Efficient Complex Event Processing in Intrusion Detection System using CNN-BiLSTM model

Aditya Kumar Singh[1*], Sakshi Chauhan[2], Dr. S. Sandosh[3]

[1*,2,3] Vellore Institute of Technology, Chennai, India

adityakumar.singh2020a@vitstudent.ac.in[1*] sakshi.chauhan2020@vitstudent.ac.in[2]
sandosh.s@vitstudent.ac.in[3]

Abstract. Intrusion detection systems (IDSs) are essential for protecting computer networks from malicious attacks.As digital guardians, intrusion detection systems (IDSs) must defend computer networks against malicious attacks.On the other hand, as opposed to using the normal signature of known attacks,conventional IDS fails in handling the unusual or unidentified attacks.Development of an innovative CNN-BiLSTM hybrid model based on real time intrusion detection by employing CEP (Complex Event Processing) is the new method presented in this paper. Think about it as a skillful and mysterious digital detective with the capability to spot both the known network attacks plus the ones that are new and yet to be discovered.It has the capacity to comprehend both the broad picture and the finest details of the network traffic, in a similar way to how a highly proficient detective might take the account of the where and when of an attack into consideration.This idea was developed by basing it on the CIC-IDS2017 dataset. This dataset can successfully identify multiple categories of attacks such as those that traditional methods of attack detection might have missed. The entries in the CEP will consist of the main information about these attacks, for instance, the source and the destination, and the time of the occurrence.This strategy is distinct in the sense of maintaining an unpredictable number of events or threats happening with nearly real-time reliability.Consequently, under this mixed strategy the CEP can be an effective tool for real-time intrusion detection.Furthermore, the proposed solution was compared with the Random Forest model as well.The Random Forest model can be considered to be superior to the other model, because it gave us higher accuracy in correctly recognizing attacks.

Keywords: Intrusion Detection System(IDSs), Complex Event Processing(CEP), Temporal characteristics, Convolutional neural network (CNN), Bidirectional long short-term memory (BiLSTM).

1 Introduction

As the digital world becomes increasingly complex, the security of networks of computers and keeping the intrusions unauthorised is the most important factor nowadays. Due to continuous upgrading of hackers characterised by unusual ways of doing things in response to technical developments IDSs become prone to misleading. Organisations hold a poor state of security since these age-old tools can hardly fit in the current threat landscape, and identifying new and confounding attack patterns is among the hardest things to achieve. Equipping computer networks with authorisation in order to prevent unauthorised access is one of the security prerequisites of the present digital environment [12]. This study analyses the viability of applying a CNN-BiLSTM hybrid model, among the many other intrusion detection techniques, for real-time intrusion detection using Complex Event Processing (CEP),delivering the requirement for more sophisticated techniques.Internet crime such as hacking, which is becoming more complicated every day, concerns not only stealing data but also intimidation of the whole state because of the possible consequences, which makes the issue more serious. The modern types of attack adapt the strategies and bypass the conventional application of intrusion detection systems (IDSs) that have been put up with their detection foundation to traditional signatures techniques that helps to identify known attack patterns [8]. The paper shows that an innovative deep-learning method may be achieved by simply combining two most powerful technologies of CNNs and BiLSTM networks. The CNN-BiLSTM hybrid model proposed in this work is similar to a smart cyber-sleuth whose mission is to detect malicious patterns and suddenly react in time as AI together with CEP. Predicting the network attacks by hand is feasible by the application of the spatial and temporal features present in network traffic data. The above placement highlights the complexity of the solution adopted and its ability to overcome the setbacks of the existing IDS.Complex Event Processing being its effective method of keeping records of distinctive factors such as locations, timestamps of wrongful action, IP addresses of destination/source etc. over time. Such information is being picked up as it is and put into the storage as the subject of the further research and analysis. Another impressive part about this methodology is that it is able to cope with a large number of complicated network assaults happening all at the same time. This is an important property during an environment that is dangerously changing and that constantly lives by the code of coordinated hacker activity basing itself on various exploitation techniques. By combining these two technologies together, the novel IDS addresses the major conceptual gap of traditional intrusion detection systems that cannot identify concurrent attacks; therefore, the CEP with the CNN-BiLSTM model plays an important role in modern cybersecurity practice. In addition, the Random Forest model and the CNN-BiLSTM hybrid model which are designed to solve the classification problems compared with each other in this study. The output layer of the model has to be modified correspondingly, so it only outputs two bits for explanation. This is a must to fairly compare the approach with the current one. By all evaluation measures, the Random Forest model should be considered the best model among them because it has greater accuracy, precision, recall, and F1 score.

2 CIC-IDS dataset

The research paper strives to identify intrusion detection techniques that are assessed by comparing them through the CIC-IDS2017 dataset which serves as a standard benchmark about the challenges faced by anomaly-based techniques [1]. Different from the datasets that are limited by the out-of-date data from the year of 1998, this latest and more relevant dataset of 2016 is advantageous [16]. The broadness of the data, network connections and protocols of the network threats that are indeed the part of the dataset CIC-IDS2017 are many. The utmost interest of CIC-IDS2017 in the investigation of the real-world cyber attacks is that it contains user profiles as well as plenty of information about the network infrastructure and data from 12 PCs in the network of the victim that make the dataset more diverse. Additionally, it further makes it possible to measure intrusion detection techniques since the dataset unambiguously distinguishes hacker and classic attacks. Recall that a CIC-IDS2017 dataset is employed as an important input option in the test of intrusion detection in this research. The purpose of the study is to demonstrate the quality of intrusion detection in actions about different attack patterns including those, which can be avoided by typical detective measures [3].

3 Motivation

This research is in connection with the advanced networked systems to be attributed to complex and continuously sophisticated cyber-attacks. Although the efficiency of IDSs in detecting malicious network attacks is unquestionable, these systems often fail when they are supposed to combat newly developing types of attacks. The CNN-BiLSTM hybrid model enriched with the Complex Event Processing (CEP) concept provides an effective solution to the mentioned critical issue regarding this type of detection [4]. The importance is in empowering this digital umbrella with the ability to discover a recently described form of the malware next to an array of known network attack signs. This article will innovate in uprooting a multilayered digital detective that can recognise the variation in network traffic the same way a trained investigation expert does. This type of decision-making approach handles multiple risks simultaneously that may be hard to foresee and be, therefore, well suited for dealing with unidentified mishaps compared to usual systems. This is done through experimenting with the CIC-IDS2017 dataset which led the network to successfully detect many different manifestations of high-risk attack patterns, exceeding the ability of conventional security mechanisms. This system is developed yet further by the incorporation of CEP [3] which enables the provision of additional context by way of the describing of the origin and destination as well as timing of a detected attack. Through this applying different methods the hybrid technique can step off the existing security models pattern and represent an extremely efficient on time possible intrusion detection system . In a comparison plot, the proposed hybrid CNN-BiLSTM model came second, scoring higher in terms of detection of and mitigation of possible attacks [11].

4 Related Works

Deep learning algorithms have emerged and given a great change to the intrusion detection scene. The fusion of CNN and BiLSTM networks, working in parallel to enhance intrusion detection precision, has, currently, been identified as a powerful solution [20]. The researchers have explored the applicability of CNN-BiLSTM hybrid models in enhancing the accuracy of the real-time intrusion detection systems. These models are very successful in elucidating the convoluted temporal and spatial correlations inherent in traffic data - which helps in finding both the known and the unknown patterns of the attacks. The employment of Complex Event Processing technology (CEP) is currently a popular approach that helps to observe the pattern of network events. This has bearing especially on real-time event analysis and anomaly detection in the instance of cybersecurity. Cyber threats are ever-evolving, which means that deep learning and CEP are promising approaches. Researchers have been focusing on overcoming scalability and resource efficiency concerns to successfully process massive network data without compromising the precision of the detection model. The research also offers a comparison of two models that were created for binary classification: the CNN-BiLSTM hybrid model as well as the Random Forest model. The denser layer of the neural network model converged to predict two classes only both lowers the risk of bias. The metrics evaluation has presented that the Random Forest model dominates with higher accuracy, precision, sensor recall and F1 score and therefore the detection solution becomes reliable. This research has a strong impact on the broadening field of intrusion detection systems by answering the existing challenge of the need to increase the accuracy and the agility of the security of the network.

4.1 Deep Learning based IDSs

Deep learning embraces convolution neural networks (CNNs), as well as Bidirectional Long Short-Term Memory (LSTM) networks. Currently, these technologies have become a part of the prototype Intrusion Detection Systems (IDSs) [7] . Those methods completed their work for the purposes of revealing well-known negative signatures to the system, as well as those which were not identified as attack patterns (Tahir, et al. 2015) [15]. CNNs can utilise the advantages of the ability to auto-learn features and feed hierarchies from the raw data into ultimately carrying out identification tasks of images very well. Besides, CNNs are important in understanding spatial features of identifications from traffic data which may be adapted to protect systems and networks from penetration attempts.

4.2 Examining the Challenges of Real-Time Intrusion Detection

The precision and the fast processing of real-time intrusion detection in high-accuracy are the challenges which are very specific. Many researchers have proved that designing models and methods to incorporate these criterias is the most feasible option to this challenge and can as well identify both the concealed and known attacks (Hamed T et al., 2017) [10]. Pertinent to react timely to security incidents, quick-response detection systems must combine operation at the low level of latency. The breaking speed of network traffic makes the detection of intrusions hard within a given timeslot, hence delays, no matter how small, make a significant difference. The low-latency of processing becomes complicated especially in case massive data volumes are concerned. Yet another obstacle: Modern networks generate so much data. Conventional intrusion detection systems sometimes face serious troubles because of their poor ability to analyse large traffic volumes in real-time.

4.3 Challenges of Intrusion Detection System in Cloud Computing

For the purpose of real-time intrusion detection in the Cloud Computing system, A.Dey al. (2018) [19] propose convolutional neural network-bidirectional Long Short Term Memory (CNN-BiLSTM) hybrid model. The model incorporates a bidirectional Long Short Term Memory to retrieve temporal intelligence from network traffic data and a CNN to yield spatial aspects. The model is tested on the NSL-KDD dataset and is proved to be effective in notifying both types of intrusions, identified and the unknown ones. From the spatial features using the CNN algorithm, it retrieves the network traffic data.

4.4 CEP-Enhanced CNN-BiLSTM Hybrid Model for Comprehensive Real-Time Intrusion Detection

In order to detect real-time intrusion in a cloud based system, Javaid A and e.t. al. propose the use of a CNN-BiLSTM hybrid model (2016) [7]. The model uses a Bidirectional End-to-end Long Short-Term Memory layer to extract the temporal information of the network traffic data and a CNN layer to extract the spatial features. The model is run on the NSL-KDD data set and is subsequently found to be effective in detecting known as well as undiscovered incursions. From the network traffic information, CNN algorithm provides required spatial features. This is essential since geographical attributes can be used to differentiate among varieties of attacks, for instance port scans and attacks aimed at accomplishing denial of service. By utilising a Temporal LSTM network to extract the temporal information of the traffic data, it represents the traffic network. So it has been trained on network traffic data which consists of both legitimate and malicious traffic patterns, it can recognize [16].

5 Proposed Methodology

5.1 Data collection

The CIC-IDS2017 dataset provides a wide range of network traffic data including normal and malicious activity [14] . It is divided into two parts: training set and test set.

5.2 Exploratory data analysis

A vital part of the research lies in preprocessing the CIC-IDS2017 dataset so as to generate clean and normalised data for extracting useful details. Dimensionality reduction, handling missing data, and performing exploratory data analysis is completed to give a better understanding of the dataset, as well as to point out anomalies [13]. The steps include importing the dataset, splitting it into a matrix of features and labels, and then finding out missing values.

5.3 Feature extraction

The imperative stage to boost the performance of the CNN-BiLSTM is to carry out feature engineering. To further the model's effectiveness, other features are extracted from the CIC-IDS2017 dataset and taken into account while the model is being trained. However, multiple parameters in the feature set taken into account like packet size, type and both source and destination IP addresses improve the accuracy of traffic pattern spotting and inconsistency detection much more in the model [5].

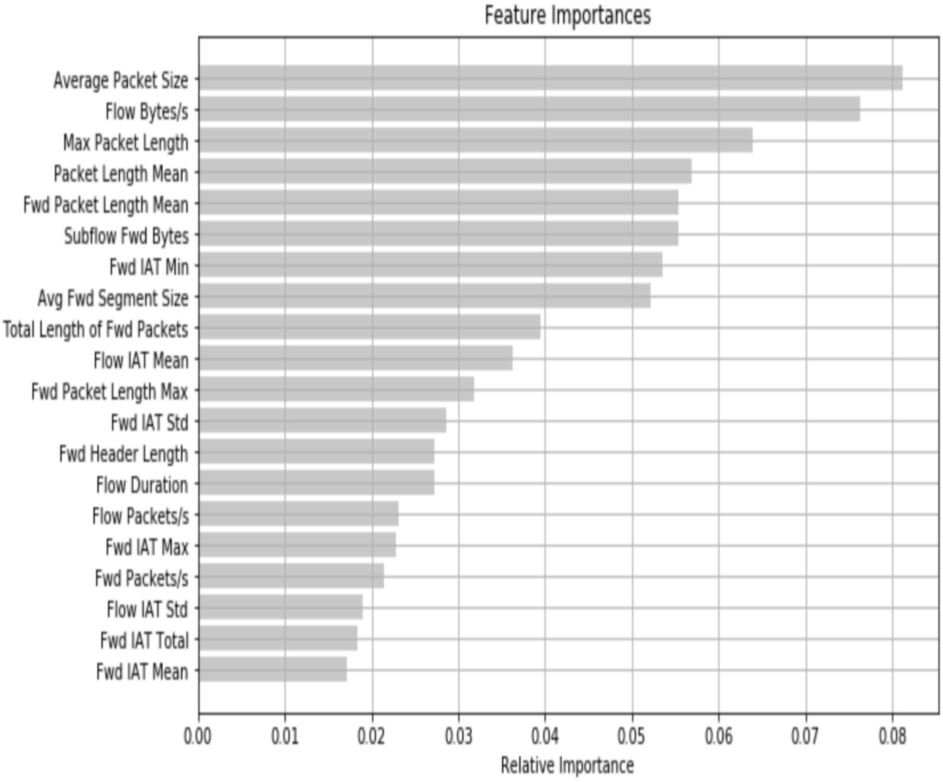


Fig. 1. Feature Importance

5.4 Data normalisation

Data normalisation techniques are used as preprocessing and enhancement methods in intrusion detection models. Prejudice to be avoided, feature vectors go through Min-Max scaling and missing values are reduced using mean imputation. Temporal normalisation renders the alignment of timestamps beneficial since it is easier to reveal the temporal dependencies [2]. Implementing such steps assures the fact that CNN-BiLSTM model stays at its top-notched performance because of the consistency CIC-IDS2017 dataset is promoted.

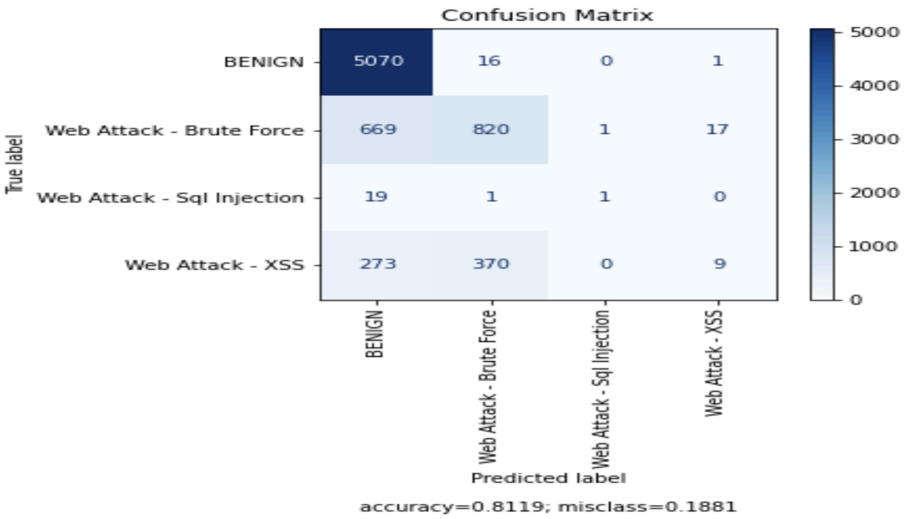
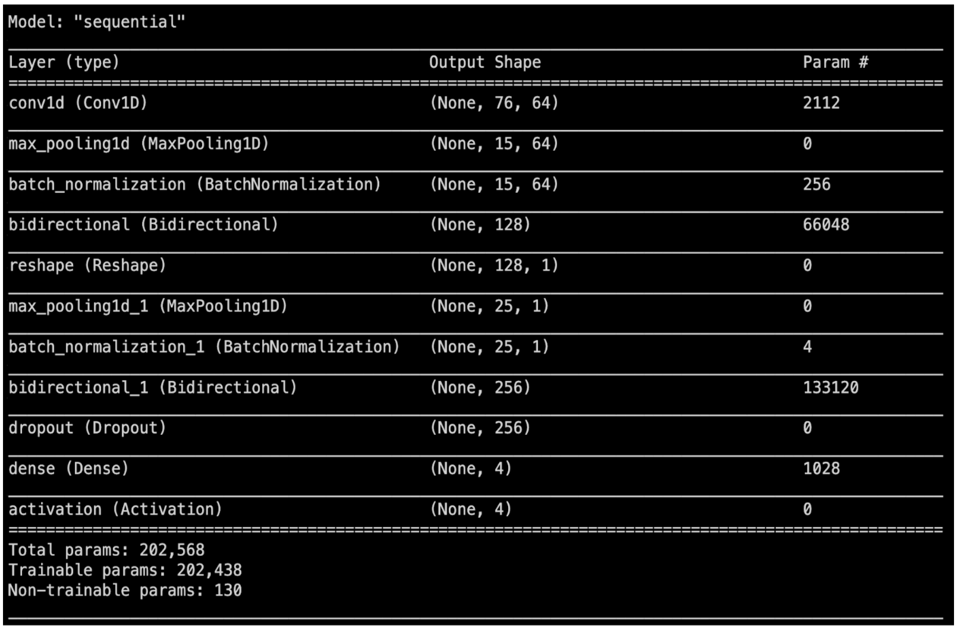


Fig. 2. Confusion matrix showing intrusion detection accuracy for different types of network attacks.

5.5 CNN-BiLSTM version training

The CNN-BiLSTM model is trained with pre-processed and normalised data. Convolutional layers for hiding spatial dependencies and BiLSTM layers for handling time factors are combined in this specially developed intrusion detection model [9].



```
Model: "sequential"
_________________________________________________________________________________________________
Layer (type)                                Output Shape                        Param #
=================================================================================================
conv1d (Conv1D)                             (None, 76, 64)                      2112
_________________________________________________________________________________________________
max_pooling1d (MaxPooling1D)                (None, 15, 64)                      0
_________________________________________________________________________________________________
batch_normalization (BatchNormalization)    (None, 15, 64)                      256
_________________________________________________________________________________________________
bidirectional (Bidirectional)               (None, 128)                         66048
_________________________________________________________________________________________________
reshape (Reshape)                           (None, 128, 1)                      0
_________________________________________________________________________________________________
max_pooling1d_1 (MaxPooling1D)              (None, 25, 1)                       0
_________________________________________________________________________________________________
batch_normalization_1 (BatchNormalization)  (None, 25, 1)                       4
_________________________________________________________________________________________________
bidirectional_1 (Bidirectional)             (None, 256)                         133120
_________________________________________________________________________________________________
dropout (Dropout)                           (None, 256)                         0
_________________________________________________________________________________________________
dense (Dense)                               (None, 4)                           1028
_________________________________________________________________________________________________
activation (Activation)                     (None, 4)                           0
=================================================================================================
Total params: 202,568
Trainable params: 202,438
Non-trainable params: 130
_________________________________________________________________________________________________
```

Fig. 3. Model Information

5.6 CNN-BiLSTM version training

Complex event processing is used to implement the CNN-BiLSTM model in real time [12]. CEP real-time traffic monitoring provides information about suspicious behaviour.

5.7 Comparison of CNN-BiLSTM and random forest model

The results of the models were evaluated by comparing the CNN-BiLSTM hybrid model with the Random Forest model, which is commonly used for the binary classification problem. The last layer of the neural network model was refactored in such a way that it could only output two classes to keep the fairness of the comparison [17]. The CNN-BiLSTM hybrid model combined with Complex Event Processing (CEP) has shown itself to be a competent intrusion detection solution, although the Random Forest model had a better accuracy, precision, recall, and F1 score. The reason for this supremacy requires some scrutiny, which illustrates the special power of CNN-BiLSTM model mainly in terms of intrusion detection.

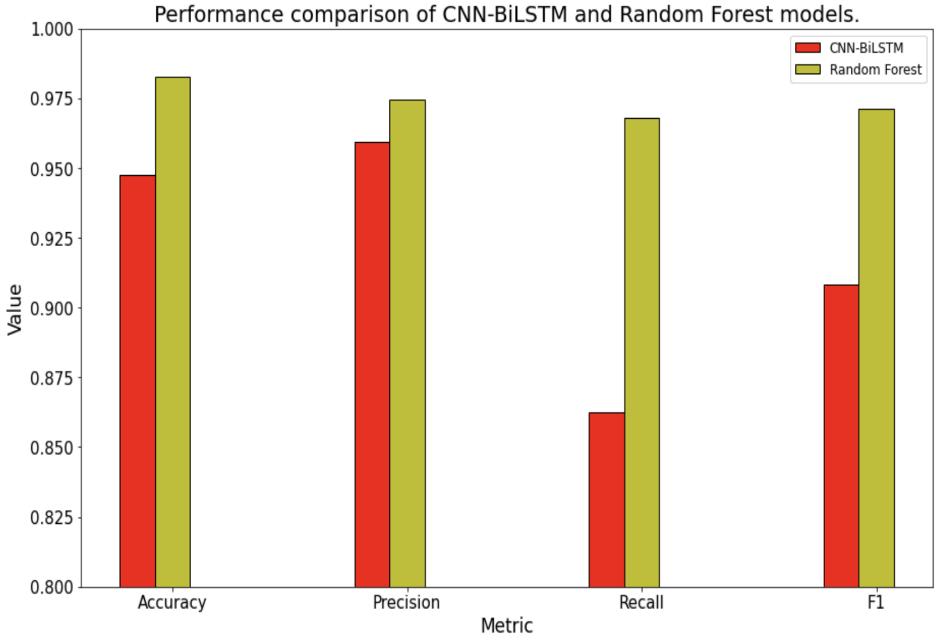


Fig. 4. Comparison of CNN-BiLSTM and random forest model

5.8 Intrusion alert analysis and response mechanism

Complex Event Processing (CEP) significantly improves decision-making and processing in real-time. The lower false alarms rate is possible by a rapid hybrid model's intrusion prediction [15]. Dynamic retraining, which is implemented actively to adjust to changing network traffic patterns, has been employed to increase effectiveness against every new attack. Alerts made by CEP are reviewed by network security people in order to recognize the threat source, understand the attack's kind, and take right actions to reduce the risks.

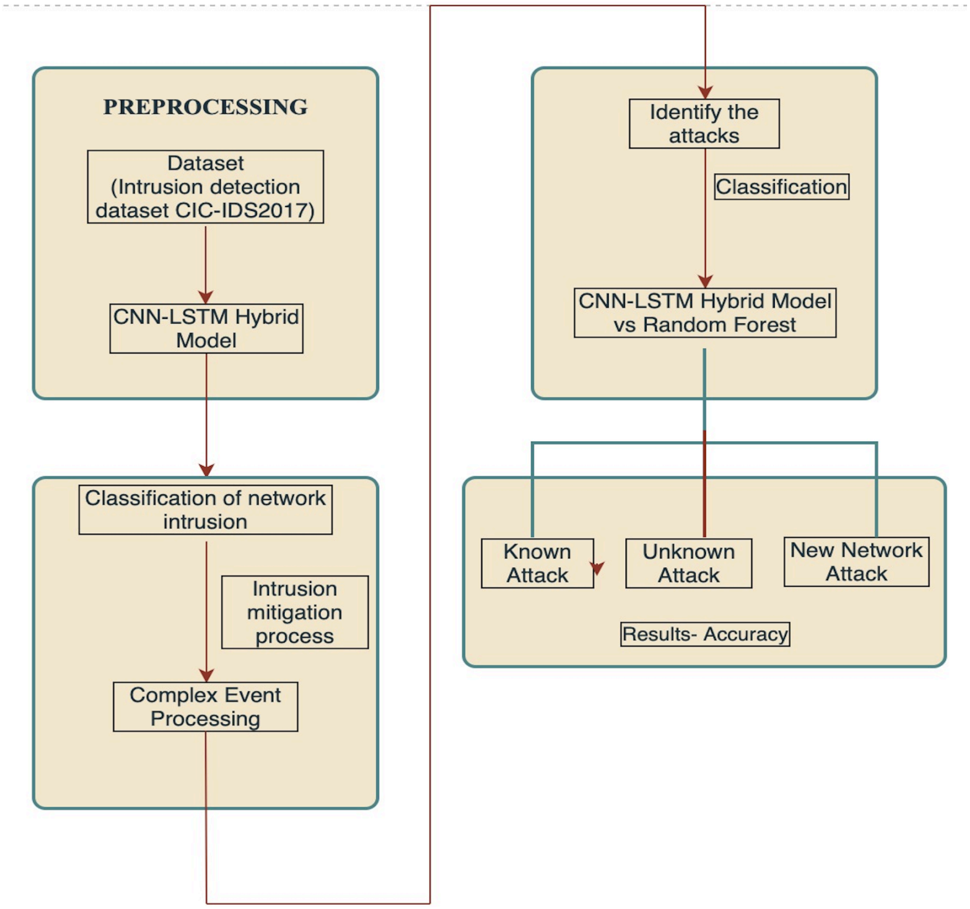


Fig. 5. System Architecture

6 Classification

The research relies on applying the machine learning models towards the categorization. The primary target of this study is the Random Forest model, as well as, the hybrid CNN-BiLSTM architecture that are designed for real-time intrusion detection through the use of Complex Event Processing (CEP). The method involves the discernment of some features from CIC-IDS2017 dataset, and features of different types of network traffic data comprise it [6]. The consequent methods will use the elements as a base of their operation. For the sake of discovering grouping of traffic in network data over a long time, the CNN-BiLSTM hybrid model utilises CNNs as feature extractors and the BiLSTM network as a sequence modeller. Random Forest determines the best split point in splitting the entire data and then all trees from the training stage are taken into consideration to detect/foresee intrusions more accurately. However, when it came to measuring performance on each model, it was shown that Random Forest model performed better than CNN-BiLSTM hybrid model in terms of accuracy in detecting genuine attacks. It is established that based on examining the data of network traffic, this kind of machine learning categorization methodology provides a viable approach that gives a real-time response to intrusion renewal.

6.1 Input for the classification function

The extracted features (the collection) which is taken as the traffic data are fed into the classifier as the input. These features possess different network-factor-related hints, which are taken from CIC-IDS2017 dataset. The features which are associated with the packet size, protocol type, source and destination IP addresses, port numbers, time intervals, service types and different others are examples of the input features [9]. For machine learning models producing the CNN-BiLSTM hybrid model and also Random Forest model, these attributes are the actual input data.

6.2 Classification result

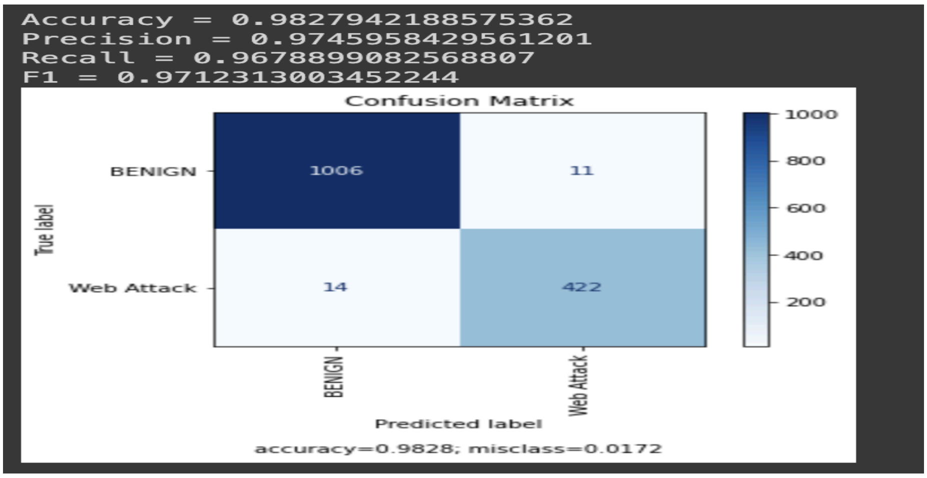
The pipeline involves training of the model able to classify or predict the network traffic data [3]. While, intrusion results in announcing that a malicious traffic shouldn't be entertained or both traffic types are benign. Here, the machine – learning model predicts the possibility that a particular traffic sector that is a network function represents an intrusion or an attack. We used a CNN-BiLSTM model or a Random Forest model in our research and the output is a binary class that takes the grain if a network traffic is an intrusion activity (attacks) or if it is normal/benign traffic. This hierarchical behaviour classification outcome becomes the starting point for the real-time intrusion detection system [1]. Through such detection, suspicious or malicious network behaviour is detected early and relevant actions of resources or alerting can be triggered accordingly.

7 The Role of Complex Event Processing in the Intrusion Mitigation Process

CEP provides a sophisticated framework for identifying and analysing various complicated patterns contained within an incoming data set. This function is a critical one among a chain of procedures during an intrusion mitigation process[4]. The feature precision process is really to consider the CEP (Complex Event Processing),which enables to collect the basic information about an attack campaign like source, destination and time. The potential of CEP is particularly useful in effectively tackling many dangers that unexpectedly emerge. With its advanced architecture CEP extracts the hidden patterns and intricate insights very accurately from incoming big objects. The skill that we talk about here is the base for real-time intrusion detection [18] . CEP helps to detect suspicious activity and activities that don't conform to the behaviour of networks' traffic. CEP massively minimises the intervention needed by humans just by recognizing probable threats, after that. The CNN-BiLSTM hybrid model considerably determines intrusion detection as the combined effect of Bidirectional Long Short-Term Memory (BiLSTM) and convolutional Neural Network (CNN). This hybrid structure not only takes advantage of the long-range dependencies being handled by the BiLSTMs, but also benefits from convolution networking that effectively determines the topological invariants. We thus develop a new hybrid model, which successfully merges the benefits of the Complex Event Processing (CEP) system with the most recent neural network architecture concepts, to support the search for intrusion [8].

8 Performance Analysis

The proposed CNN-BiLSTM combined model has been enriched with a performance study. Accuracy, precision, recall, and F1-score are the key metrics included to make the analysis more complex providing more details about where the model has performed well [6]. Metric of accuracy shows the general reliability of model's classifications, which is the most important metric evaluated. The level of calculated precision is 0.9476 and the model has the level of accuracy which is 0.9592 showing that the right direction has been taken in predicting the model results. This indicates good results in the right standard. This provided thorough proof about the location where the data was likely to provide the optimal results, thus reducing false negatives and improving the system overall reliability. It is calculated by the recall metric of how well the model detects any intrusion events and comes in at 0.8624. The model proves to identify 69.8 percent of the actual events by reinforcing the regime of the malicious activity. The F1-measure, accompanied by the accuracy and recall, have shown 90.82%. Stressing the facts that the model has proved to be good in identifying structures and balancing out the rate of false positives and making the rate of false negatives the balanced score will be the focus of this discussion.



```
Accuracy = 0.9827942188575362
Precision = 0.9745958429561201
Recall = 0.9678899082568807
F1 = 0.9712313003452244
```

Fig. 6. Performance analysis using all metrics

8.1 Accuracy

Accuracy indicates how close the value to be calculated is to a certain number or acceptance. They can be described as subjective estimates of recall and recall rotation (weighted by dispersion) and estimates of accuracy and precision (weighted by bias) [10].

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

8.2 Precision

The precision, often called the positive analytic rate, is part of the quality of the recovered data.

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

8.3 Recall

The fraction of retrieved contexts relative to the total number of contexts is called recall score.

$$\text{Recall} = \frac{\textit{True Positive}}{\textit{True Positive} + \textit{False Negative}}$$

8.4 F-1 score

The F1-measure of a system is defined as the weighted harmonic mean of accuracy and recall.

$$\mathbf{F1} = 2 \times \frac{\textit{Precision} \times \textit{Recall}}{\textit{Precision} + \textit{Recall}}$$

9 Conclusion

The efficiency of a CNN-LSTM fusion model regarding CEP-based real-time intrusion detection has been analysed in the present paper. This hybrid model was confronted with the Random Forest model during the research, and it showed better results concerning various types of network attacks. This study is mostly devoted to the problems of intrusion detection system management security, it is necessary to consider the readiness for self-adaptive systems. We are going to discuss how the Intrusion Detection System processes the alerts and how to guess the gaps between true positive and false positive rates that have the key role in the reliable system detection. The actual architecture which satisfies these objectives must include recognized vulnerabilities along with the features which will be stable, reliable, secure and interoperable. The role of Complex Event Processing is highlighted in this paper while its advantages and disadvantages are compared to Intrusion Detection System. In improving alert detection and event processing rates, future studies may go ahead and include a wider array of algorithms and embed adaptive and autonomous frameworks as well.

10 Future work

The prospective investigation on this matter can involve utilising the intrusion detection system (IDS) on a bigger and more complex network. The system may be substantially improved to detect both tried intrusions and also attacks that already occurred. Alteration of classification algorithms would spend less time doing analysis, it will therefore be able to catch cases at a much higher rate. Shortening the time of detection and making detecting the process more accurate will be performed with the help of better algorithms. In addition, future work should deal with expanding the range of threats addressed especially inside complex networks in order to let the IDS operate optimally.

References

1. S. Sandosh, V. Govindasamy, G. Akila, “Enhanced intrusion detection system via agent clustering and classification based on outlier detection”, Peer-to-Peer Networking and Applications https://doi.org/10.1007/s12083-019-00822-3,Springer 2020.

2. Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks", IEEE Access, vol. 7, pp. 42210-42219, 2019.
3. S. Sandosh, V. Govindasamy, G. Akila, "Enhanced Learning Vector Quantization for Detecting Intrusions In IDS", International Journal of Web Portals, Volume 12, Issue 1, June 2020.
4. C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks for real time intrusion detection", IEEE Access, vol. 5, pp. 21954-21961, 2017.
5. W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, et al., "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection", IEEE Access, vol. 6, pp. 1792-1806, 2018.
6. Aditya Kumar Singh, (2023) "A Periodic Validation in Blockchain-based Mobile Edge Computing (MEC) through Key Management." Available at: https://ijarsct.co.in/Paper12774.pdf. DOI: 10.48175/IJARSCT-12774.
7. Javaid A et al (2016) A deep learning approach for Comprehensive intrusion detection systems. In: Proceedings of EAI international conference on bio-inspired information and communications technologies (formerly BIONETICS), pp. 21–26
8. Aljawarneh S et al (2018) Signature-based intrusion detection sys- tem through feature selection analysis and building hybrid efficient models. J Comput Sci 25:152–160
9. Faisal MA et al (2015) Spatial Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study. IEEE Syst J 9:31–44
10. Hamed T., & Kremer, S. C. (2017). Intrusion detection in contemporary real time environments. In Computer and Information Security Handbook (Third Edition) (pp. 1-26). Elsevier.
11. Sadiq, A. S., Alkazemi, B., Mirjalili, S., Ahmad, N., Khan, S., Ali, I., Pathan, A. S. K., & Ghafoor, K. Z. (2018). An efficient IDS using hybrid CNN LSTM model. IEEE Access, 6, 29041–29053.
12. R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying convolutional neural networks for network intrusion detection",pp. 812-6009, DOI: 10.1109/ICACCI.2017.8126009.
13. U. Ravale, N. Marathe, and P. Padiya, "Feature selection based hybrid anomaly intrusion detection system", vol. 45, pp. 428-435, DOI: 10.1016/j.procs.2015.09.062.
14. Shi Y et al (2018) Malicious domain name detection based on extreme machine learning. Neural Process Lett 48:1347–1357
15. M. Tahir, N. I. Udzir, and A. Azman, "A Hybrid Deep Learning Technique for Intrusion Detection System," pp. 1-6, DOI: 10.1109/ICCI.2015.7470789.
16. Creech G, Hu J (2013) Generation of a new IDS test dataset: time to retire the KDD collection. In: IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp 4487–4492.
17. Y. Shi, L. Chen, and Y. Wang, "Malicious domain name detection based on extreme machine learning," Neural Processing Letters, vol. 48, no. 3, pp. 1347-1357, 2018.
18. P. Shettar, A. V. Kachavimath, M. M. Mulla, and D. G. Narayan, "Intrusion detection system using MLP and chaotic neural networks," in Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–4, Coimbatore, India, January 2021.
19. Dey, "Deep IDS : a deep learning approach for real time Intrusion detection based on IDS 2018," in Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1–5, Dhaka, Bangladesh, December 2020.
20. Sainath, T.N., Vinyals, O., Senior, A., Sak, H.: Convolutional, long short-term memory, fully connected deep neural networks. In: Google, Acoustics, Speech and Signal Processing (ICASSP), pp. 4580–4584. IEEE (2015).