
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 5, pp. 2286–2295, DOI 10.12694/scpe.v26i5.5037

NETWORK TRAFFIC ANOMALY DETECTION ALGORITHMS ON DISTRIBUTED SYSTEMS USING COGNITIVE INTELLIGENCE

NING PAN*

Abstract. Network traffic monitoring is one of the important roles to maintain the security and confidentiality between distributed systems particularly in detecting early cyber threats. Distributed system is a large network interconnected device, which are connected with one another. So, detecting anomalies is a major challenge in these systems. Traditional systems fail to detect anomalies in early stages, because threats are too advanced which are not handled by the traditional capacities. To address this issue the present study proposed and improved version network traffic monitoring system called (Net-IV). This approach combines the advantages of 1D-CNN, Long Term-Short Term Memory (LSTM) and GRU (Gated Recurrent Units). Accoridng to this, 1D-CNN which is well known for its feature extraction ability, whereas LSTM helps to analyse the temporal dependencies, finally GRU refine the overall performance and helps to detect anomalies with greater precision. The model was evaluated using CIC-1DS-2017 dataset, a complete benchmark dataset for intrusion detection system. Through the simulation, we observed that the suggested Net-IV achieves a remarkable accuracy rate of 99.78% and F1-Score of 99.56% which is 0.05% higher than the existing DCGCANet model. Thus, the results suggested that the proposed Net-IV system could be effectively installed in real-time, to protect the distributed system confidentialities from various forms of cyber-attacks.

Key words: Network traffic anomaly detection, CNN, LSTM, GRU, distributed system, cognitive intelligence

1. Background.

1.1. Distributed Systems Advantages and the Impacts of Cyber Threat. Distributed system is one of the advanced technologies which interconnected with multiple systems to achieve a specific goal. This involves the advantages of resource sharing, fault tolerance, scalability and parallel processing which is very helpful for large scale applications like cloud computing, data processing, and network services [13, 1]. One of the main advantages of the distributed system is their ability to operate efficiently and continuously, even in the situations of individual system failure. But however, the decentralized nature of distributed systems also introduces risks in the form of cyber-attacks, which targets any node or system can disturb the entire process and the confidentiality of the privacy data. Distributed Deniel of Service (DDoS) attacks, man in the middle attacks, and malware propagation are some of the common risks which impacts the data privacy availability and confidentiality [12, 4]. Since distributed systems depends on network communication for, by using this advantage these attacks are spread quickly and leads to the sever impacts like network corruptions, data breaches, leakages in privacy data. So, there is an increasing demand of advanced anomaly detection algorithms, cognitive intelligence solutions to continuously monitor the network traffic, detecting anomalies in real-time and prevent possible security risks [9]. This helps to anomaly free transformations between the systems and helps to improve the security of distributed systems also to guarantees the safety of confidential data.

1.2. Previous Techniques and its Drawbacks. Most effective techniques are proposed in the existing articles to address the anomaly detection issues, but however these techniques also face some common limitations which is discussed below.

This study [3] used the benefit of unstructured log analysis technique with Finite State Automaton (FSA) for anomaly detection. Thos approach mainly depends on log keys; these keys are not able to capture all the system behaviors effectively. This paper [16] identifies the anomalies by using the triangular approach, this model also fails in accurately identifies the anomalies due to the limitations of big dimensionality. VeLog a VAE variational autoencoder method is used to detect anomalies in distributed systems is the main of this study [14],

*Hubei University Big Data Center,Wuhan,430062, China, email: ningpancampupeas@rediffmail.com

but however we find the difficulties regarding fine tuning the models in real-time large-scale environments. In this study [8] Fuzzy base clustering approach is used to handle the network anomalies, but there is an increase in clustering it leads to computational overload and make the possibility in network complexities. This study [5] used a deep learning based BiLSTMtransformer-based model for anomaly detection. This approach also highlights the drawback regarding extensive computational resource.

1.3. Suggested Net-IV and its advantages. By thoroughly analysing the existing studies advantages and disadvantages, the present study focuses to present the hybrid model called Net-IV, which combines the benefits of powerful deep learning techniques: 1D-CNN, LSTM, and GRU, which are combined to create the effective structure to address the risk of threats, also detects the anomalies early to avoid the severe impacts.

The main aim of the study is to construct a new network traffic anomaly detection system called Net-IV and examine its ability to learn and operate on distributed cognitive intelligence systems. we seek to improve the performance and speed of anomaly detection by integrating 1D-CNN for feature embedding, LSTM to capture temporal dependencies, and GRU for performance tuning and precision improvement. The study focuses on offering a comprehensive method to secure distributed systems in real time as an alternative to existing solutions that are incapable of addressing the problem of recognizing low and high level cyber attacks including advanced persistent threats.

The main contributions of the paper as follows

1. In Net-IV, ID-CNN is responsible for extracting the essential features from raw network traffic data by identifying abnormal patterns and provide the strong foundation for further analysis.
2. LSTM and GRU are used to capture temporal dependencies in the data and allows the system to understand the sequence and flow of traffic over time.
3. Finally, Net-IV model is simulated using CIC-IDS-2017 network traffic dataset

1.4. Literature Discussions. According to the proof of 2016 Mirai-injected IP camera attack, risk will take place due to the, unsecured cheap devices, some of the attacks happening is denial-of-service (DDoS) attacks in IoT environments. By analyzingthis, the study [6], suggested D-PACK mechanismwhich combines a CNN with an unsupervised autoencoderdetects traffic anomalies with near-perfect accuracy and a low false-positive rate. Existing machine learning based anomaly detection facility commonly struggles due to the adaptability and handling the multiple data. To address this, the study [17] proposed LSTM based approach to classify the abnormal traffic data with high precision. Article [15] also suggests the LSTM based period wise detection approach to achieve the better performance in real time anomaly detection. Study [11] investigates the anomaly detection by using the proposed model as conditional variational autoencoder (CVAE) and random forest (RF) classifier to effectively improve the detection ability of anomalies. Traditional deep learning drawbacks in anomaly detection and how it is addressed using the advanced deep learning solution was discussed in the study [10]. This study achieves encouraging scores demonstrating how deep learning can improve anomaly detection by processing raw network traffic data without requiring domain expertise for feature selection.

The task of identifying anomalies in distributed systems is an overwhelming task that comes with many complications due to the size, complexity, and changing nature of these ever expanding networks. Distributed systems often consist of various interconnected devices that produce large amounts of diverse data making it hard to detect thinly layered or hidden anomalies related to cyber threats. Conventional means of detecting anomalies, such as static rules or baselines, are ill-equipped to respond to changing attack patterns by unforeseen or sophisticated threats. For example, stealthy types of Advanced Persistent Threats (APTs) target other forces over a long period to penetrate the systems and remain undetected by conventional methods. To addition, zero day attacks focus on unknown vulnerabilities making them able to bypass signature based detection systems. Distributed Denial of Service (DDoS) attacks propagate vast amounts of legitimate traffic never been witnessed before making conventional systems unable to determine whether an attack is in progress or whether there is a peaceful activity. Encrypted traffic and polymorphic malware that constantly mutates even more contribute to the problems of detection. Traditional approaches fail in both handling that amount of data in a reasonable time frame or analyzing the current scene of traffic therefore making comprehensive distrust of such distributed systems possible. These challenges underline the need for advanced anomaly detection techniques, cognitive intelligence models for instance, which are fitted for the needs of such complicated environments.

The traditional anomaly detection approaches are limited in many ways to effectively identify early-stage

and more complex threats. Even though these systems can detect anomalies, advanced cognitive and predictive threat analytics would assess predefined signatures, static threshold limits, or statistical baselines. More advanced threats, such as Advanced Persistent Threats (APTs) and zero-day exploits, have been purposely developed to defeat these types of detection mechanisms–they target becoming undetectable or take advantage of never before seen attack vectors. For instance, polymorphic malware makes frequent alterations to its code structure hence bypassing signature-based systems. Encrypted traffic, on the other hand, harbors vicious activity as traditional approaches cannot analyze encrypted patterns.

Similarly, they cannot process real-time large volumes of high-dimensional data streams produced by distributed environments. This leads to slow times in detection and response times, especially in the presence of compounds in the traffic patterns. The temporal dependencies of sequential data are also not confined by traditional approaches; for example, an attack could be started by minor changes in user behaviors or the flow of a network before it becomes fully aggressive. This absence of context compounds the issues of very high false positive rates and undermines the confidence in these systems.

2. Methodology.

2.1. Net-IV Structure Outline. The proposed methodology consists of 3 layers: Initial layer involves, 1D-CNN based feature extraction, LSTM for further analysing the extracted patterns and finally GRU helps to detect anomalies, LSTM and GRU are the two main Recurrent Neural Network layers helps to thoroughly analysing the traffic patterns and detect the anomalies with high precision. Here, ID-CNN processes raw network traffic data to extract meaningful spatial features. This componenthelps to identify the relevant patterns by reducing the dimensionality and fed into the layer of LSTM and GRU for further analysis. Together with these layers (LSTM and GRU), the model thoroughly analyze the normal behavior of traffic sequence and identifying abnormalities with high accuracy. The final component of the architecture is fully connected layer that combines the outputs of both LSTM and GRU followed by the softmax layer for classification. This allows the model to identify the final predictions about the network traffic is normal or abnormal. The whole framework is designed to handle the large-scale network traffic data in real-time. Finally, the model is assessed using the real-world comprehensive dataset and highlight the effective output, and acts as an efficient contribution for monitoring traffic in distributed systems. Figure 2.1 presents the visual illustration of proposed architecture.

The Net-IV model brings together three cutting-edge branches of neural networks; namely, 1D-CNN, LSTM, and GRU into the network traffic anomaly detection process to enhance accuracy and precision. The 1D-CNN (One-Dimensional Convolutional Neural Network) deals with feature extraction, allowing for the identification of important spatial features in the traffic flow data including packet sizes and flow attributes. Its convolutional layers go through the raw inputs of the data and capture high-order features about the most relevant attributes for anomaly detection while noise and redundancy are minimized.

2.2. 1D-CNN based Feature Extraction. The initial layer of 1D-CNN performs the initial feature extraction in the suggested Net-IV architecturewhich helps to handling the unprocessed network traffic data. The input layer, convolutional layer, pooling layer, fully connected layer, and output layer are the main layers of conventional 1D-CNN architecture. The input layer receives the time-series, raw network traffic data and prepares it for convolutional processes, which will further convert it. Applying convolutional kernels to the input data is the main job of the next convolutional layer in Net-IV. This allows for the extraction of important spatial information from the network traffic data, about anomaly patterns.

The convolutional kernel in a 1D-CNN refers one-dimensional array. The convolution procedure significantly reduces the number of parameters in a 1D-CNN by sharing weights among neurons. Then output of convolutional layer's expressed as

$$ax_n^j = g\left[\sum_{i\in N}\left(ax_{n-1}^i kl_n^{ij}\right) + bi_n^j\right] \tag{2.1}$$

Here, ax_n^j denotes the output of the $j-th$ neuron in the $n-th$ layer, ax_{n-1}^i is the previous layer input and kl_n^{ij} denotes the kernel connecting the $i-th$ neuron pf the previous layer to the $j-th$ neuron in the current layer, bi_n^j is the bias terms and g is the activation function. After convolution the pooling operation is applied

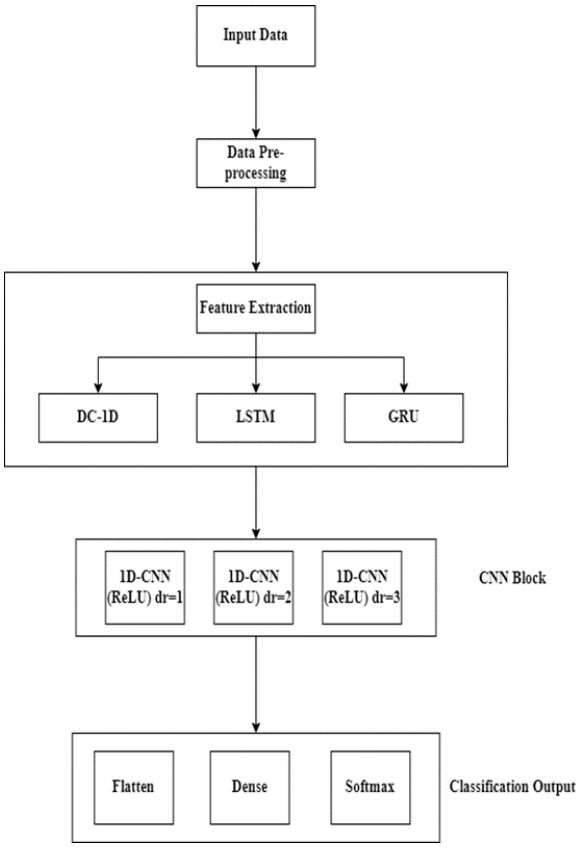

Fig. 2.1: Suggested Framework

downsample the data and reduce the complexity. Pooling can perform using either max pooling or average pooling. Max pooling selects the maximum value within the specific window and average pooling calculates the average value in the same window. These can be defined as

$$pz_n^i = maxpool(ax_{n-1}^i, s1, s2) \tag{2.2}$$

$$pz_n^i = avepool(ax_{n-1}^i, s1, s2) \tag{2.3}$$

Here, pz_n^i denotes the output of the pooling operation in the i-th neuron in the n-th layer and s1, s2 is the pooling scale and step size respectively. This pooling helps to reduce the size of feature map and safeguard the most important data when the process of eliminating redundant data takes place.

2.3. Integration of LSTM-GRU layers. The integration of GRU and LSTM networks in the Net-IV architecture provideseffective way for managing the temporal dependencies present in network traffic data. The sequential data processing abilities of LSTM and GRU helps to perfectly identifying abnormalities in real-time network traffic data.

Using its cell state, input gate, forget gate, and output gate processes, LSTM is used in Net-IV to maintain long-term dependencies in the network data. The LSTM network changes its hidden state for a given input sequence $\{ax\}_{t=1}^{N}$?, where ax_thighlights a sequence of input vectors and N denotes the total number of occurrences. This can be expressed as

$$pz_t^i = \sigma(w\ ax_t^i + u\ pz_{t-1}^i) \tag{2.4}$$

where w and u are the weight matrices and σ is the activation function. The hidden state pz_t^i at each time step is used to capture long term dependencies in the input data. The LSTM output is then, processed through the fully connected layer (FCN) and the softmax function for classification, this process is expressed as

$$p\left(y-i \mid ax\right)=softmax\ \ (wax+bi)=\frac{e^{w_i ax+bi_i}}{\sum_j e^{w_j ax+bi_j}} \tag{2.5}$$

The LSTM process helps to learn the temporal dependencies over long sequence, but it highlights the limitations of computationally expensive performance. To reduce the complexity in managing the performance Net-IV involves GRU layer on the other side of LSTM. GRU are simply faster using few parameter functions. It involves the update and reset gate to process the flow of information. These are expressed as the following

$$rt_t = sig(w_{rt} \cdot [h_{t-1}, ax_t]) \tag{2.6}$$

$$pz_t = sig(w_{pz} \cdot [h_{t-1}, ax_t]) \tag{2.7}$$

$$\tilde{h}_t = tanh(w_h \cdot [rt_t \times h_{t-1}, ax_t]) \tag{2.8}$$

$$h_t = (1 - pz_t) \cdot h_{t-1} + pz_t \cdot \tilde{h}_t \tag{2.9}$$

Here rt_t controls the reset gate, pz_t is the update gate and h_t is the hidden state at time step t. When compares to LSTM GRU simplify the process of the model and effectively capturing the dependencies.

The Net-IV architecture makes use of both the efficiency of GRU and LSTM by combining the outputs of the two. With the least amount of training time and computational resources, our hybrid technique guarantees that the model can accurately identify complex anomalies in network data. To train both models, the back-propagation algorithm is used, this helps to minimizes the cost function CL, which is expressed as

$$CL = \sum_{i=0}^{|D|} \log(p\left(ay\right) = (ay_i \mid ax_i, w, bi)) \tag{2.10}$$

This is the final optimization which ensures the model identifies the best parameters for detecting anomalies in large-scale real time network environments.

3. Results and Experiments.

3.1. Dataset Description. Developed in 2017, the CIC IDS 2017 dataset was created by the Faculty of Computer Science from the University of New Brunswick, aiming to improve the ISCX 2012 dataset. Advancing the earlier work, this dataset defines a realistic depiction of network usage and is intended to remedy the drawbacks present in prior intrusion detection system (IDS) datasets. The researchers claim that the CIC IDS 2017 dataset complies with 11 requirements regarding the design of IDS datasets, such as full network configuration, labeled set, different types of attacks, and extensive meta-data. These criteria allow us to say that the dataset is representative and of adequate size to assess the effectiveness of the IDS.

The dataset encompasses daily traffic and attack data for five days, yielding more than 225,745 network packets, which may have up to 80 different features. It incorporates not only normal network activity but also a range of intrusion activities, collected within a week. The simulated attacks in this dataset are divided into 7 types, which are Brute Force Attack, Heartbleed attacks, Botnet, DoS attacks, DDoS attacks, Web Attacks, and Infiltration Attacks.

The present research takes into consideration the DDoS (Distributed Denial of Service) attacks where a target system or network is assaulted with a flood of traffic mostly from a botnet to bring the system down. Please note some of the key traits associated with DDoS attacks are: inter-arrival times (IAT) of flows (minimum, mean, maximum), flow bandwidth measures, and flow duration. The higher these attributes' values are, the

Table 3.1: Dataset Features

Category	**Details**
Dataset	CIC-IDS-2017
Training Data Period	July 3-July 7, 2017
Types of Traffic	Normal (BENIGN) + 9 Attack Types
Training and Testing Ratio	7:3
Attacks Considered	(DDoS, Brute Force, Infiltration, etc.) - 9
Framework	TensorFlow
Operating System	Windows 11 64-bit
CPU	Intel i7-12700H
GPU	NVIDIA GeForce RTX 3070 Ti
Programming Language	Python 3.6
IDE	PyCharm 2020.1

greater the likelihood that DDoS has been employed. In the case of abuse network behavior, the attributes such as B. Len Min sub server byte length, the number of subflows, total packet size and mean packet size are of more relevance.

The proposed study evaluated using the CIC-IDS-2017 dataset inspired from[2], according to the details we extract the necessary features to evaluate the proposed Net-IV. Table 3.1 provides the clear illustration about the dataset.

3.2. Pre-processing CIC-IDS-2017 Dataset. Two important processes are involved in preprocessing the CIC-IDS-2017 dataset: Feature normalization and one-hot encoding. Non-numeric features, like category attributes, are converted into binary vectors using one-hot encoding. Then it is used as input in the deep learning model. The model was able to process features such as 'protocol_type' efficiently because they were converted into binary representations. Features were also normalized to address the significant differences in feature scales. The performance of the model is affectedby some features, such as "Flow IAT Max" and "Total Length of Fwd Packets". To address this, all features were scaled to a range of [0, 1] using mean-variance normalization.

According to parameter setting, inspired from the study[7], according to the procedures we perform the evaluation of proposed framework.

3.3. Evaluation Criteria. The proposed model is evaluated using the common performance metrics of accuracy, recall, precision and F1-Score. The process of evaluation is conducted according to the attack types. Figure 3.1 highlights the model's efficacy in different attack types. According the epoch of 10 the accuracy of the proposed model reached up to 99.78%. Overall, the Bot and Portscan highlights the slight decrease. But when compared with the accuracy, the proposed obtains an effective score in all the attack types.

Figure 3.2 presents the efficacy of models in terms of accuracy, precision, recall and F1-score, according to this the proposed Net-IV model is compared with the existing KNN, ID3, MLP, RF, CNN, AFM-1CNN-1D, CNN-GRU, DCGCANeT. From the figure we observed that the proposed model significantly out performs all the models with its remarkable accuracy. Also, it shows that the proposed Net-IV achieves the accuracy about 99.78%, 99.82% and 99.72% of precision and recall respectively. And finally, the F1-score is about 99.58%, when compared with the existing DCGCANet the proposed model significantly outperforms the DCGCANet model due to its additional involvement of GRU

Similarly Figure 3.3 presents the efficacy of models in terms of computation time. The computation time of the suggested model 250.12 seconds, when compared with the tradition individual techniques of KNN, RF, CNN, ID3 the fusion model utilizes the additional timing to process the data effectively, as a results, it slightly higher than the traditional individual models. When compared with the existing fusion methods the proposed model really beats the other models with its less inference time.

Figure 3.4 presents the results of generalization ability of the models. According to this we involve 4 subsets called SP1, SP2, SP3 and SP4 to test the entire CIC-IDS-2017 dataset was inspired from[7]. In this section

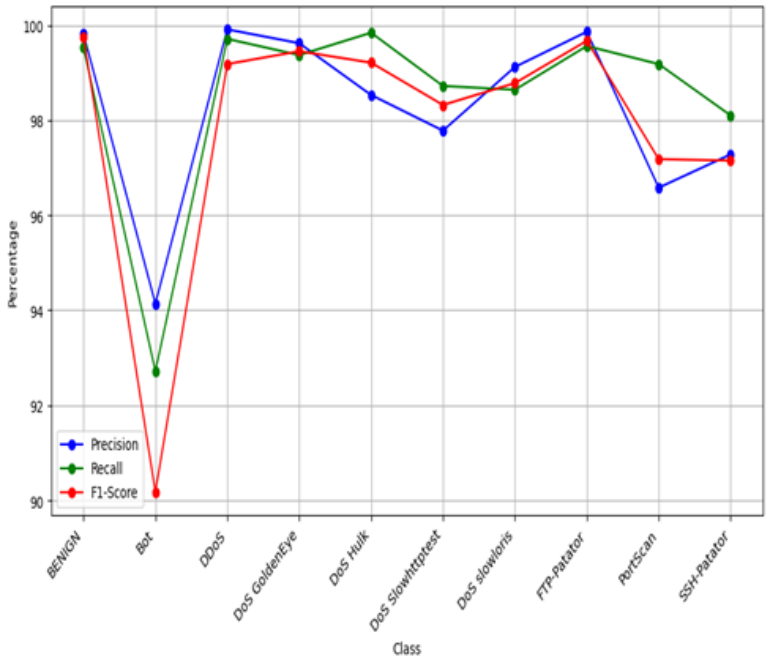

Fig. 3.1: Performance Evaluation under CIC-IDS-2017 Based Attack Types

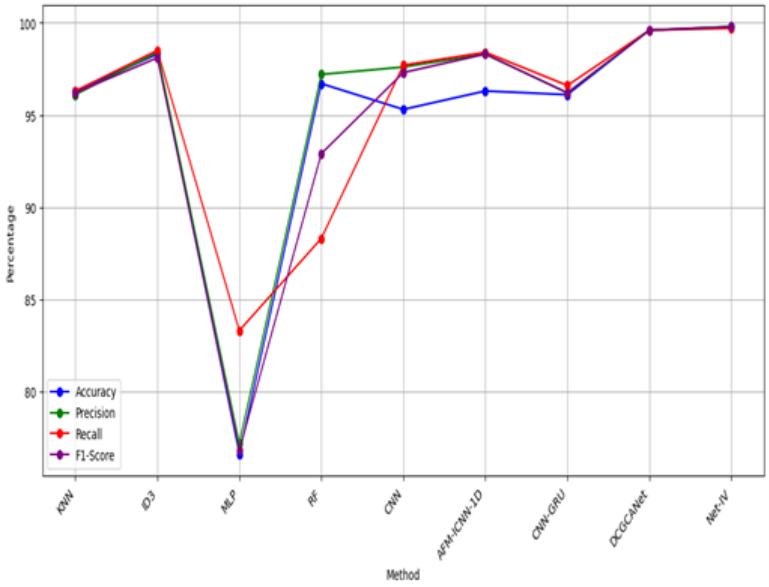

Fig. 3.2: Overall Performance Comparison of Models

the proposed Net-IV model is compared with the existing effective DCGCANet model. This model is a fine competitor of proposed Net-IV model. But the result highlights the proposed Net-IV model outperforms the DCGCANet with its effective outcomes.

The use of 1D-CNN, LSTM, and GRU for network related activity monitoring thesis can be explained

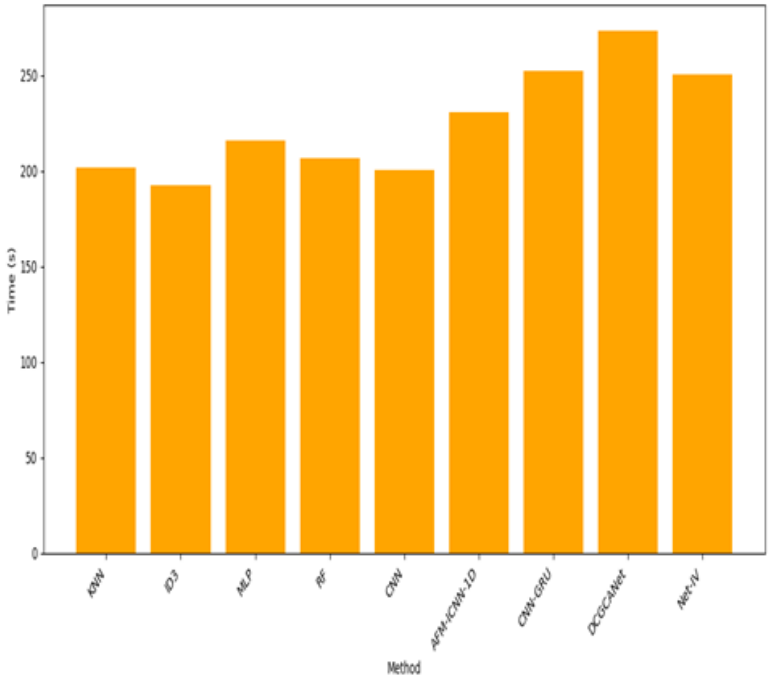

Fig. 3.3: Comparison of Computational Time

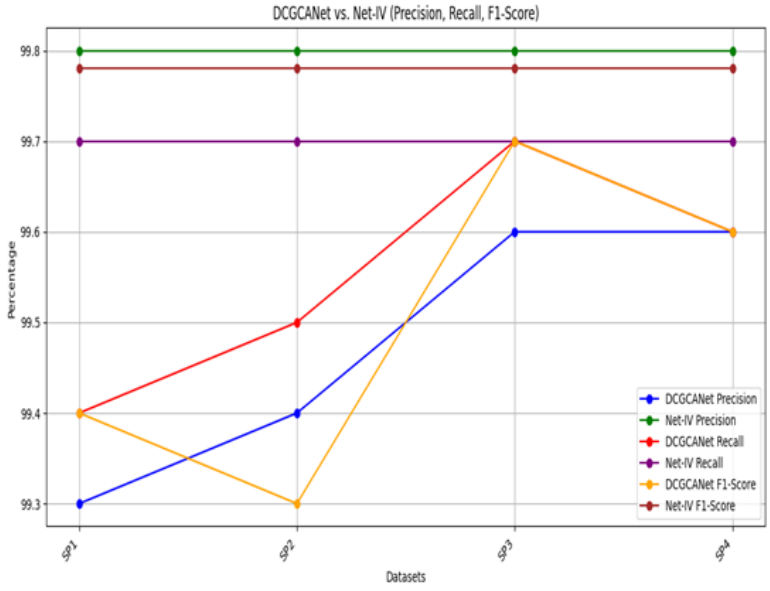

Fig. 3.4: Subset Based Efficiency Analysis

by the fact that these networks show a combination of complementing strengths in capturing sequential and high dimensional data respectively. The one dimensional convolution network (1D-CNN) was picked mainly because it is more efficient at extracting particular traffic data spatial features such as packet size and flow

patterns at less computational cost than 2-D CNN. The convolutional layers within it capture local patterns quite effectively which are very useful in detecting any abnormalities within network traffic. However, a Long Short-term Memory (LSTM) LSTM was added to solve the requirement of the network traffic's time related features in sequential data analysis. Long short term memory (LSTM) networks are very good at remembering information for long periods, using its memory cells to assist in detecting time dependent, minute anomalies quite easily, such as advanced persistent threats (APTs) and traffic variability over time.

LSTMs and GRUs (Gated Recurrent Units) governance or structures are thought to be integrated due to their hierarchical efficient structure and their potential to cause problems often referred to as the vanishing gradient in recurrent neural networks (RNNs). Because GRUs have fewer parameters than LSTMs, GRUs are quicker to train and validate while maintaining precision. The model's overall effect is improved since maximum memory and processing efficiency are used.

4. Conclusion. The present study introduced the effective Net-IV model to analyse and identify the network traffic anomalies. The proposed model effectively combines the advantages of ID-CNN, LSTM and GRU to finely detect the abnormalities in network raw data. The suggested model is evaluated with CIC-IDS-2017 dataset, a comprehensive benchmark dataset used to evaluate in the intrusion detection scenarios. By compare the results of our proposed model with the existing models particularly, with the existing DCGCANet model, Net-IV proves it efficacy with the accuracy score of 99.78% and 99.56% of F1-score which is 0.05 % improvement when compared with the existing DCGCANet model. The future search is needed to effectively reduce the computational complexities was raised due to the fusion of the models. The future search is needed to effectively reduce the computational complexities was raised due to the fusion of the models. When incorporating continuous learning frameworks, the model will be able to smoothly transition towards new or newer threat behaviours without the need for total retraining, and therefore maintain their reliability and relevance over time.

REFERENCES

[1] V. Chandola, A. Banerjee, and V. Kumar, *Anomaly detection: A survey*, ACM computing surveys (CSUR), 41 (2009), pp. 1–58.

[2] K. Fotiadou, T.-H. Velivassaki, A. Voulkidis, D. Skias, S. Tsekeridou, and T. Zahariadis, *Network traffic anomaly detection via deep learning*, Information, 12 (2021), p. 215.

[3] Q. Fu, J.-G. Lou, Y. Wang, and J. Li, *Execution anomaly detection in distributed systems through unstructured log analysis*, in 2009 ninth IEEE international conference on data mining, IEEE, 2009, pp. 149–158.

[4] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, *Real-time big data processing for anomaly detection: A survey*, International Journal of Information Management, 45 (2019), pp. 289–307.

[5] P. Han, H. Li, G. Xue, and C. Zhang, *Distributed system anomaly detection using deep learning-based log analysis*, Computational Intelligence, 39 (2023), pp. 433–455.

[6] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, *An unsupervised deep learning model for early network traffic anomaly detection*, IEEE Access, 8 (2020), pp. 30387–30399.

[7] C. Ji, H. Yu, and W. Dai, *Network traffic anomaly detection based on spatiotemporal feature extraction and channel attention*, Processes, 12 (2024), p. 1418.

[8] H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, *Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling*, Journal of Parallel and Distributed Computing, 73 (2013), pp. 790–806.

[9] H. Li and Y. Li, *Logspy: System log anomaly detection for distributed systems*, in 2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE), IEEE, 2020, pp. 347–352.

[10] G. Marín, P. Casas, and G. Capdehourat, *Rawpower: Deep learning based anomaly detection from raw network traffic measurements*, in Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos, 2018, pp. 75–77.

[11] M. Monshizadeh, V. Khatri, M. Gamdou, R. Kantola, and Z. Yan, *Improving data generalization with variational autoencoders for network traffic anomaly detection*, IEEE Access, 9 (2021), pp. 56893–56907.

[12] A. Pamukchiev, S. Jouet, and D. P. Pezaros, *Distributed network anomaly detection on an event processing framework*, in 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2017, pp. 659–664.

[13] A. D. Pazho, G. A. Noghre, A. A. Purkayastha, J. Vempati, O. Martin, and H. Tabkhi, *A survey of graph-based deep learning for anomaly detection in distributed systems*, IEEE Transactions on Knowledge and Data Engineering, 36 (2023), pp. 1–20.

[14] Y. Qian, S. Ying, and B. Wang, *Anomaly detection in distributed systems via variational autoencoders*, in 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2020, pp. 2822–2829.

[15] Z. Shi, J. Li, C. Wu, and J. Li, *Deepwindow: An efficient method for online network traffic anomaly detection*, in 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International

Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2019, pp. 2403–2408.

[16] S. Thudumu, P. Branch, J. Jin, and J. Singh, *A comprehensive survey of anomaly detection techniques for high dimensional big data*, Journal of Big Data, 7 (2020), pp. 1–30.

[17] Y. Zhong, W. Chen, Z. Wang, Y. Chen, K. Wang, Y. Li, X. Yin, X. Shi, J. Yang, and K. Li, *Helad: A novel network anomaly detection model based on heterogeneous ensemble learning*, Computer Networks, 169 (2020), p. 107049.

Edited by: Rajkumar Rajavel
Special issue on: Cognitive Computing for Distributed Data Processing and Decision-Making in Large-Scale Environments
Received: Sep 27, 2024
Accepted: Nov 26, 2024