Ndung'u Kamau (2021). SSH-Brute Force Attack Detection Model based on Deep Learning.

[3] Kuljeet Singh, Amit Mahajan and Vibhakar Mansotra. Hybrid CNN-LSTM Model Combined with Feature Selection and SMOTE for Detection of Network Attacks, 2024.

[4] Asmaa Halbouni, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Murad Halbouni; Mira Kartiwi, Robiah Ahmad. CNN-LSTM Hybrid Deep Neural Network for Network Intrusion Detection System.

[5] Afrah Gueriani, Hamza Kheddar, Ahmed Cherif Mazari. Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems,2024.

[6] Luxembourg, J., Hynek, K., & Cejka, T. (2020). HTTPS Brute-force dataset with extended network flows [Data set]. Zenodo.