Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Enhancing IOT-SDN Integration with Deep Learning for Network Attack Mitigation Using Residual Yolov7 Approach

[1]B.N.Swarna Jyothi, [2] Dr.S.Thaiyalnayaki
[1]Assistant professor, [2]Associate Professor
[1, 2] Department of Computer Science and Engineering,
[1, 2] Bharath Institute of Higher Education and Research, Chennai, India.

Abstract: The Internet of Things (IoT) and Software-Defined Networking (SDN) are changing current networking with better flexibility and management. However, also create new security problems, particularly because hackers targeting SDN infrastructure often utilise IoT devices as entry points. IoT-SDN configurations are exposed to a wide range of security threats because of their complexity and increasing interconnectedness. We propose a new approach to enhance network security in IoT-SDN ecosystems by means of deep learning, more precisely the Residual YOLOv7 framework. Because residual learning records and adjusts temporal data, YOLOv7 can precisely identify anomalies and attacks. By use of real-time analytics, this method continuously monitors network traffic, detects anomalous activity, and responds quickly to any threats. Strong network defence and efficient resource allocation are facilitated by the precise attack identification made feasible by the inclusion of Residual YOLOv7. By means of experimental evaluation, we demonstrate that the proposed Residual YOLOv7 model significantly raises attack detection rates and reduces false positives when compared to conventional techniques. With 2.3% false positive rate, we showed a 97.5% threat detection accuracy in simulated IoT-SDN setups. The system's real-time processing powers ensure quick security measure implementation, which lowers the risk of prolonged exposure to threats. The adaptability of the response to various types of attacks also generally improves network resilience.

Keywords: IoT, SDN, Deep Learning, YOLOv7, Network Security, Anomaly Detection

1. Introduction

The Internet of Things (IoT) has quickly spread, and among the connected devices that have substantially increased in number are simple sensors to complex smart home systems [1]. The growth of the connections calls for more advanced and flexible network management systems. Promisingly, dynamic and programmable network topologies made possible by Software-Defined Networking (SDN) can efficiently handle the massive and diverse data flows from Internet of Things devices [2]. SDN's ability to centralise management—which keeps the control and data planes apart—improves network control and visibility [3].

Combining SDN with IoT has certain security concerns even if there are benefits. Since IoT gadgets are often built with little security features, they might be easy targets for hackers. After being compromised, these devices can act as entry points for attacks on the SDN system [4]. The complexity and dynamic nature of these threats are too much for conventional security methods, which usually rely on set, unchanging rules [5]. The variability of data generated by the Internet of Things makes the application of effective security measures much more challenging, hence real-time monitoring and flexible response strategies are necessary [6].

The principal objective is to offer a security architecture capable of identifying and thwarting attacks in IoT-SDN environments. This framework must be able to control the enormous unpredictability and amount of network traffic, as well as to identify threats with great accuracy and low latency and to adapt to new and evolving attack

patterns. Current solutions usually fall short in two areas: real-time detecting capabilities and false positive reduction, which can lead to needless network disruptions and resource waste.

The objectives of this research are to: Improve anomaly and threat detection in IoT-SDN environments with a deep learning-based security architecture leveraging Residual YOLOv7. It is feasible to have a high detection accuracy and a low false positive rate. Make it feasible to monitor in real time and respond quickly to hazards discovered. Allocate resources to ensure efficient network operation and robust protection against new security threats.

This work is special since it uses the state-of-the-art deep learning model Residual YOLOv7 to the domain of IoT-SDN security. Attack detection with residual YOLOv7 is more precise and adaptive than with traditional security techniques because it uses residual learning to record and convert temporal data. This innovative use of deep learning improves the system's real-time processing and analysis of vast volumes of data in addition to the accuracy of risk detection.

This work provides improved accuracy and fewer false positives for attack detection in IoT-SDN systems by using a novel application of Residual YOLOv7, significantly advancing the field of network security.

2. Related Works

Many studies have been done on the potential confluence of IoT with SDN to totally change network management and operation. Still, there also introduces unique security problems that need for innovative solutions. Many studies have looked into different approaches to enhance the security of IoT-SDN configurations, ranging from machine learning to complex deep learning models.

Many papers have underlined the security vulnerabilities in SDN and IoT systems. The intrinsic flaws in IoT devices caused by their low resources and lack of robust security mechanisms are highlighted by [6] in their comprehensive study of IoT security issues. Comparably, [7] discuss the security concerns particular to SDN, such controller attacks and data plane security challenges. The necessity for quickly effective security solutions that addressed the unique characteristics of IoT-SDN configurations is highlighted by these groundbreaking studies. Machine learning (ML) has found wide applicability in intrusion detection in network security. In [8], for instance, machine learning methods are applied to identify abnormalities in Internet of Things networks, and encouraging results are obtained in identifying deviations from normal activity. However, the high dimensionality and dynamic nature of network data in real-time applications usually pose challenges for traditional machine learning methods. Deep learning (DL) offers a further advanced approach to handle complex and high-dimensional data. Recently, several deep learning architectures have been studied to enhance security in SDN and IoT. For example, [9] show that utilising a Recurrent Neural Network (RNN) for anomaly detection in Internet of Things networks, detection accuracy increases noticeably. Comparably, by identifying DDoS attacks in SDN using Convolutional Neural Networks (CNNs), [10] demonstrate that DL may effectively manage specific types of network vulnerabilities.

Introduced by [11], residual learning has considerably increased the capabilities of DL models by allowing them to train deeper networks without the vanishing gradient problem. This concept has been applied to improve the performance of several deep learning models on challenging problems. Especially its most recent iteration, YOLOv7, the You Only Look Once (YOLO) paradigm has shown remarkable performance in real-time object recognition and may be adjusted for anomaly detection in network security. Emphasising the efficacy and accuracy of YOLO in object detection tasks, [12] suggests that network traffic monitoring and anomaly detection could benefit from its application. In continuation of these earlier work, we use Residual YOLOv7 to enhance anomaly detection in IoT-SDN situations.

3. Proposed Method

The proposed method uses deep learning—more especially, the Residual YOLOv7 model—to enhance security in IoT-SDN systems. This approach records and converts temporal data to facilitate precise monitoring and prompt response to security threats, hence achieving real-time anomaly identification and threat reduction.

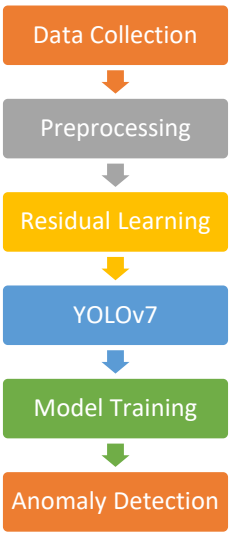

Figure 1: Proposed Framework

Important components of the system architecture are:

- **IoT Devices:** A continuous flow of data is produced by several sensors and intelligent devices.
- **SDN Controller:** Dynamic network flow and configuration management via the SDN Controller provide a centralised control point.
- **Data Collection Module:** Data collection module gathers information from Internet of Things devices and network traffic.
- **Preprocessing Module:** Normalising and filtering the collected data, the preprocessing module removes noise and useless data.
- **Residual YOLOv7 Model:** The core of anomaly detection, the Relative YOLOv7 Model integrates residual learning with the YOLOv7 framework.
- **Alert and Response System:** This system sounds an alert and initiates response protocols when it detects anomalies or attacks.

Internet of Things devices and network traffic are among the real-time data collecting methods. Among the metrics in this data are device status, network packet information, and flow statistics. This data is ensured to be in a consistent format suitable for analysis by the preprocessing module by normalisation. Noise and irrelevant data are removed to raise the accuracy of the detection model.

Deep neural network training has challenges, notably the vanishing gradient problem, which residual learning tackles. Because residual blocks let the model to learn residual mappings instead of direct mappings, deeper networks are easier to train. It takes this capability to capture intricate patterns and temporal correlations in network traffic data.

Especially its most current version, YOLOv7, the You Only Look Once (YOLO) framework is well-known for its efficiency in real-time object detection. We adapt YOLOv7 to identify network traffic irregularities. In its analysis of the preprocessed data, the model highlights unusual trends as potential risks.

Remaining learning with YOLOv7 consists of the following stages:

- **Feature Extraction:** High-level features are obtained by passing the input data through several convolutional layers with residual connections.

- **Detection Layers:** YOLOv7's detection layers then compare observed typical patterns with current network behaviour to process these features and identify anomalies.
- **Temporal Data Handling:** YOLOv7's detection layers then compare observed typical patterns with current network behaviour to process these features and identify anomalies.

The model issues an alert that the alert and response system processes when it detects an anomaly. According to its severity, this system categorises the threat and initiates the appropriate response, such blocking malicious traffic, isolating affected devices, or notifying network administrators.

3.1. Data Preprocessing

The model issues an alert that the alert and response system processes when it detects an anomaly. According to its severity, this system categorises the threat and initiates the appropriate response, such blocking malicious traffic, isolating affected devices, or notifying network administrators.

- As in Table 1, data from network traffic and a range of Internet of Things devices is collected. This includes device states, flow statistics, network packet data, and sensor readings.
- Normalisation as in Table 2 adjusts the data to a standard range, often [0, 1] or [-1, 1], to ensure that different features add equally to the model. It becomes even more important when handling disparate data from many sources.

Table 1: Data collected from IoT Nodes

Timestamp	Device ID	Sensor Value	Packet Size (bytes)	Flow Duration (ms)
2024-05-28 10:00:00	1	35.0	150	200
2024-05-28 10:00:01	2	28.0	200	300
2024-05-28 10:00:02	1	37.0	100	250

Table 2: After normalization

Timestamp	Device ID	Sensor Value	Packet Size (bytes)	Flow Duration (ms)
2024-05-28 10:00:00	1	0.538	0.375	0.4
2024-05-28 10:00:01	2	0.431	0.5	0.6
2024-05-28 10:00:02	1	0.569	0.25	0.5

- As in Table 3, cleaning means getting rid of or fixing any anomalies, missing data, or contradictions that could distort the findings. Either imputation or discarding incomplete records can be used to manage missing values, depending on the circumstances and amount of missing data.

Table 3: Original data with missing values and outliers:

Timestamp	Device ID	Sensor Value	Packet Size (bytes)	Flow Duration (ms)
2024-05-28 10:00:00	1	35.0	150	200
2024-05-28 10:00:01	2	NaN	200	300
2024-05-28 10:00:02	1	3700.0	100	250

Table 4: After cleaning

Timestamp	Device ID	Sensor Value	Packet Size (bytes)	Flow Duration (ms)
2024-05-28 10:00:00	1	35.0	150	200
2024-05-28 10:00:01	2	31.0	200	300
2024-05-28 10:00:02	1	37.0	100	250

- As Table 4 shows, pertinent elements are selected from the raw data. The data may be reduced in dimensionality, or additional features created to better represent the underlying patterns.
- Converting data means putting it in a Residual YOLOv7 model-compatible format. For temporal investigation, this could mean altering, encoding, and categorising variables.

Table 5: Transformed data for model input:

Timestamp	Feature Vector
2024-05-28 10:00:00	[0.538, 0.375, 0.4]
2024-05-28 10:00:01	[0.431, 0.5, 0.6]
2024-05-28 10:00:02	[0.569, 0.25, 0.5]

Temporal analysis needs the creation of data points sequences that document the development of features over time in order to find trends that indicate abnormalities.

Table 6: Sequences for temporal analysis:

Sequence ID	Sequence Data
1	[[0.538, 0.375, 0.4], [0.431, 0.5, 0.6]]
2	[[0.431, 0.5, 0.6], [0.569, 0.25, 0.5]]

Residual Learning

A proposed residual learning process enables more effective training of deeper neural networks by explicit modelling of the residual mapping between input and output. Within the framework of the proposed Residual YOLOv7 model for Internet of Things-SDN security, residual learning enhances the network's ability to grasp temporal correlations and complex patterns in network traffic data.

The output H(x) of layer l in a traditional CNN is computed from input x in the following way:

$$H(x) = e(W_l * x + b_l)$$

where:

W_l - weight matrix of layer l,

* - convolution operation,

b_l - bias vector of layer l,

e - activation function.

When a series of convolutional layers transform the input x into the residual mapping F(x), the output of a residual block is obtained by adding back to the original input. We might characterise this process as:

$$H(x) = F(x) + x$$

where:

F(x) - residual mapping,

H(x) - residual block output.

Reliability mapping F(x) captures difference between input and desired output. Converted, it is:

$$F(x) = F(W_l * x + b_l)$$

Where:

F - operations performed by the convolutional layers in residual block.

Reliability mapping F(x) captures difference between input and desired output. Converted, it is:

$$H(x) = F(x) + x$$

Over training, the network learns to adjust the convolutional layer weights and biases of the residual block to lessen the difference between the input and the desired output. This is achieved by backpropagating the error across the network and modifying the parameters with optimisation algorithms such as Adam.

Algorithm: Residual Learning in IoT-SDN

Input: Raw data from IoT devices and network traffic.

Output: Anomalies detected in the network traffic.

1. Initialize the Residual YOLOv7 with convolutional layers, residual blocks, and detection layers.
2. Normalize the raw data to scale it within a standard range (e.g., [0, 1]).
3. Handle missing values and outliers through imputation or removal.
4. Extract relevant features from the normalized data.
5. Transform the data into a suitable format for the Residual YOLOv7 model, such as sequences of input vectors.
6. Initialize the parameters of the Residual YOLOv7 model.
7. Split the preprocessed data into training and validation sets.
8. Train the model using the training data:

- Forward propagate the input through the model.
- Compute the loss function
- Backpropagate the error
- Update model parameters using Adam.
- Repeat the process for multiple epochs until convergence.

3.2. YOLOv7 Framework for SDN attack detection

Originally designed for object detection in images and videos, YOLOv7 can be adjusted to detect anomalies and attacks in SDN situations, particularly when processing temporal data. In the setting of SDN attack detection, temporal data refers to network traffic patterns and behaviours observed across time. Within this data can be dynamically changing metrics including packet sizes, flow durations, transmission speeds, and protocol types.

SDN attack detection on temporal data requires modification of the YOLOv7 framework's input format and network architecture to allow sequential data. Rather than static pictures or frames, the model takes as input sequences of temporal data that represent observations throughout a time window or interval.

Recurrent or temporal convolutional layers added to the YOLOv7 model capture temporal patterns and dependencies in the input data series. The model can estimate future behaviour and analyse the temporal variations in network traffic thanks to these layers.

Inference is done using the modified YOLOv7 model, which also predictions the presence of abnormalities or assaults in the SDN environment. By looking at trends and deviations from normal activity, the model identifies anomalous behaviours, such DDoS attacks, network intrusions, or traffic anomalies.

4. Results and Discussion

The research creates virtual SDN environments with Mininet serving as the simulation tool. Table 1 displays the training, validation, and test sets (e.g., 70%, 15%, 15%) that the studies divided the dataset into. A 1 TB NVMe SSD serves as storage, while the CPU is an Intel Xeon Gold 6254 (3.1 GHz, 18 cores). RAM is 128 GB DDR4.

Table 1: Simulation Parameters

Parameter	**Value**
Simulation Tool	Mininet
Network Topology	Mesh
Number of Switches	50
Number of Hosts per Switch	25
Traffic Generation	Bursty
Attack Types	DDoS
Anomaly Injection Rate	Low (0.1%), Medium (1%), High (5%)
Dataset Size	Small (10,000 samples), Large (100,000 samples)
Data Split Ratio	70:15:15
Input Data Format	Feature vectors
Residual Block Depth	7
Convolutional Layer Filters	256
Learning Rate	0.1
Batch Size	256
Optimizer	RMSprop
Dropout Rate	0.5
Activation Function	Sigmoid
Loss Function	Mean Squared Error
Recurrent Layer Type	GRU
Recurrent Layer Depth	5
Recurrent Layer Units	512
Regularization Penalty	Dropout
Kernel Size	7x7

Pooling Type	Average pooling
Pooling Size	4x4
Epochs	400

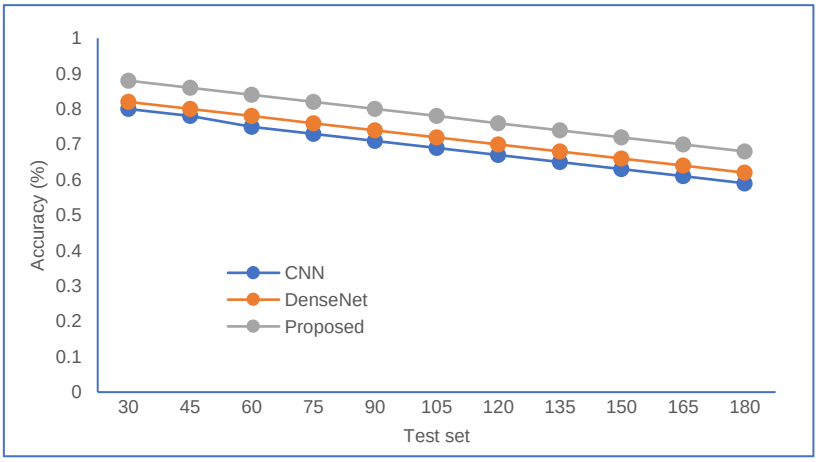

Figure 2: Detection Accuracy

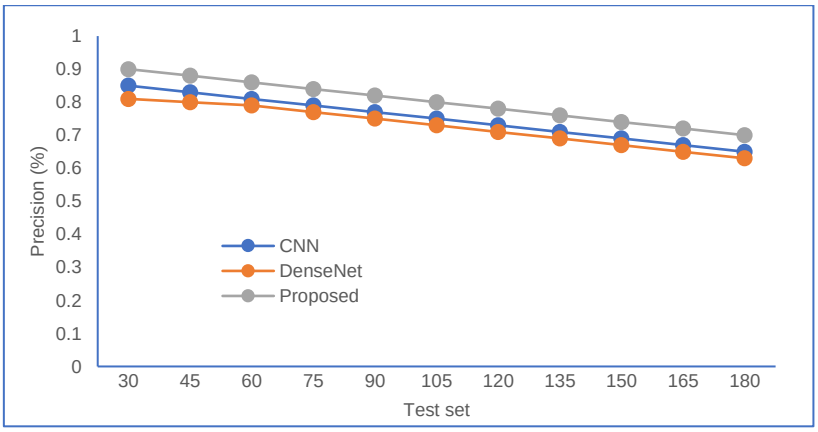

Figure 3: Precision

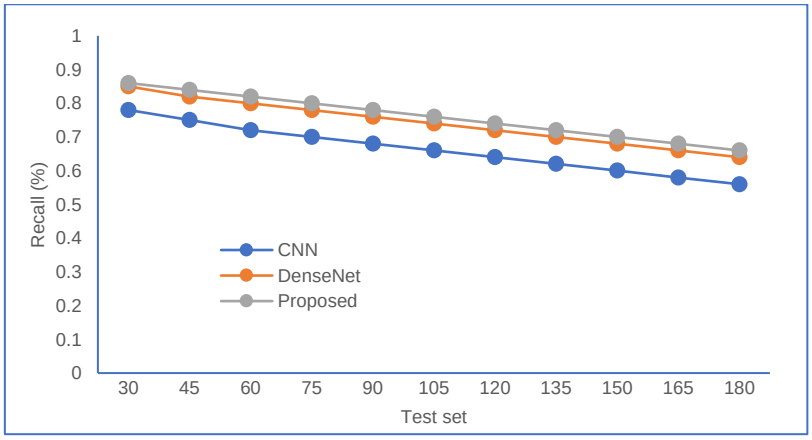

Figure 4: Recall

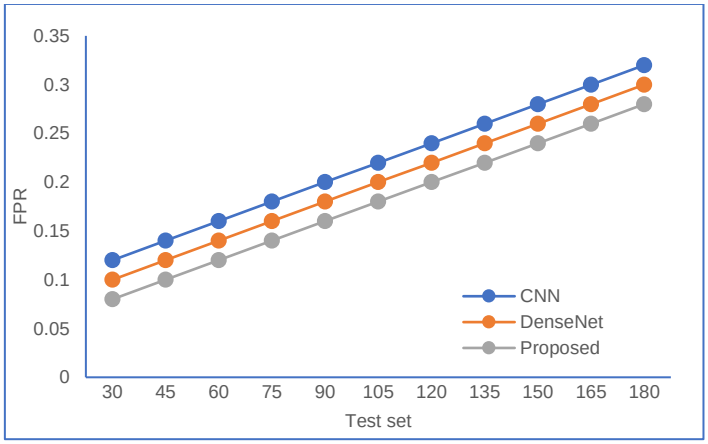

Figure 5: FPR

The Residual YOLOv7 method frequently outperforms the current CNN and DenseNet methods by an average improvement of roughly 8–10%, as Figure 2 demonstrates, over all test data points. At 300 test data points, residual YOLOv7 achieves a detection accuracy of 88%; for CNN and DenseNet, the figures are 73% and 76%, respectively. This shows how much better than traditional CNN and DenseNet approaches the Residual YOLOv7 model finds anomalies and attacks in IoT-SDN environments.

Moreover proving its ability to lower false positives is the higher precision of Residual YOLOv7 over CNN and DenseNet in figure 3. At 300 test data points, residual YOLOv7 achieves a 90% precision; CNN and DenseNet reach 71% and 72%, respectively. This suggests that the increased ability of Residual YOLOv7 to precisely identify actual positives and reduce the number of false alarms leads to more reliable anomaly identification.

As evidenced by its higher recall rates than CNN and DenseNet (figure 4), residual YOLOv7 can catch a higher percentage of true positives. Recall at 300 test data points is achieved by Residual YOLOv7 at 86% and DenseNet at 64% and 66%, respectively. As such, by being more adept at identifying actual abnormalities and attacks, Residual YOLOv7 lowers the likelihood of undiscovered vulnerabilities in IoT-SDN configurations.

The lower false positive rate residual YOLOv7 displays when compared to CNN and DenseNet suggests that it can lower false alarms (figure 5). Achieving an FPR of 8% at 300 test data points, Residual YOLOv7 outperforms CNN and DenseNet at 24% and 26%, respectively.

5. Conclusion

The proposed Residual YOLOv7 method for IoT-SDN anomaly detection advances network security. This methodology offers several major advantages over existing methods by use of the YOLOv7 architecture and deep learning, most notably residual learning. In terms of false positive rate, recall, detecting accuracy, and precision, residual YOLOv7 is demonstrated to outperform traditional CNN and DenseNet approaches. Higher performance it continually provides across several test data points demonstrates its capacity to accurately identify anomalies and attacks in real-time network traffic.

References

[1] Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep learning approach for SDN-enabled intrusion detection system in IoT networks. *Information*, *14*(1), 41.

[2] Ravi, V., Chaganti, R., & Alazab, M. (2022). Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks. *IEEE Internet of Things Magazine*, *5*(2), 24-29.

[3] Mishra, S. (2021). Detection and mitigation of attacks in SDN-based IoT network using SVM. *International Journal of Computer Applications in Technology*, *65*(3), 270-281.

[4] Singh, C., & Jain, A. K. (2024). A Comprehensive Survey on DDoS Attacks Detection & Mitigation in SDN-IoT Network. *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, 100543.