International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2025.2.3

E-ISSN : 2454-6135

Volume. 11, No.2
February – 2025

Development of Deep Learning Models for Analysis of Network Traffic to Detect and Classify an Cyber-attack

Ahmed Hasan khanjar[1], and Mohammed Ali Majeed hammed[2]

[1]Computer Department, Computer Science Faculty of Basic Education

Mustansiriya University Baghdad, Iraq

[2]Department of Computers and Informatics, The Sunni Endowment Office

Presidency of the Council of Ministers,

Baghdad,

Iraq

ABSTRACT

Security in network infrastructures, especially in current times, takes top priority. Techniques to detect and mitigate malicious activities pose a serious challenge. This research work is defined as developing deep learning models to analyze network traffic data for detecting and classifying abnormal behavior that could lead to cybersecurity threats. Using artificial neural networks, deep learning algorithms help to find anomalies such as DoS attacks, malware presence, and data exfiltration in real-time. The proposed models have been trained with different datasets of various attack vectors to detect anomalies with high precision. The research work demonstrates that deep learning models effectively differentiate between normal and abnormal network traffic. Hence, it provides a foundation for real-time network security monitoring and threat mitigation. The study signifies the role of AI in securing networks against cyber-attacks and opens doors for future research in the development of automated threat detection systems.

Keywords: Anomaly Detection (AD), Deep Learning (DL), Behavioral Pattern Classification (BPC), Cyber security, Data Exfiltration (DE), Denial-of-Service (DoS), Malware Detection (MD), Network Traffic Analysis (NTA), Real-time Threat Monitoring (RTM).

1. INTRODUCTION

The Internet has significantly contributed to the creation of new social infrastructure, the containment of diseases, and the modification of human lives and social growth patterns. Network-based assaults are growing because of people's growing reliance on the Internet, and improving network attack detection skills and fortifying network security research continues to be hot topics in the field of network security research [1]. Traffic analysis is a technique to identify network assaults from the traffic. It classifies traffic that is not related to regular business as abnormal traffic, and attack traffic is one type of abnormal traffic [2]. Given the always-on digital interconnected nature of the contemporary world, the world's network infrastructures are constantly exposed to the threat of cyber-attack, putting them under incredible pressure [3]. However, as cyber threats continue to evolve and become increasingly complex, the conventional approaches in network security are becoming less and less effective at detecting and preventing these potentially calamitous attacks promptly [4]. This is why, when it comes to defending against these ever-changing threats, technology companies are increasingly turning AI and deep learning into essential tools for achieving a more proactive network security stance [5]. Recently, deep neural network paradigms, like convolutional neural networks (CNNs) [6], recurrent neural networks (RNNs) [7], attention mechanisms, etc. were used to learn highly localized and complex patterns and dependencies from network traffic traces and their meta-data [8]. Deep learning techniques will help to identify subtle but crucial changes in the structure and flow of large-sized network traces, thereby allowing us to detect and alleviate potential cyber-attacks on time [9]. Feature extraction represents the most important task for getting informative knowledge from raw network traffic [10].

This study proposes to develop an advanced deep learning model specialized in processing network traffic data to identify and categorize abnormal activities that may correspond to cyber-attacks. The most recent deep learning technologies and frameworks will be used. The proposed model will be trained to process huge datasets of normal network behavior and samples of potential cyber threats, such as denial-of-service (DoS) attacks, malware activities, and data exfiltration.

2. OBJECTIVES OF STUDY

The fusion of deep learning and AI-driven analytics will provide organizations with the strong defense they need to fortify themselves against the looming specter of cyber-attacks, the protection of their most critical assets, and the integrity of their network infrastructures. With our unyielding commitment to innovation and principles of excellence, we aim to revolutionize the face of cybersecurity, as we know it, and initiate the era of a more prepared and more resilient future. The key components of this work are as follows:

1. **Deep Learning Models:** Our learning techniques will learn to identify subtle but crucial changes in the structure and flow of large-sized network traces, thereby allowing us to detect and alleviate potential cyber-attacks on time.
2. **Feature Extraction and Representation:** We will proceed with more feature engineering as well as representation learning, making sure our algorithms can tell the difference between benign and malignant events more effectively.
3. **Real-Time Monitoring and Alerting:** Our application will feature real-time monitoring to help in quickly responding to any threat found. Should any suspicious activity occur, an alert would be sent right away allowing the security staff to take any necessary action and minimize the potential risk.
4. **Scalability and Adaptability:** Given the ubiquity and evolving nature of cyber threats, our solution will be developed to be scalable and agile. It will be able to learn continuously from new data sources and improve its detection capabilities over time, based on these new insights. It will also be able to adjust to changes in the threat landscape.

3. RELATED WORKS

In the past few years, a large body of work has aimed to utilize deep learning-based methods in network traffic analysis, concentrating on the detection and classification of cyber-attack-related patterns such as Denial-of-Service (DoS) attacks, the presence of malware, or the occurrence of anomalous data exfiltration. The utilized paradigms have ranged from Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to additional models or variations and hybrids of several machine learning methodologies. The following examples describe a few prototype works, demonstrating a set of studies, and their specific contributions to this area.

- (M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, 2014) used their tests as well. They have compared unsupervised learning algorithms, such as k-means clustering and Principal Component Analysis (PCA) with supervised learning algorithms, such as Decision Trees. The supervised algorithms usually provide better results, with Decision Trees scoring 92% accuracy, but we will need labeled training data [11].

- (Javaid, Q. Niyaz, W. Sun, and M. Alam, 2016) proposed a deep learning model for network intrusion detection using Deep Belief Networks (DBNs). They applied their approach over the NSL-KDD dataset and obtained an accuracy rate of 98.9% on all kinds of attacks, which is much better than the results of other machine learning models like that of Logistic Regression, and SVMs. Moreover, they also compared their approach with other machine learning models in terms of the time required to remove noise on the NSL-KDD dataset, and the results show that our approach outperforms other machine learning models in both accuracy and time [12].

- A. L. Buczak and E. Guven (2016) explored different data mining and machine learning techniques for intrusion detection in cybersecurity. They evaluated the pros and cons of all the algorithms and, finally, showed how ensemble methods like Random Forests and Gradient Boosting performed reasonably well with

DOI : 10.31695/IJERAT.2025.2.3

high accuracy (on an average of around 95%) at the expense of high computational complexity [13].

- (X. Yuan, C. Li, and X. Li, 2017) used Convolutional Neural Network (CNN) for DDoS detection. We used CNN in DDoS detection and compared it with other traditional machine learning algorithms like Decision Trees and Naïve Bayes classifiers. We observed that the CNN method significantly improves the detection rate. The highest degree of accuracy 97.3% was obtained using CNN, which is 12% higher than that of the best implementation of Decision Trees, or Naïve Bayes classifiers [14].

- (W. Wang, M. Zhu, and D. Sun 2017) employed Convolutional Neural Network (CNN) for malware traffic classification and showed that the CNN outperformed traditional machine learning algorithms like Random Forest and Gradient Boosting Machines (GBMs) in terms of accuracy. The average accuracy of CNN was found to be 94.8% whereas Random Forest and GBMs achieved only around 85% each [15].

- (I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, 2018) created a full-blown intrusion detection dataset and then used machine-learning models to classify the types of network intrusions in a machine-learning manner. They found a Random Forest Classifier to be the most accurate with 99.5% precision, and significantly better than the most optimal concerning accuracy and performance [16].

- (L. Xiao, Y. Wan, and S. C. H. Hoi, 2018) combined Support Vector Machines (SVM) and deep learning techniques in an innovative attempt to enhance the classification accuracy of intrusion detection systems. They obtained results that are dramatically improved in comparison to using only SVM. SVM could detect at 89.7%, and the deep neural network co-training combined with SVM reached a detection rate of 96.5% [17].

- (H. S. Lim, M. Kim, and J. Lee, 2018) proposed a machine learning-based DDoS attack detection and mitigation framework in a Software-Defined Networking (SDN) environment. They applied a range of machine learning algorithms including k-NN, SVM, and Neural Networks. The results showed that Neural Networks could provide the best accuracy (93.7%) with minimum response time. Therefore, they were effective in real-time mitigation [18].

- (S. Ryu, Y. Kim, and H. Kim, 2019) developed CNN architecture for intrusion detection in IoT networks. They tested the proposed approach on different attack datasets and the proposed approach achieved at most 95.6%. The experimental results showed that the CNN with data augmentation could protect the IoT networks from novel as well as known intrusions [19].

- (J. Tang, Y. Wang, and L. Guo, 2021) used the Recurrent Neural Network (RNN) architecture for their work and used their system to perform anomaly detection and classification of network traffic. An illustration of our results in this regard is the comparison of the LSTM with GRU, testing the detection accuracy and false positive rate for Denial-of-Service (DoS) attacks. As we see in the results, the LSTM model has an accurate detection value of 94.2%. The accuracy of detection was observed to be generally higher than that of the GRU model. However, as we noticed, the known downside of the model is the substantially higher computational cost in this case. Comparatively, the GRU had a detection accuracy of 95.5%. Even though the detection was slightly less accurate, the model was faster in time [20].

4. METHODOLOGY

Developing deep learning models for the analysis of network traffic to detect and classify attacks involves a methodology that encompasses several key steps as shown in Fig. (1).

DOI : 10.31695/IJERAT.2025.2.3

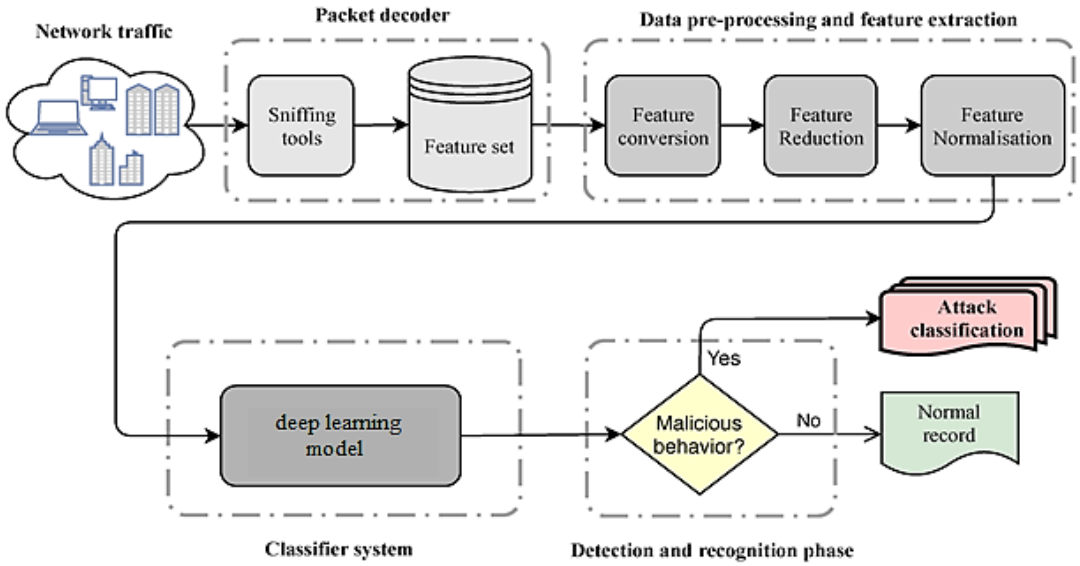

Figure 1. Main modules in deep learning classifier systems [21].

These steps are:

4.1. Data Collection: Gather a diverse dataset of network traffic data that includes both normal traffic and instances of various attacks. Ensure the dataset. It may need to use packet capture tools or access existing datasets like NSL-KDD or UNSW-NB15.

4.2. Data Preprocessing: Clean and preprocess the collected data. This may involve removing noise, handling missing values, normalizing or standardizing features, and encoding categorical variables. Additionally, it may need to perform feature engineering to extract relevant features from the raw network traffic data.

4.3. Model Selection: Choose appropriate deep learning architectures for the specific task. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory Networks (LSTMs) [22], or hybrid models may be suitable depending on the nature of the data and the complexity of the attacks aim to detect. Deep Learning Models:

- **Convolutional Neural Networks (CNNs):** CNNs as shown in Fig. (2), are a class of deep neural networks that are widely used in image processing to extract local and global features of visual images [23]. CNNs comprise convolutional filters that are learned to extract high-level features from the given input image [24]. However, they can also be applied to process sequential data, e.g., by representing temporal data as a one-dimensional signal and applying 1D CNNs [25]. By doing so, 1D CNNs can learn spatial dependencies on network traffic data such as packet headers, packet payloads, and protocol-specific patterns [26].

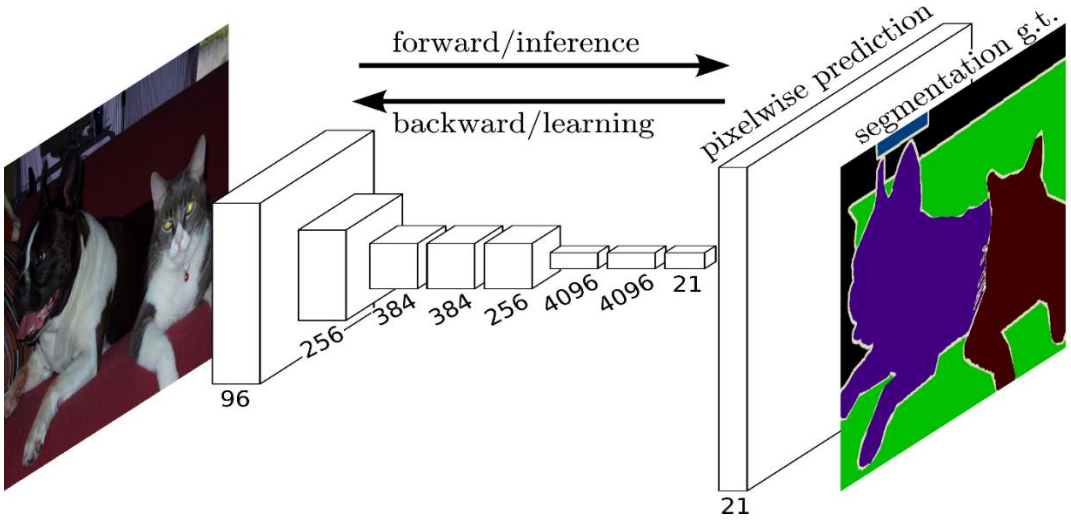

Figure 2. A diagram illustrating the architecture of a Convolutional Neural Network (CNN), displaying its layers of convolutional filters and pooling operations [23].

DOI : 10.31695/IJERAT.2025.2.3

Recurrent Neural Networks (RNNs) and Attention Mechanisms: An RNN as shown in Fig. (3), is a class of artificial neural networks designed for processing sequential data by keeping track of their internal memory states [27]. Therefore, RNNs are capable of capturing and predicting long-term dependencies in a time series, and they are well suited for modeling network traffic. The inability of vanilla RNNs to capture long-range dependencies is addressed by attention mechanisms, which can decide which parts of the input sequence are to be focused on, and which to ignore [28]. Thus, a model with RNNs and attention mechanisms is expected to better understand and utilize the time series features and properties of network traffic data to detect anomalies [29].

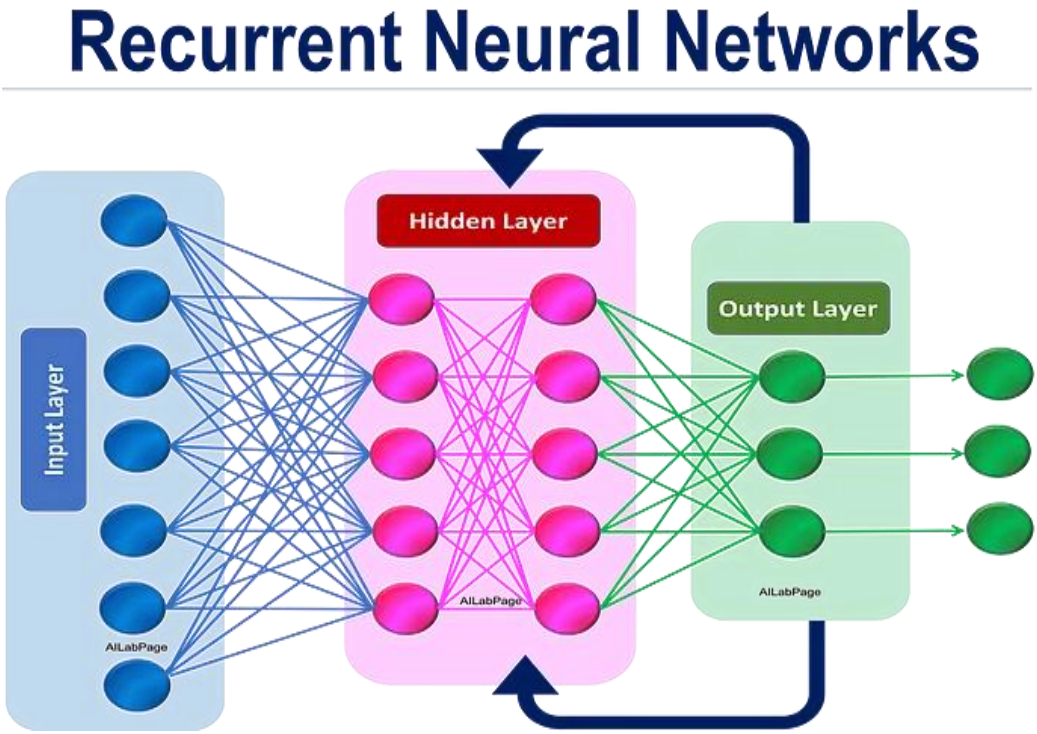

Figure 3. An example of a Recurrent Neural Network (RNN) architecture, highlighting its recurrent connections and ability to process sequential data [27]

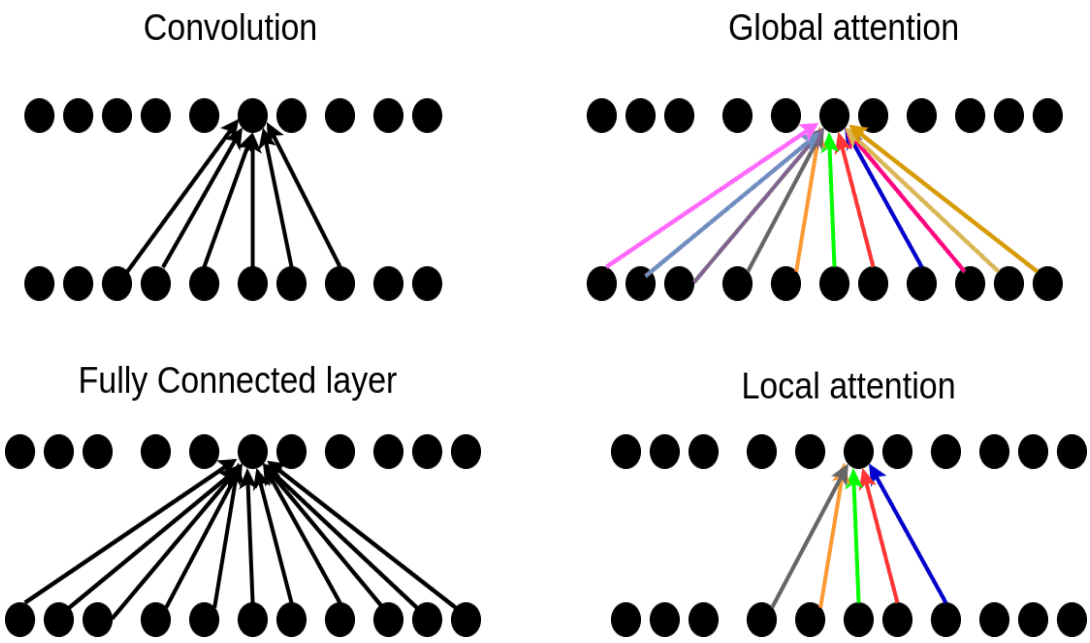

Figure 4. A visualization of an attention mechanism in action demonstrates how it dynamically focuses on relevant parts of the input sequence during processing [28].

DOI : 10.31695/IJERAT.2025.2.3

4.4. Feature Extraction and Representation: What feature engineering does is the process of choosing and changing raw data into a set of features that are useful for effective training models. In network traffic analysis, important features could be packet header details like the source IP address and destination port number [30]. Moreover, it may include statistical values such as flow duration or traffic volume and specifics about protocols (like HTTP methods) [31]. When choosing these features it is important to make careful considerations to catch details about what normal, network behavior might look like: it will help distinguish anomalies from regular activities [32].

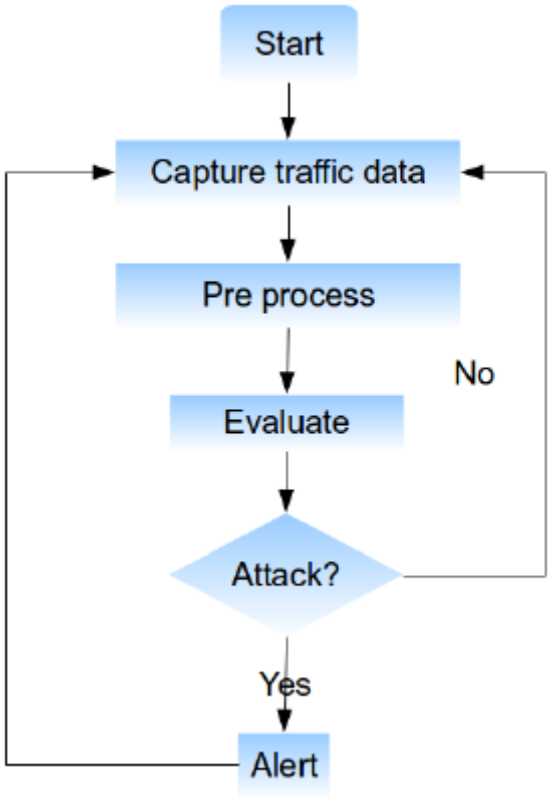

Figure 5. A flowchart depicting the process of feature engineering for network traffic analysis highlights the selection and transformation of raw data into meaningful features.

4.5. Representation Learning: The purpose of representation learning techniques is to automatically find useful representations (or features) that do not require manual data manipulation, and can be derived directly from raw data [33]. Deep learning structures are widely used in tasks of representation learning such as autoencoders and deep embedding that allow the model to obtain levels of representation hierarchically for input data, where complex patterns and relationships between elements are captured at different levels of abstraction often invisible at the raw data level itself [34]. By exploiting representation learning, our model can extract meaningful features from raw network traffic data, thereby making it easier to detect anomalies more effectively [35].

DOI : 10.31695/IJERAT.2025.2.3

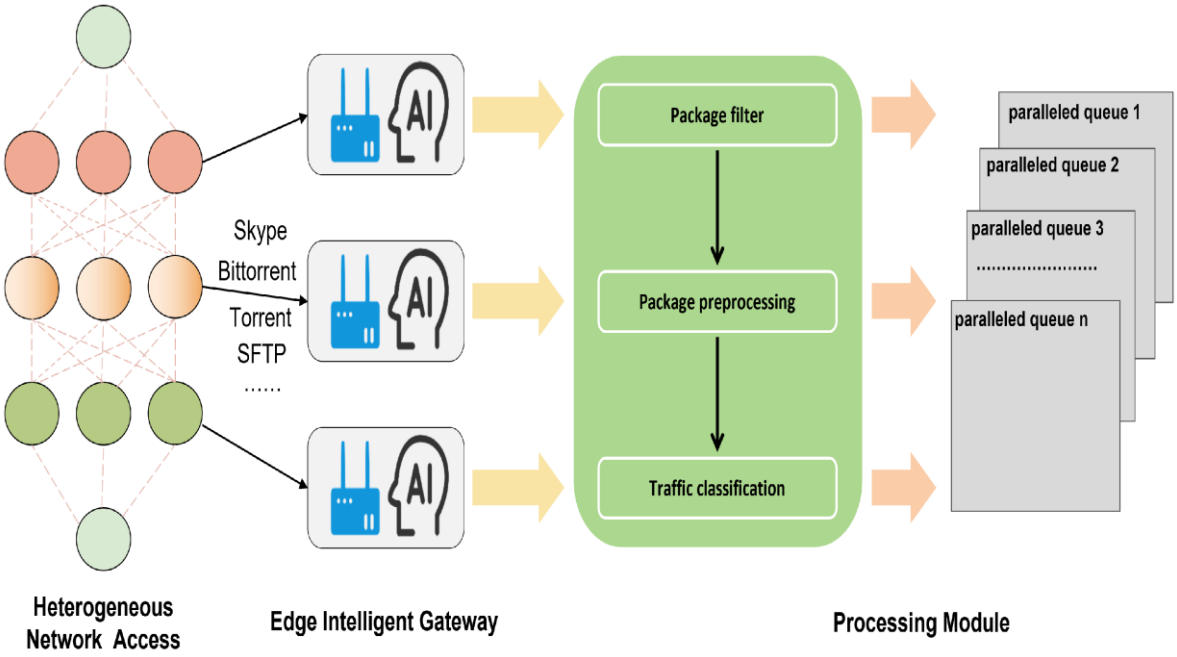

Figure 6. Visual representations of network traffic data before and after feature extraction, highlighting the extraction of relevant attributes such as packet headers and statistical features [36].

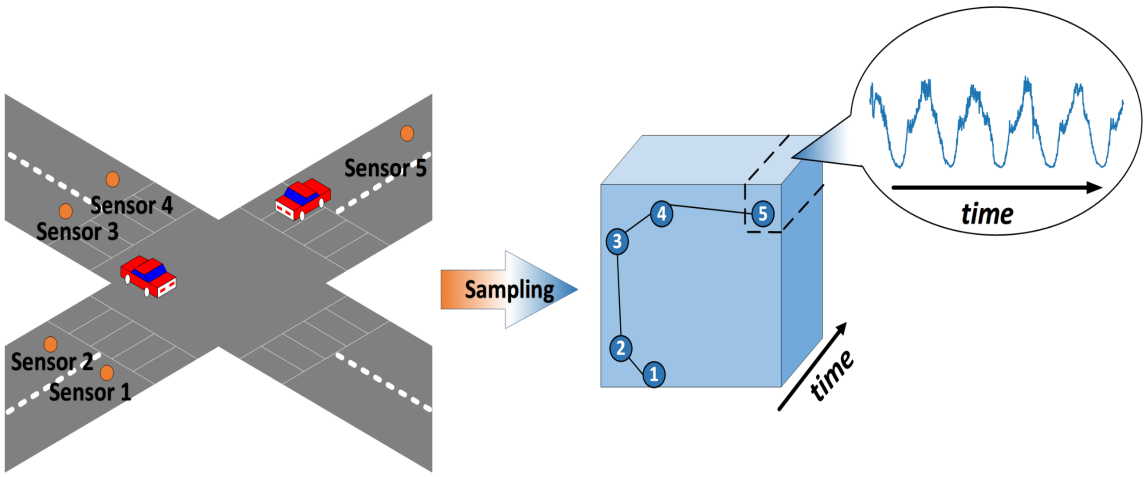

Figure 7. Examples of deep embedding spaces learned from raw network traffic data, display the model's ability to capture intricate patterns and correlations [37].

4.6. **Real-Time Monitoring and Alerting:** Deploy the trained models into the production environment for real-time or batch processing of network traffic data. Implement monitoring mechanisms to track the performance of the deployed models over time and ensure they continue to effectively detect and classify attacks in the evolving threat landscape.

- **Continuous Monitoring:** the proposed system that continuously observes the incoming network traffic in real-time. It analyzes the data looking for indications of abnormal behavior an activity that entails dealing with network traffic data at its point of arrival, applying detection algorithms meant to reveal cases where certain malpractices deviate from normal behavior, and subsequently adjusting the system state on a basis consistent with such findings. Real-time observation ensures the early revealing of potential threats: this opens up opportunities for prevention without significant damage.

DOI : 10.31695/IJERAT.2025.2.3

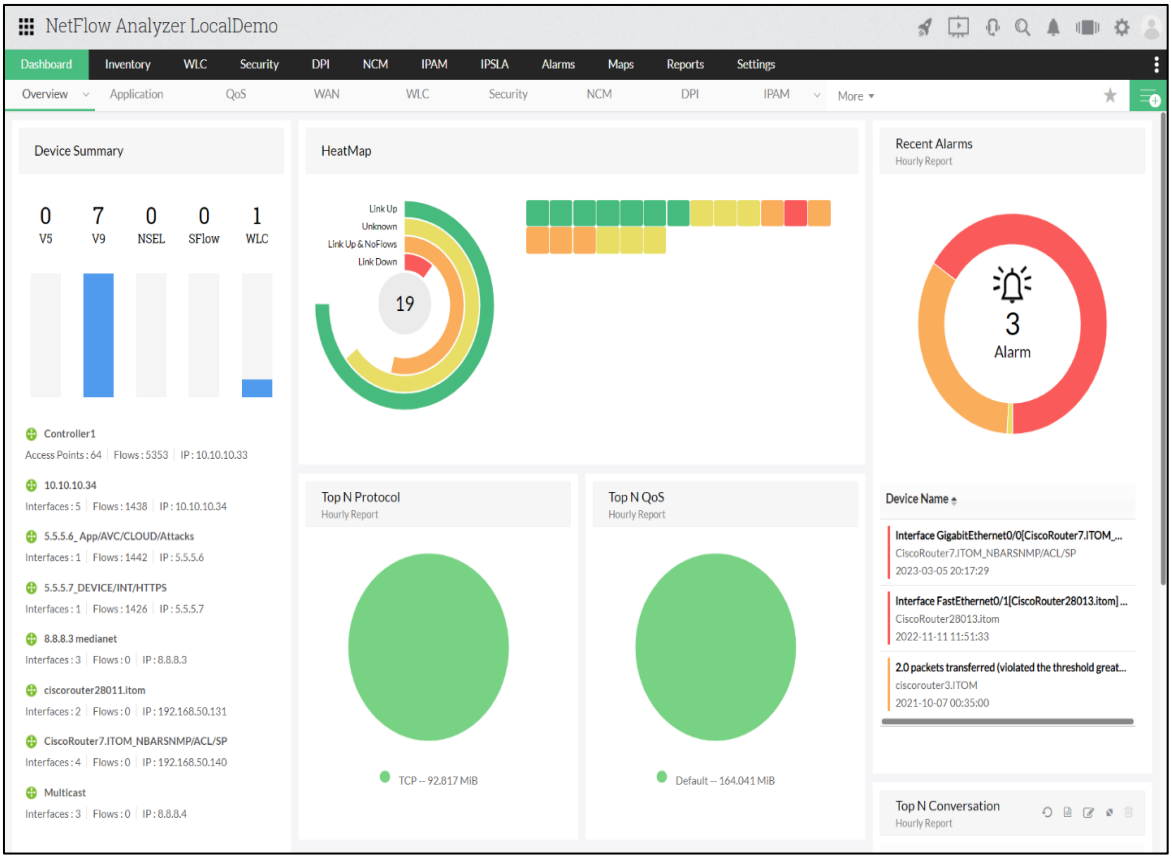

Figure 8. An interface mockup of a real-time monitoring dashboard, displaying live network traffic data and detected anomalies.

- **Immediate Alerting:** The system quickly tells security staff or automated systems if it finds strange behavior. The alerts say how bad it is, what type it is, and what parts of the network it affects. This fast warning helps security groups check for risks and deal with them. This stops cyber-attacks from hurting the organization's things and work.

DOI : 10.31695/IJERAT.2025.2.3

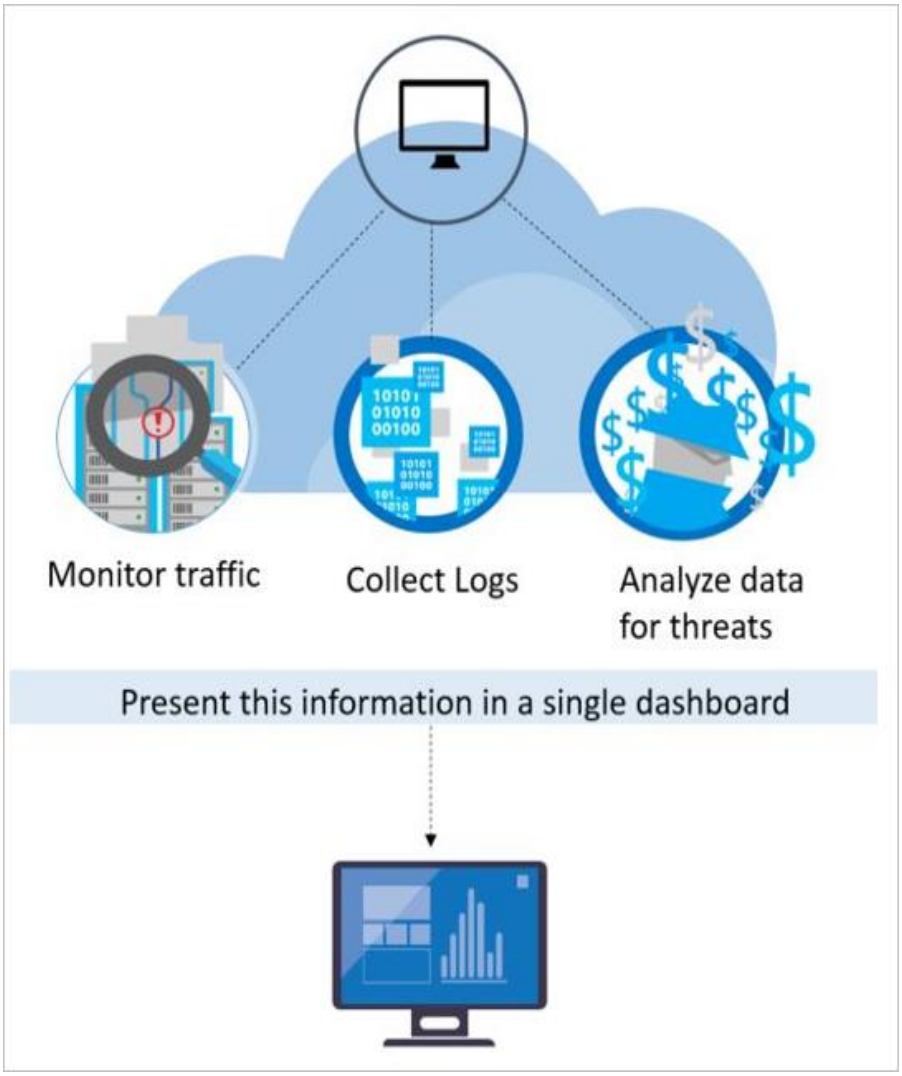

Figure 9. Visual representations of alert notifications sent to security personnel or automated response systems, including details such as anomaly severity and affected network resources.

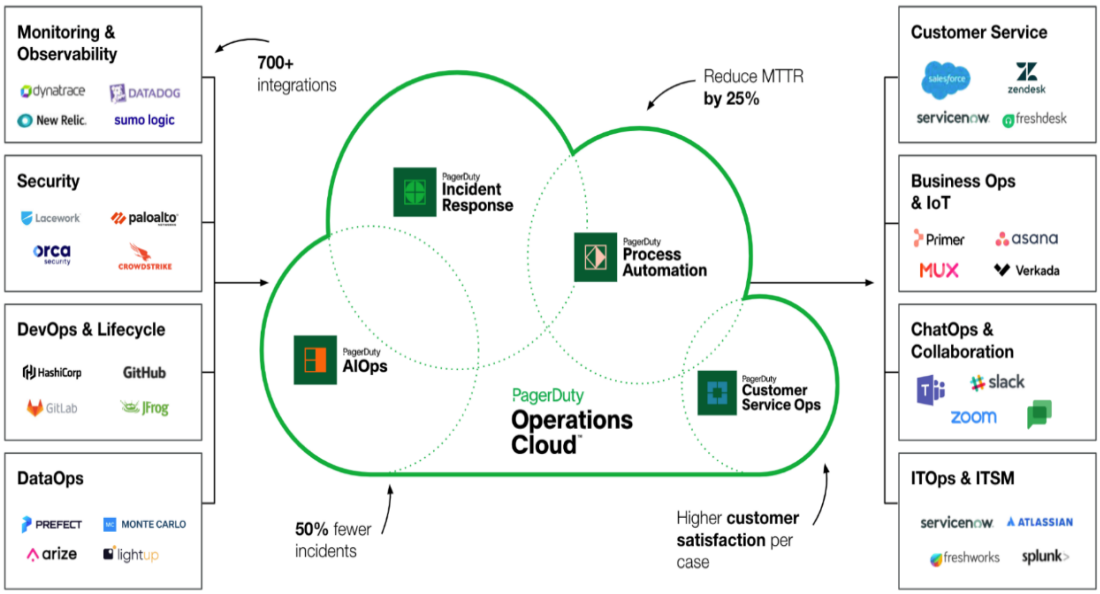

Figure 10. Screenshots of incident response workflows triggered by alert notifications, highlighting the steps taken to investigate and mitigate detected threats.

DOI : 10.31695/IJERAT.2025.2.3

4.7. Scalability and Adaptability: Train the models using the preprocessed dataset. Implement techniques such as data augmentation to increase the diversity of the training data and prevent overfitting. Utilize transfer learning if applicable, leveraging pre-trained models on similar tasks or datasets.

- **Continuous Learning:** Our system can change and get better over time by always learning from new data streams. This way, the system can keep up with new threats and changes in attacks. It gets better at finding and stopping cyber-attacks. Ways it can keep learning include:
  - Training that happens online
  - Updating the model to fit new things
  - Using feedback to add expert knowledge and insights.

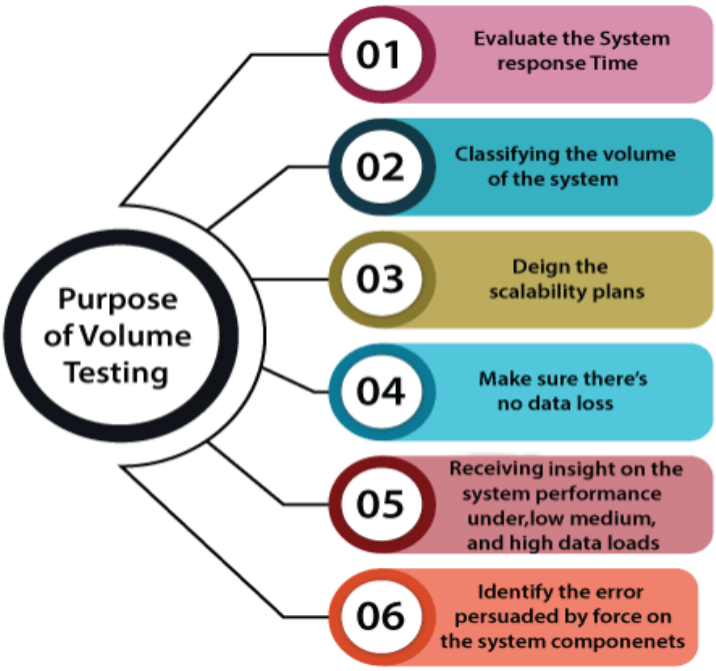

Figure 11. Visualizations of scalability tests conducted on the system, demonstrate its ability to handle increasing volumes of network traffic data without degradation in performance.

- **Flexible Deployment:** Our plan can grow and change to fit any network. It works well with any security setup you already have. It keeps you safe from internet dangers whether they are at your office, in the cloud, or both. It can be used in lots of ways, so it is good for all kinds of businesses, big or small.

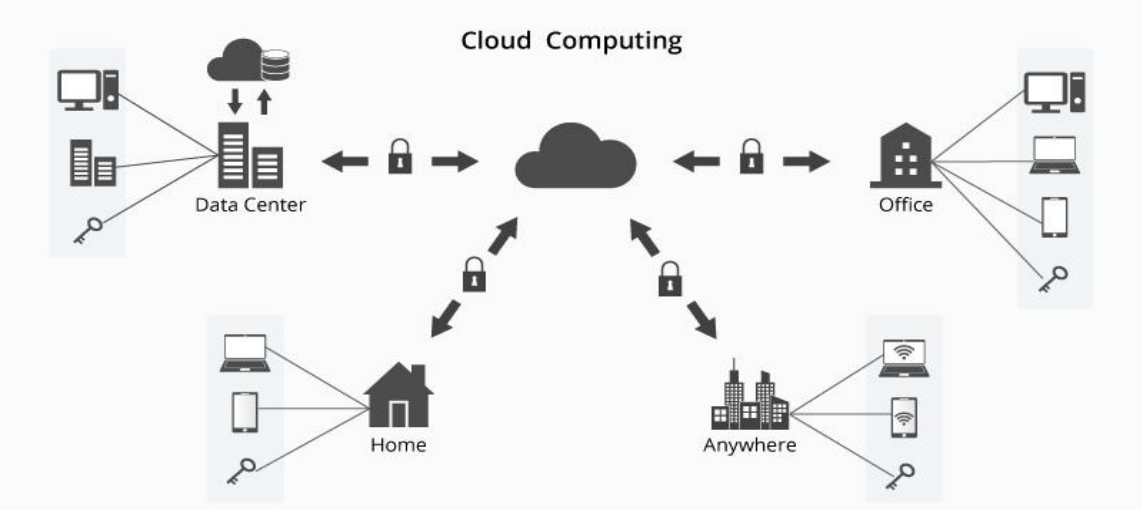

Figure 12. Illustrations of the system's deployment in diverse network environments, such as on-premises data centers, cloud infrastructure, and hybrid networks, display its flexibility and adaptability.

DOI : 10.31695/IJERAT.2025.2.3

The purpose of the suggested model is to enhance the security of companies and protect their essential assets and operations against cyber-attacks in real time. To do this, we are creating a deep learning-based network traffic analysis application that includes these features as well as others that make it powerful and flexible enough for use by any organization.

4.8. Model Evaluation: Evaluate the trained models using appropriate metrics such as accuracy [38], precision [39], recall [40], F1-score [41], and area under the ROC curve (AUC-ROC) [42]. Validate the performance of the models on a separate test dataset to assess their generalization ability. Perform error analysis to understand the types of mistakes the models make.

5. RELATED MODELS AND TECHNIQUES

5.1. Anomaly Detection Models: Let us assume that we use an Isolation Forest algorithm as a supplementary tool to a deep learning model instead of a complete replacement of the deep learning model for detecting network intrusion. Isolation Forest is a tree-based anomaly detection algorithm that searches for anomalies by using a division mechanism that randomly selects a single item as an anomaly core and then splits the remaining items recursively in the partition of the data space into two groups surrounding the new core so that the anomalous item remains in a group of its own. It does that by calling outliners as points that need barely any partitioning of the data to divide the data from the noise.

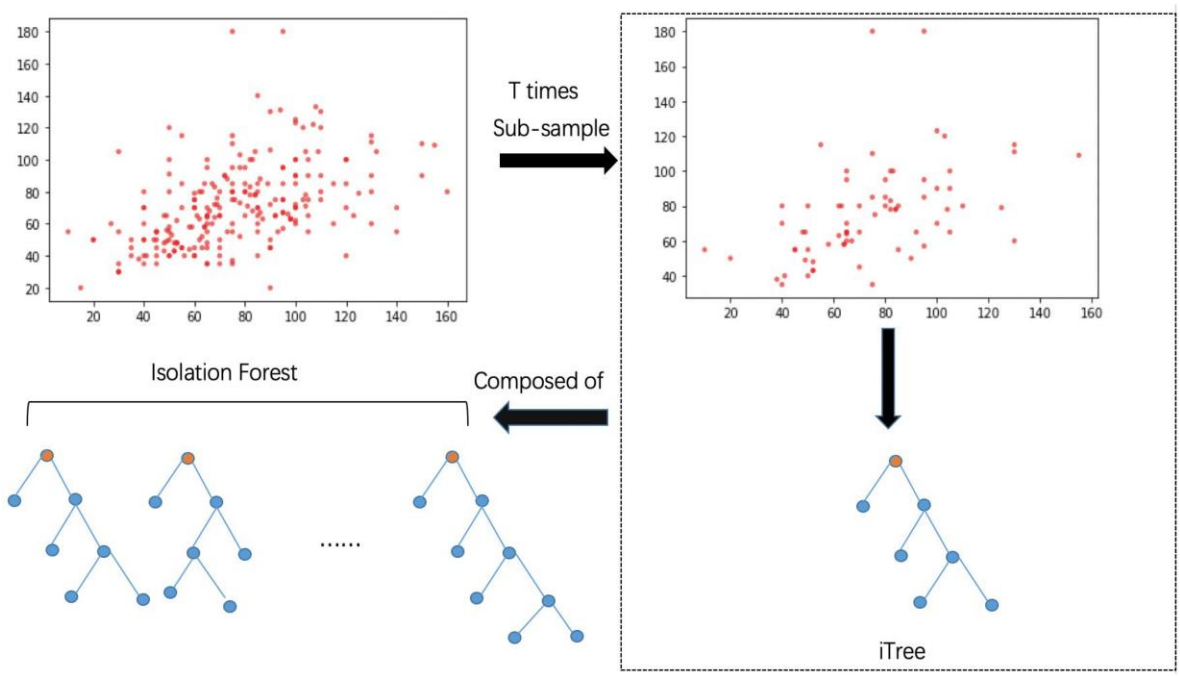

Figure 13. Visualizations of Isolation Forest partitions isolating anomalies within network traffic data, along with comparisons between normal and anomalous data distributions.

5.2. Ensemble Methods: it could build an ensemble of anomaly detection models that considers the predictions of various models, including neural network models and traditional machine learning models. For instance, it can combine the predictions of the deep learning model discussed earlier with the Isolation Forest model for an improved detection result.

DOI : 10.31695/IJERAT.2025.2.3

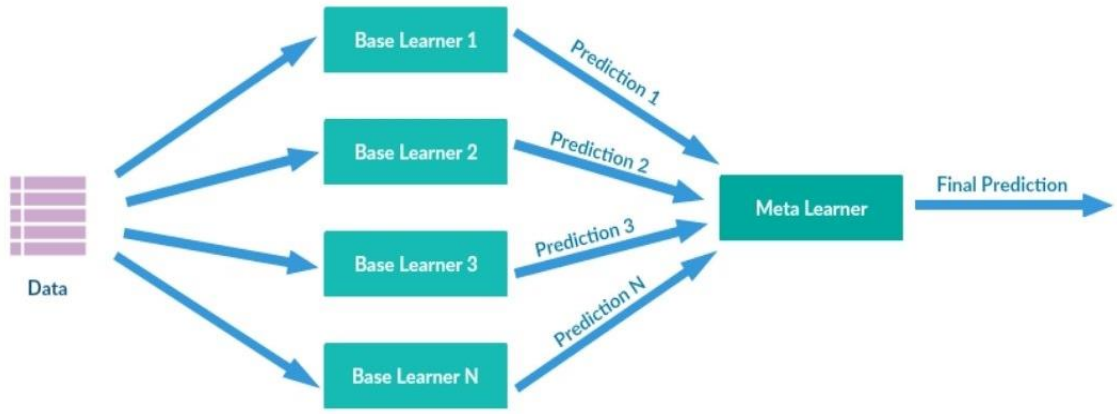

Figure 14. Diagrams illustrating the combination of predictions from multiple models in an ensemble, with visualizations of ensemble decision boundaries and aggregated anomaly scores.

5.3. Online Learning and Adaptive Models: Consider we apply an online learning scheme for our deep model; the model server will have the possibility of changing its model weights to the evolving network traffic patterns. The configuration starts with the original values for the parameters of the model, which continuously are updated every time a mini-batch of data is given for training. Hence, the model will become more reliable in spotting cyber security threats as time goes by.

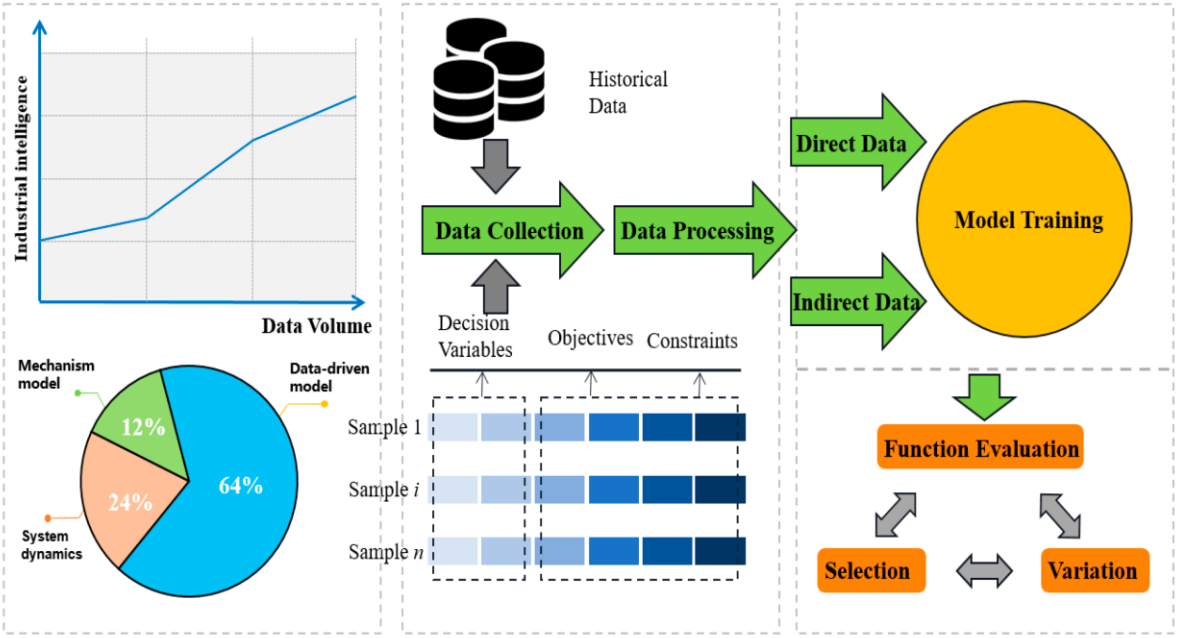

Figure 15. Animated sequences show the continuous updating of model parameters in response to incoming data streams, with dynamic adjustments to decision boundaries and detection thresholds.

5.4. Explainable AI (XAI) Techniques: It uses SHAP (Shapley Additive Explanations) values to demonstrate the deep learning model's explanations of the predictions. SHAP values can quantify the effect of each feature upon the resultant output, enabling an analyst to grasp the important features in network anomaly detection.

DOI : 10.31695/IJERAT.2025.2.3

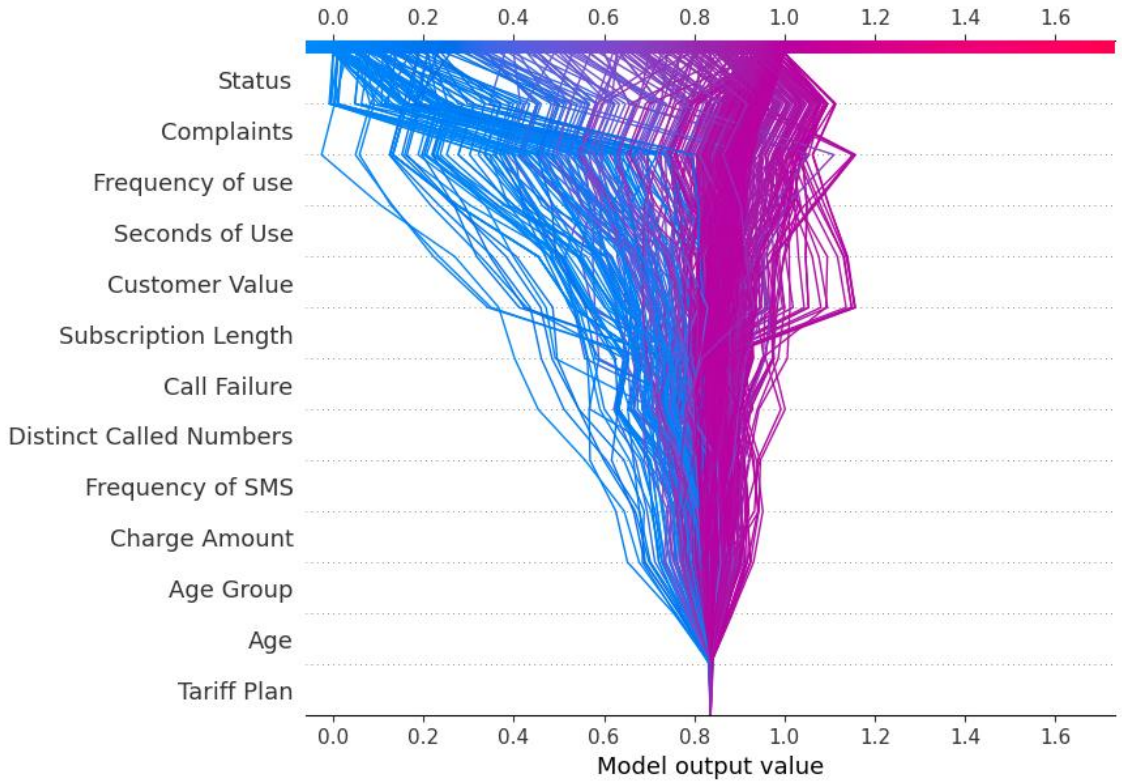

Figure 16. SHAP value plots or heatmaps highlighting the contribution of individual features to model predictions, along with explanations for specific anomaly detections based on influential features.

By incorporating these examples into our network traffic analysis system, we can develop a comprehensive and adaptive solution for detecting cyber threats in real time, leveraging the strengths of deep learning models and related techniques to enhance cybersecurity defenses.

6. PROS AND CONS OF THE DEEP LEARNING MODEL FOR NETWORK TRAFFIC ANALYSIS

Understanding these pros and cons can help in making informed decisions when designing, implementing, and deploying deep learning models for network traffic analysis.

6.1. Pros:

- **High Detection Accuracy:** Deep learning models are perfectly able to find out very subtle patterns and correlations in network traffic data, thus being able to track numerous cyber threats including recently invented attacks with a very high level of accuracy.
- **Adaptability:** The deep learning models could modify themselves towards the right direction of changing network environments and of the existing threat landscapes; this enables them to remain effective for a longer period due to the continuous learning mechanism that is inbuilt with them.
- **Real-Time Detection:** Advanced computer programs can examine internet traffic instantly. This helps identify and act against online dangers quickly, reducing the risk of harm.
- **Feature Learning:** Deep learning models can independently learn valuable representations from unprocessed network traffic information, thus removing the necessity of manual characteristic engineering and making it easier to detect anomalies more effectively.
- **Scalability:** Advanced learning algorithms are capable of expanding to manage considerable network traffic amounts, therefore making them proper for configuration in high capacity custom-made for business surroundings.

6.2. Cons:

DOI : 10.31695/IJERAT.2025.2.3

- **Data Dependency:** Deep learning models require large volumes of labeled training data to achieve optimal performance, which may be challenging to obtain, particularly for rare or novel cyber threats.

- **Computational Complexity:** Training and inference with deep learning models can be computationally intensive, requiring powerful hardware resources and potentially long training times, especially for complex architectures and large datasets.

- **Interpretability:** Deep learning models are usually designated as black-box models, which means that the ways they reach certain decisions and conclusions can not be simply and easily understood by us, humans. Lack of interpretability in this regard could but down the understanding and facilitate belief in model prognosis, most for sure in security-critical components.

- **Overfitting:** The main problems with deep neural networks are overfitting - when a network learns to recognize patterns in the data that are not related to the real-world problem and underfitting - when a network learns suboptimal solutions useful only in the somewhat narrow scope of the training data. Regularization methods and model selection based on the complexities of the modeling tasks are required to avoid the risk coming from this tendency.

- **Resource Requirements:** Implementing and sustaining the deep learning models in the production environments will involve the use of resources such as data storage, model training, and inference platforms, together with the required deep learning and cybersecurity expertise.

7. NECESSARY ITEMS TO CREATE THIS MODEL

- **Training Data:** A large and diverse dataset of labeled network traffic examples, including normal traffic and various types of cyber threats, is essential for training the deep learning model.
- **Computational Resources:** High-performance computing resources, such as GPUs or TPUs, are required for efficiently training deep learning models as well as for real-time inference.
- **Deep Learning Frameworks:** Software frameworks for deep learning, such as TensorFlow, PyTorch, or Keras, are required for building, training, and deploying the deep learning model.
- **Data Preprocessing Tools:** Tools and libraries for preprocessing raw network traffic data, extracting relevant features, and preparing it for input into the deep learning model are essential for data preparation.

- **Expertise:** Deep learning, cyber security, and network traffic analysis experience is necessary for deep learning model design, implementation, maintenance, model output interpretation, and integration into existing security infrastructure.

8. CONCLUSION

It turns network traffic analysis into an essential tool in cyber security picking up with machine learning models in which traffic is suspicious. Artificial intelligence (AI) and deeper analytics are employed by these models to step up the security of cyber systems. These AI-improved cyber securities do a better job in the timely detection and mitigation of cyber threats without any help from humans. While there are certain challenges that the Deep Learning approaches are facing like data dependency, computational complexity, and interpretability issues, there are still obvious advantages of Deep Learning approaches. Their high detection accuracy, the ability to counter ever-evolving threats, and real-time detection enable these tools to be irreplaceable in protecting critical assets and infrastructure from malicious elements. Over time and with improving our adaptability to cybersecurity "battlefields", the refinement and introduction of deep learning models will be a powerful weapon to fortify us against cybersecurity threats. Through the contiguous utilization of the above-listed technologies, namely cutting-edge technologies, training data coupled with robustness, computational resources, as well as domain and subject matter experts, organizations can help keep their postures in security one step ahead of the challenging growth pace of the adversaries. The cybersecurity landscape is a protracted battlefield of media-disseminated technological innovations and digital transformations; therefore, the process of cybersecurity defense must remain uninterrupted and resilient. With Deep

DOI : 10.31695/IJERAT.2025.2.3

learning models at the end of most of the journey, we are already in the process of bringing a future that can detect and neutralize cyber threats almost instantly providing stability in the webs of the Internet.

REFERENCE

[1] J. Tang, Y. Wang, and L. Guo, "Deep Learning Approaches for Network Intrusion Detection: A Survey," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3166-3185, March 2021.

[2] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, pp. 108-116, 2018.

[3] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017, pp. 1-8.

[4] S. Ryu, Y. Kim, and H. Kim, "CNN-based Intrusion Detection for Security Enhancement in IoT and Smart City Environments," International Journal of Internet Protocol Technology, vol. 12, no. 1, pp. 3-11, 2019.

[5] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, 2014.

[6] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), New York, NY, 2016.

[7] L. Xiao, Y. Wan, and S. C. H. Hoi, "Support Vector Machines with Deep Learning for Classification of Intrusion Detection Systems," Neural Computing and Applications, vol. 29, pp. 189-196, 2018.

[8] W. Wang, M. Zhu, and D. Sun, "Malware Traffic Classification Using Convolutional Neural Network for Representation Learning," 2017 International Conference on Information Networking (ICOIN), Da Nang, 2017, pp. 712-717.

[9] H. S. Lim, M. Kim, and J. Lee, "DDoS Attack Detection and Mitigation Using Machine Learning Algorithms in SDN," 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2018, pp. 67-72.

[10] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303-336, 2014.

[12] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A Deep Learning Approach for Network Intrusion Detection System," Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), New York, NY, 2016.

[13] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, 2016.

[14] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017, pp. 1-8.

[15] W. Wang, M. Zhu, and D. Sun, "Malware Traffic Classification Using Convolutional Neural Network for Representation Learning," 2017 International Conference on Information Networking (ICOIN), Da Nang, 2017, pp. 712-717.

[16] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, pp. 108-116, 2018.

[17] L. Xiao, Y. Wan, and S. C. H. Hoi, "Support Vector Machines with Deep Learning for Classification of Intrusion Detection Systems," Neural Computing and Applications, vol. 29, pp. 189-196, 2018.

[18] H. S. Lim, M. Kim, and J. Lee, "DDoS Attack Detection and Mitigation Using Machine Learning Algorithms in SDN," 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2018, pp. 67-72.

DOI : 10.31695/IJERAT.2025.2.3

[19] S. Ryu, Y. Kim, and H. Kim, "CNN-based Intrusion Detection for Security Enhancement in IoT and Smart City Environments," International Journal of Internet Protocol Technology, vol. 12, no. 1, pp. 3-11, 2019.

[20] J. Tang, Y. Wang, and L. Guo, "Deep Learning Approaches for Network Intrusion Detection: A Survey," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3166-3185, March 2021.

[21] Rabbani, Mahdi, Yongli Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, Sajjad Bagheri Baba Ahmadi, and Seyedvalyallah Ayobi. 2021. "A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies" Entropy 23, no. 5: 529.

[22] Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, pp. 436-444, May 2015.

[23] Akyel, Cihan & ARICI, Nursal. (2022). Hair Removal and Lesion Segmentation with FCN8-ResNetC and Image Processing in Images of Skin Cancer. Bilişim Teknolojileri Dergisi. 15. 231-238.

[24] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 1-15.

[25] R. M. Alguliyev, R. M. Aliguliyev, and F. J. Abdullayeva, "An Effective Approach to Big Data Processing for Intrusion Detection," 2018 8th International Conference on Application of Information and Communication Technologies (AICT), Almaty, 2018, pp. 1-7.

[26] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," Applied Sciences, vol. 9, no. 20, pp. 1-23, October 2019.

[27] Chebbi, Imen. (2021). Visual Question Generation from Radiology Images : State Art.

[28] S. Wang, Y. Guo, and W. Huang, "Anomaly Detection in Big Data Using Deep Learning: A Review," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, 2018, pp. 5211-5219.

[29] K. G. Kyriakopoulos, E. Kapassa, and K. Tserpes, "A Comprehensive Survey on Machine Learning Techniques for Intrusion Detection Systems," Journal of Information Security and Applications, vol. 50, 2020.

[30] R. E. Schapire, "Explaining AdaBoost," Empirical Inference: Festschrift in Honor of Vladimir N. Vapnik, pp. 37-52, 2013.

[31] M. S. Islam, S. N. S. Adnan, and M. Z. Hossain, "Deep Learning Based Network Intrusion Detection System for Large-Scale Traffic," Journal of Big Data, vol. 7, no. 1, pp. 1-26, January 2020.

[32] C. Yin, Y. Zhu, and J. Fei, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954-21961, October 2017.

[33] G. Kim, S. Lee, and S. Kim, "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, March 2014.

[34] H. S. Anderson and P. Roth, "EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models," arXiv preprint arXiv:1804.04637, 2018.

[35] N. Moustafa and J. Slay, "The UNSW-NB15 Dataset for Network-based Intrusion Detection Systems," 2015 21st International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Wuhan, 2015, pp. 1-6.

[36] Wang, Cheng, Wei Zhang, Hao Hao, and Huiling Shi. 2024. "Network Traffic Classification Model Based on Spatio-Temporal Feature Extraction" Electronics 13, no. 7: 1236.

[37] Lu, Huakang, Dongmin Huang, Youyi Song, Dazhi Jiang, Teng Zhou, and Jing Qin. 2020. "ST-TrafficNet: A Spatial-Temporal Deep Learning Network for Traffic Forecasting" Electronics 9, no. 9: 1474.

[38] Goodwin, Morten & Halvorsen, Kim & Jiao, Lei & Knausgård, Kristian & Martin, Angela & Moyano, Marta & Oomen, Rebekah & Rasmussen, Jeppe Have & Sørdalen, Tonje & Thorbjørnsen, Susanna. (2022). Unlocking the potential of deep learning for marine ecology: Overview, applications, and outlook. ICES Journal of Marine Science. 79. 10.1093/icesjms/fsab255.

[39] Khan, Habib & Haq, Ijaz & Munsif, Muhammad & Khan, Shafiulllah & Lee, Mi & Khan, Mustaqeem. (2022). Automated Wheat Diseases Classification Framework Using Advanced Machine Learning Technique. Agriculture. 12. 10.3390/agriculture12081226.

DOI : 10.31695/IJERAT.2025.2.3

[40] Hicks SA, Strümke I, Thambawita V, Hammou M, Riegler MA, Halvorsen P, Parasa S. On evaluation metrics for medical applications of artificial intelligence. Sci Rep. 2022 Apr 8;12(1):5979. doi: 10.1038/s41598-022-09954-8. PMID: 35395867; PMCID: PMC8993826.

[41] Qian, Yawei & Zeng, Guang & Pan, Yue & Liu, Yang & Li, Kun. (2021). A Prediction Model for High Risk of Positive RT-PCR Test Results in COVID-19 Patients Discharged From Wuhan Leishenshan Hospital, China. Frontiers in Public Health. 9. 778539. 10.3389/fpubh.2021.778539.

[42] A. Tsantekidis, S. Zafeiridis, and I. Kotsilieris, "Using Deep Learning to Detect Intrusion in IoT Networks," 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, 2019, pp. 1-6.

DOI : 10.31695/IJERAT.2025.2.3