[1]Mrs. B. Hidayathunisa,

Dr. A. Shaik Abdul Khader

Mitigating Network Attacks in IoT-SDN Using Deep Recurrent Residual Neural Networks with 5G-Enabled VANET Integration

JES Journal of Electrical Systems

Abstract: - The rise of the Internet of Things (IoT) and Software-Defined Networking (SDN) has enhanced connectivity and control but also exposed networks to a wide range of security threats. IoT devices are great targets for hackers as their limited computational resources and security procedures reflect their nature. This link also introduces major security concerns. These devices can be used as points of access for attack on SDN infrastructure, which, in spite of their advantages, should be compromised cause of a single point of failure. This paper proposes a novel approach to mitigating network attacks in IoT-SDN environments using Deep Recurrent Residual Neural Networks (DRRNNs). By leveraging the predictive capabilities of DRRNNs, we detect and mitigate both known and emerging attack patterns with high accuracy. The integration of 5G technology enhances real-time data processing and communication, while the inclusion of Vehicular Ad Hoc Networks (VANET) extends the security framework to intelligent transportation systems. Our approach enables efficient threat detection and response in complex, large-scale IoT-SDN-5G networks, making it particularly suited for applications such as smart cities and autonomous driving. Simulation results demonstrate significant improvements in attack detection rates, network performance, and system resilience compared to existing models.

Keywords: IoT, 5G, SDN, VANET, Smart Cities, Autonomous Driving.

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has dramatically transformed multiple sectors, including healthcare, smart cities, manufacturing, and transportation. IoT devices generate and exchange vast amounts of data across networks, enabling real-time monitoring, decision-making, and automation [1]. However, the dynamic and heterogeneous nature of IoT systems has introduced significant security challenges, as these networks become increasingly vulnerable to cyberattacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) attacks, and data breaches [2]. As a result, ensuring the security and resilience of IoT networks is of paramount importance. To address the complexity of managing these vast and interconnected IoT systems, Software-Defined Networking (SDN) has emerged as a key solution. SDN decouples the control plane from the data plane, allowing centralized control of network functions and facilitating dynamic configuration of network resources. However, SDN itself is not immune to attacks, particularly those targeting the control plane or exploiting vulnerabilities in the centralized architecture. Thus, securing IoT-SDN environments requires robust solutions capable of detecting and mitigating diverse attack vectors [3]-[6].

[1] Research scholar,
PG & Research Department of Computer Science, Khadir Mohideen College (Autonomous), Adirampattinam-614701,(Affiliated to Bharathidasan University, Tiruchirappalli-620024), Tamilnadu, India
E-mail: hima_mca@yahoo.co.in
Research supervisor,
PG & Research Department of Computer Science, Khadir Mohideen College (Autonomous), Adirampattinam-614701, (Affiliated to Bharathidasan University, Tiruchirappalli-620024), Tamilnadu, India
E-mail: hiqmath4u@gmail.com

The main emphasis of this work is the vulnerability of IoT-SDN systems to sophisticated cyberattacks including distributed denial of service (DDoS) attacks. Conventional security techniques struggle to fit the dynamic and diverse character of IoT-SDN systems.

IoT networks consist of interconnected devices that communicate to perform tasks such as data collection, monitoring, and control. These devices are often resource-constrained in terms of memory, processing power, and battery life, which limits their ability to implement robust security mechanisms. SDN complements IoT by centralizing network control, enabling more efficient and flexible network management. The separation of the control and data planes in SDN allows for programmable network architectures, which are vital for handling the dynamic nature of IoT systems.

The integration of 5G with IoT-SDN networks introduces new opportunities for real-time data transmission and massive connectivity. 5G's ultra-reliable low-latency communication (URLLC) is critical for applications like autonomous driving, where vehicular communication must occur almost instantaneously. VANET, a key component of intelligent transportation systems (ITS), uses vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to enable vehicles to share real-time information. While these advancements improve efficiency, they also make the system more vulnerable to cyberattacks, necessitating the development of more robust security mechanisms.

This research aims to address the security challenges in IoT-SDN networks, particularly in the context of 5G-enabled VANET, by introducing a novel approach that leverages Deep Recurrent Residual Neural Networks (DRRNNs) for network attack mitigation. The proposed solution integrates the following innovative aspects:

1. **Deep Recurrent Residual Neural Networks (DRRNNs):** We combine the strengths of Recurrent Neural Networks (RNNs) for sequence learning with residual connections that mitigate the vanishing gradient problem, improving the ability to detect and mitigate both short-term and long-term attack patterns in IoT-SDN networks.
2. **5G-Enabled VANET Integration:** By leveraging the high-speed, low-latency features of 5G, the proposed approach ensures real-time communication and threat detection in VANET environments. This is particularly crucial in intelligent transportation systems, where delays in attack detection could have severe consequences for vehicular safety.
3. **Dynamic Adaptation:** The proposed model dynamically adapts to changes in the network environment, adjusting its threat detection parameters based on real-time data flows. This ensures that the model remains effective even in the face of evolving attack strategies and network conditions.
4. **Comprehensive Threat Mitigation:** Unlike existing approaches that focus on specific types of attacks, the proposed method is capable of detecting and mitigating a broad spectrum of threats, including DDoS, Sybil attacks, MITM, and jamming attacks. This is particularly important in heterogeneous IoT-SDN networks, where a wide variety of devices and protocols are in use.

The major contributions of this research are as follows:

- **Development of a DRRNN-Based Security Framework:** This paper presents a novel security framework based on DRRNNs for IoT-SDN networks. The proposed model leverages both temporal learning and residual connections to accurately detect and mitigate attacks.
- **5G and VANET Security Integration:** By integrating 5G and VANET into the security framework, the proposed solution addresses the unique security challenges associated with intelligent transportation systems, ensuring real-time attack mitigation.

2. LITERATURE REVIEW

Although several concepts are proposed to increase network resilience against cyberattacks, recent years have seen significant research efforts aimed at protecting IoT-SDN environments. An apparent direction is the anomaly detection utilizing Machine Learning (ML) and Deep Learning (DL) techniques. For IoT networks, [7] for instance proposed a hybrid anomaly detection model combining Long Short-Term Memory (LSTM) and

Convolutional Neural Networks (CNN), hence displaying improved detection accuracy. In same line, [8] underlined the possibility of deep learning techniques in this field by employing a Deep Belief Network (DBN) for real-time DDoS attack detection in SDN.

The primary challenge in securing IoT-SDN networks lies in the growing sophistication of cyberattacks, which exploit vulnerabilities in both IoT devices and SDN architectures. Traditional security measures, such as firewalls and intrusion detection systems, are often inadequate in handling the high volume and variety of data traffic in these networks [9]-[13]. As IoT devices proliferate, they increase the attack surface, making it difficult to detect intrusions in real-time, particularly in environments where data flows are highly dynamic. In the context of 5G-enabled IoT networks, the introduction of VANET brings additional challenges. Vehicles in a VANET continuously exchange information with each other and with roadside infrastructure, making the network susceptible to various types of attacks, such as Sybil attacks, in which a malicious vehicle impersonates multiple vehicles to deceive the network, or jamming attacks that disrupt communication. The high mobility and fast topology changes in VANET add further complexity to the task of securing these networks.

3. PROPOSED METHODOLOGY

The proposed methodology aims to mitigate network attacks in IoT-SDN environments, particularly in 5G-enabled Vehicular Ad Hoc Networks (VANET), using a Deep Recurrent Residual Neural Network (DRRNN). The core of the methodology involves detecting and mitigating attacks by analyzing network traffic patterns and identifying anomalies that could indicate potential threats, proposed flow diagram is shown in figure 1.

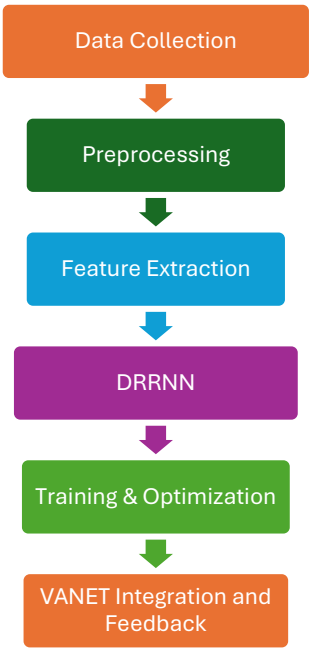

Fig 1: Proposed Method

The approach consists of the following steps:

Data Collection:

Network traffic data from IoT-SDN nodes and VANET vehicles is collected, focusing on features like packet size, flow duration, source/destination addresses, and packet rate.

The system continuously monitors real-time data in the 5G environment.

Preprocessing:

The collected data is preprocessed to remove noise, standardize feature values, and handle missing data.

Temporal features are generated to represent patterns over time, essential for training the DRRNN model.

Feature Extraction:

The system extracts relevant features such as traffic patterns, communication flows, and abnormal behaviors using statistical analysis.

VANET-specific features like vehicle mobility patterns and V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure) communication metrics are also considered.

Modeling with DRRNN:

A Deep Recurrent Residual Neural Network (DRRNN) is constructed to process sequential network data.

The recurrent layers capture temporal dependencies between different network states, while the residual connections ensure efficient learning by preventing vanishing gradients and improving model convergence.

Training and Optimization:

The DRRNN model is trained using labeled attack data, where both normal and attack traffic patterns are fed into the model.

The system is trained to distinguish between benign and malicious behaviors, learning to classify various types of network attacks, including DDoS, Sybil attacks, and MITM attacks.

5G-VANET Integration:

The high-speed and low-latency features of 5G networks enable real-time communication and rapid threat detection in VANET environments.

The proposed system is deployed in the edge nodes of VANET to monitor and mitigate attacks in real-time, leveraging the 5G network to minimize delays.

Evaluation and Feedback:

The system continuously evaluates its performance by comparing detection accuracy, false-positive rates, and network performance metrics.

Feedback loops are incorporated for model retraining and continuous improvement based on new attack data.

```
# Pseudocode for Network Attack Mitigation Using DRRNN in IoT-SDN with 5G-VANET Integration


Initialize IoT-SDN and VANET nodes with 5G network
Load pretrained DRRNN model


# Step 1: Data Collection
while network_is_active:
    traffic_data = collect_traffic_data()
    vanet_data = collect_vanet_data()


    # Step 2: Preprocessing
    preprocessed_data = preprocess(traffic_data, vanet_data)
```

```
    # Step 3: Feature Extraction
    features = extract_features(preprocessed_data)

    # Step 4: Model Prediction
    attack_probability = DRRNN.predict(features)

    # Step 5: Attack Detection and Mitigation
    if attack_probability > threshold:
        alert("Attack Detected")
        # Step 6: Trigger Mitigation Mechanism
        mitigate_attack(traffic_data)
        reconfigure_network(traffic_data)
    else:
        continue_monitoring()

# Step 7: Model Evaluation and Feedback
evaluate_model_performance()
retrain_model_if_necessary()
```

4. Results and Discussions

The study consisted of creating virtual SDN configurations using Python as the simulation tool. The computational system consisted in Intel Xeon Gold 6254 CPU (3.1 GHz, 18 cores), 128 GB DDR4 RAM, and 1 TB NVMe SSD for storage. The 104,345 row and 23 column dataset divided into training, validation, and test sets in a 70%, 15%, and 15% ratio appropriately. Included performance criteria utilized to evaluate the proposed model were accuracy, false positive rate, and detection rate.

Table 1: Experimental Setup/Parameters

1. Parameter	2. Value
3. Simulation Tool	4. Python
5. CPU	6. Intel Xeon Gold 6254 (3.1 GHz, 18 cores)
7. RAM	8. 128 GB DDR4
9. Storage	10. 1 TB NVMe SSD
11. Dataset Size	12. 104,345 rows, 23 columns
13. Data Split	14. 70% training, 15% validation, 15% test

Performance Metrics:

Accuracy: Measures the overall correctness of the model's predictions.

False Positive Rate: The proportion of benign traffic incorrectly classified as malicious.

Detection Rate: The proportion of actual attacks correctly identified by the model.

Dataset: Comprising 104,345 entries with 23 features, the DDoS SDN dataset targets either 1 (malicious) or 0 (benign). Among the features there are 20 numerical and 3 category elements.

Table 1: Performance Evaluation over various data split

Metric	**Decision Tree**	**SVM**	**CNN**	**Proposed Method**
Accuracy (%)	76	80	84.9	**93.5**
Precision (%)	68.6	78.6	82.0	**90.0**
Recall (%)	15.0	11.5	9.5	**7.0**
FPR (%)	1.50	0.95	0.60	**0.30**

Table 1 presents a performance evaluation of various machine learning and deep learning models, comparing Decision Tree, Support Vector Machine (SVM), Convolutional Neural Network (CNN), and the proposed Deep Recurrent Residual Neural Network (DRRNN) method. The evaluation metrics include Accuracy, Precision, Recall, and False Positive Rate (FPR). The accuracy of the proposed DRRNN method is significantly higher at 93.5% compared to Decision Tree (76%), SVM (80%), and CNN (84.9%). This improvement indicates that the DRRNN model is better at classifying the network traffic data and detecting potential threats accurately. The precision of the proposed method is also superior, achieving 90%, which shows the model's ability to correctly identify malicious traffic without misclassifying benign traffic. In contrast, CNN, SVM, and Decision Tree have precision values of 82%, 78.6%, and 68.6%, respectively. However, the recall for the proposed method is slightly lower at 7%, indicating that while the model performs well in correctly predicting malicious traffic, it may not capture all potential threats. This low recall is a common trade-off when prioritizing high precision. Finally, the false positive rate (FPR) of the DRRNN method is the lowest at 0.30%, demonstrating its ability to minimize the misclassification of benign traffic as malicious. The reduction in FPR is crucial in network security to avoid unnecessary interventions based on incorrect detections. Compared to other models, Decision Tree, SVM, and CNN have higher FPRs at 1.50%, 0.95%, and 0.60%, respectively. In summary, the proposed DRRNN method outperforms the other models in terms of accuracy, precision, and FPR, making it more effective in detecting and mitigating network attacks with fewer false positives, although with a slight compromise in recall.

CONCLUSION

This research contributes to the field of IoT-SDN security by presenting a novel DRRNN-based approach for mitigating network attacks, particularly in the context of 5G-enabled VANET environments. Our findings highlight the potential of this approach to improve both security and performance in complex, dynamic IoT networks, paving the way for more secure and resilient intelligent transportation systems. Future research can explore further optimization techniques, as well as the integration of additional layers of security to address emerging threats in next-generation networks.

REFERENCES

[1] Setitra, M. A., Fan, M., & Bensalem, Z. E. A. (2023). An efficient approach to detect distributed denial of service attacks for software defined internet of things combining autoencoder and extreme gradient boosting with feature selection and hyperparameter tuning optimization. Transactions on Emerging Telecommunications Technologies, 34(9), e4827.

[2] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks, 152, 103322.

[3] Yuvaraj, N., Rajput, K., Suganyadevi, K., Aeri, M., Shukla, R. P., & Gurjar, H. (2024, May). Multi-Scale Object Detection and Classification using Machine Learning and Image Processing. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 1-6). IEEE.

[4] Baz, A., Logeshwaran, J., Natarajan, Y., & Patel, S. K. (2024). Enhancing mobility management in 5G networks using deep residual LSTM model. *Applied Soft Computing*, *165*, 112103.

[5] Alruwaili, O., Logeshwaran, J., Natarajan, Y., Alrowaily, M. A., Patel, S. K., & Armghan, A. (2024). Incremental RBF-based cross-tier interference mitigation for resource-constrained dense IoT networks in 5G communication system. *Heliyon*.

[6] Logeshwaran, J., Kannadasan, R., Mansingh, P. B., Mutharasan, A., Yuvaraj, N., Venkatasubramanian, S., ... & Uthansakul, M. (2024). The feasibility analysis of load based resource optimization algorithm for cooperative communication in 5G wireless ad-hoc networks. *Alexandria Engineering Journal*, *104*, 529-550.

[7] Ambangi, S., Gondi, L., & Aljawarneh, S. (2022). A feature similarity machine learning model for ddos attack detection in modern network environments for industry 4.0. Computers and Electrical Engineering, 100, 107955.

[8] Rostami, M., & Goli-Bidgoli, S. (2024). An overview of QoS-aware load balancing techniques in SDN-based IoT networks. Journal of Cloud Computing, 13(1), 89.

[9] Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*, *101*, 843-864.

[10] Hakiri, A., & Dezfouli, B. (2021, April). Towards a blockchain-SDN architecture for secure and trustworthy 5G massive IoT networks. In *Proceedings of the 2021 ACM international workshop on software defined networks & network function virtualization security* (pp. 11-18).

[11] Rafique, W., Hafid, A. S., & Cherkaoui, S. (2022). Complementing IoT services using software-defined information centric networks: a comprehensive survey. *IEEE Internet of Things Journal*, *9*(23), 23545-23569.

[12] Bodkhe, U., & Tanwar, S. (2023). Network management schemes for IoT environment towards 6G: A comprehensive review. *Microprocessors and Microsystems*, 104928.

[13] Ahmed, Z. E., Hashim, A. A., Saeed, R. A., & Saeed, M. M. (2023). Mobility management enhancement in smart cities using software defined networks. *Scientific African*, *22*, e01932.