Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/BA08.20250155
Published: December 20, 2025

Classification of AI-based Attack Detection for 6G Network Slices

Mithun Pal and Fahrin Rahman
Department of Electrical and Electronic Engineering
European University of Bangladesh
Dhaka, Bangladesh
mmithunpal101@gmail.com, fahrin@eub.edu.bd

Abstract

With the advent of 6G technology, communication networks are predicted to enable ultra-high data transmission rates, extremely low latency and highly reliable connectivity. A key enabler of these innovations is network slicing, which allows numerous virtualized slices to coexist on the same physical infrastructure, each customized to specific service requirements. However, this flexibility also presents new security concerns. In this paper, we propose a slice-specific attack classification system that employs artificial intelligence to detect important threats, including spoofing, distributed denial of service (DDoS), and eavesdropping. Using a balanced dataset of slice kinds (Ultra-High-Speed, Autonomous, IoT) and attack categories, we train and test machine learning and deep learning models to analyze traffic patterns and classify attacks. Our results show both the potential and limitations of classical classifiers such as Decision Trees and Random Forests, which produce high training accuracy but suffer from overfitting and poor test performance. These findings underscore the future demand for lightweight, adaptive, and federated learning techniques to offer scalable and real-time security. Overall, our research contributes to the design of secure 6G slice architectures by providing a baseline foundation for attack detection and a path for future research in adaptive AI-based defense systems.

Keywords
AI-based Attack Detection, Network Slicing, Network Security, Privacy, 6G Network.

1. Introduction
The creation of 6G networks signals a new era in telecommunications, enabling ultra-high data rates, greater reliability, and the capacity to handle different applications. At the basis of the 6G architecture lies the concept of network slicing (Moreira and Silva, 2024), which enables operators to develop customized virtual networks tailored to specific service requirements. However, this flexibility also poses substantial security issues, as each slice is exposed to distinct sorts of cyber-attacks. Ensuring secure slice operations demands complex mechanisms capable of evaluating vast amounts of data with minimal delay. Artificial intelligence (AI), with its ability to learn from data and adapt to dynamic circumstances (Eziama et al., 2025), has emerged as a viable strategy for detecting and mitigating cyber threats. We have concentrated in this research on the classification of AI-based data-driven attack detection for 6G network slices. Specifically, we have categorized methods of artificial intelligence based on their effectiveness in identifying attacks, performance metrics, and real-time applicability.

1.1 Objectives
Our research aims at AI-based detection and classification of attacks on 6G network slices. Our goal is to develop a reliable model to detect threats in real-time, thereby increasing the security and performance of 6G networks. Our

work will provide more protection in future 6G network slices.

2. Literature Review

2.1 Background

The 6G network includes a revolution in the telecommunication system that embeds network slicing in its original architecture (Ren et al., 2022). Although slicing enables customized virtual networks according to the demand for different types of services, this flexibility creates new types of security risks. Each slice faces multi-dimensional cyber threats for example spoofing, distributed denial of service (DDoS), man-in-the-middle (MITM), and cross-slice attacks (De Alwis et al., 2023). We see recent works also emphasize that deep learning can provide adaptive protection against evolving threats, underscoring the importance of slice-aware security frameworks (Gupta et al., 2023).

2.2 Existing Research

Over the past decade, researchers have experimented with various machine learning (ML) and deep learning (DL) methods to detect attacks. For example, Support Vector Machine (SVM) and Random Forest (RF) have been used for DoS detection, achieving moderate accuracy, but they have limitations in real-time applications. Recent studies have used Deep Neural Network (DNN), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) models, which gained high accuracy in identifying threats (Eziama et al., 2025). We also see that (Saeed et al., 2023) proposed a hybrid ML approach combining correlation feature selection with RF and SVM, achieving 99.9% accuracy on the CICDDOS2019 dataset. Similarly, (Gupta et al., 2023) introduced a CNN-based framework using heatmap transformations of traffic data and demonstrated robust detection of DoS, probe, and Sybil attacks in 6G networks.

2.3 Limitations of Current Approaches

Following the initial commercial deployments of 5G networks, both industry and academic institutions have begun work on the design, capabilities, and requirements of 6G mobile networks. The 6G vision presupposes deep inclusion of artificial intelligence (AI) in the network, resulting in a move from “connected things” to “connected intelligence”, and provision of global and instant connectivity to a far higher number of devices than in the previous generation (Kukliński et al., 2021; Asensio-Garriga et al., 2024; Cáceres-Hidalgo & Avila-Pesantez, 2021). However, most current IDS approaches remain generic and fail to address slice-specific threats, limiting their scalability and adaptability.

2.4 Research Gaps and Future Directions

AI can play a vital role in protecting 6G network slicing, but several gaps exist. Future research should stress lightweight models, federated learning, online learning, and real-time processing to construct scalable, adaptive, and efficient attack detection systems. Each data type and security slice presented in this research will strengthen 6G networks and assure confidentiality (Moreira & Silva, 2024). Building on prior works (Saeed et al., 2023; Gupta et al., 2023), our study contributes a slice-specific attack classification framework, establishing a baseline for secure 6G slice architectures and offering a roadmap for adaptive AI-driven defense systems.

3. Methods

The goal of this study is to categorize AI-based attacks for 6G network slicing. We have designed to detect various cyber-attacks through AI, especially on the application of machine learning (ML) and Deep Learning (DL) models.

3.1 Data Collection

In this paper, we used a dataset obtained from Kaggle. Using this dataset, we simulated network characteristics and attack types within 6G network slices. The key features include:

- **Network Slice Types:** From the dataset we get, Ultra-high-speed, autonomous, etc.
- **Traffic Load:** From the dataset we get, high, medium, and low.
- **Performance Metrics:** We get, Packet loss rate, latency, data rate, etc.
- **Attack Types:** From our dataset, we get, Spoofing, Distributed Denial of Service (DDoS), Eavesdropping, etc.

3.2 Attack Classification

For 6G network attacking slices, we categorized the relevant cyber-attacks as follows:

- **Spoofing:** This attacker is attacked by a valid user or device disguised.

- **DDoS:** This attack overloads the network to disrupt the service.
- **Eavesdropping:** This attack contains unauthorized interference of network data while traveling between devices to get access to sensitive information.

3.3 6G Network Security Slicing Process

- **Security Requirements:** We need to ensure the reliability and availability of intelligent services to deal with the AI-powered protection system, physical level protection, strong network slicing protection, and new attack vectors to identify real-time threats.
- **Slice Creation:** Security slices need to be created.
- **Slice Isolation:** Separate slices to maintain network security.
- **Security Policy Enforcement:** Security policies must be enforced.
- **Security Monitoring:** Security needs to be monitored and problems solved (Figure 1).

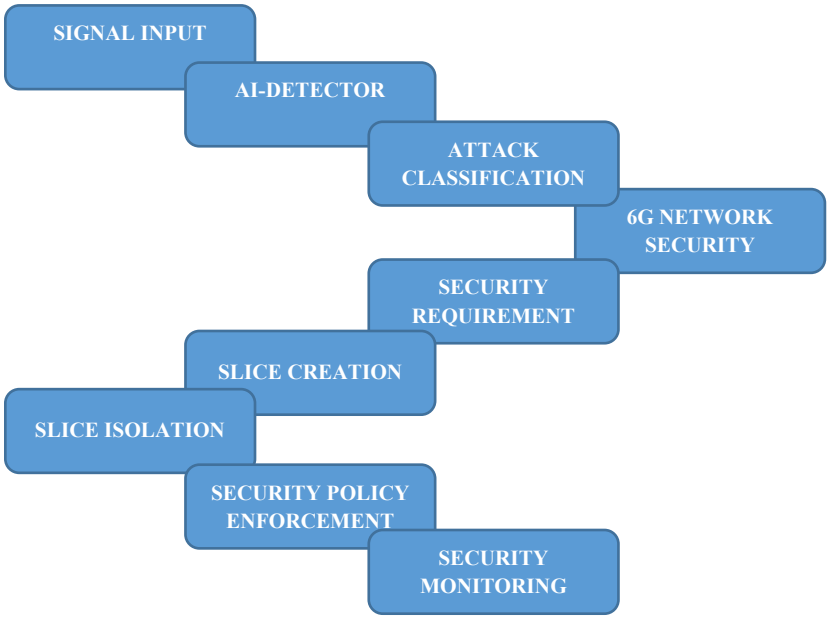

Figure 1. 6G Network Security Slicing Process

4. Results and Discussion

From our dataset, we have gotten some different types of bar graphs.

A. Distribution of Attack Types

The frequency of each attack on the dataset is calculated in the frequency Figure 2. There are three different types of attacks on the dataset. The bar graph below shows that there are 338 instances of spoofing attacks in the dataset, 347

instances of DDOS attacks, and 315 instances of attacks on Eavesdropping. It shows that the dataset is evenly distributed among the types of attack, which is convenient for training machine learning models because no one type of attack is excessively dominant.

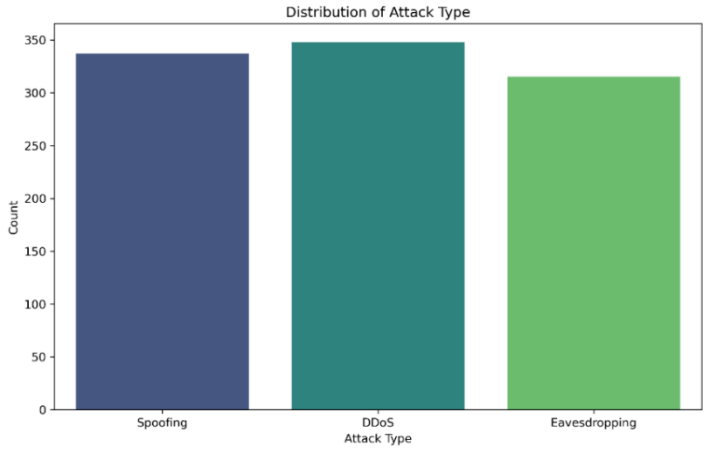

Figure. 2**.** Distribution of Attack Type

B. Distribution of Slice Types

The frequency of each slice on the dataset is calculated in the frequency Figure 3. There are three different types of slices in the dataset. The bar graph below shows that there are 321 instances of Ultra-High-Speed slice in our dataset, 354 instances of Autonomous slice, and 325 instances of slice on the IoT. It shows that the dataset is evenly distributed among the types of slices, which is convenient for training machine learning models because no one type of slice is excessively dominant (Figure 3).

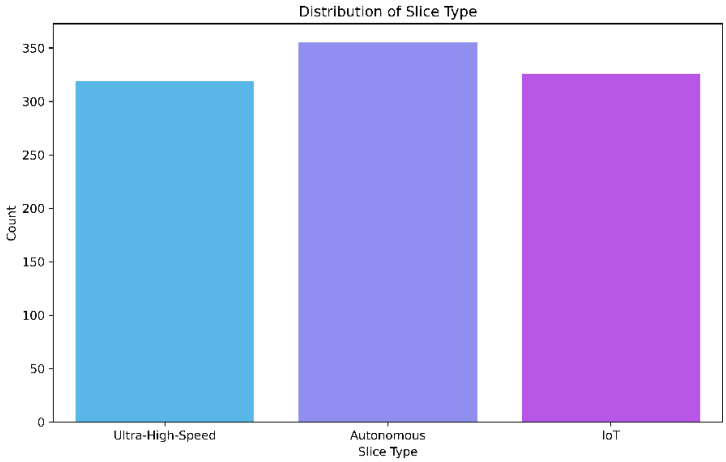

Figure 3. Distribution of Slice Type

C. Heatmap of Slice Type vs Attack Type

To analyze the distribution of cyberattacks across 6G network slices, we constructed a heatmap based on frequency counts of three major attack types (DDoS, Eavesdropping, and Spoofing) across three slice categories (Autonomous, IoT, and Ultra-High-Speed). As shown in Figure:4, Spoofing attacks were most frequent in Autonomous slices (125 attacks), whereas Eavesdropping was least frequent in Ultra-High-Speed slices (88 attacks). These results show that slice-specific security models will be needed to protect against attackers (Figure 4).

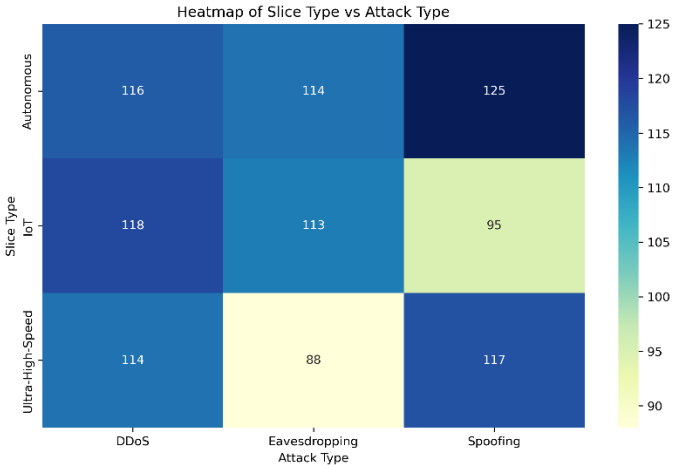

Figure 4. Heatmap of Slice Type vs Attack Type

D. Graph of Accuracy, Precision, Recall, F1 Score, and Execution Time for DecisionTreeClassifier

In this case, we have used 10% of the data as test data, and the other 90% data has been classified as trained data. From Figure 5 as depth increases, train accuracy curve (solid circle blue) rapidly rises, approaching 0.68 at depth 9. At all depths, the test accuracy (dashed x blue) is flat, ranging from 0.33. Even though the tree is getting deeper, there isn't any noticeable improvement. With depth increases, Train Precision, Recall, and F1 Score overlap (solid green, orange, and pink) and gradually approach perfect scores (>0.68). This demonstrates that the model is retaining the training data. With nearly no upward trend, test precision, recall, and F1 Score (dashed green, orange, and pink) remain flat and very near 0.32–0.33. Finally, in depths 5.5–6, Execution Time (red) peaks at about 0.015 seconds, increasing with depth (Figure 5).

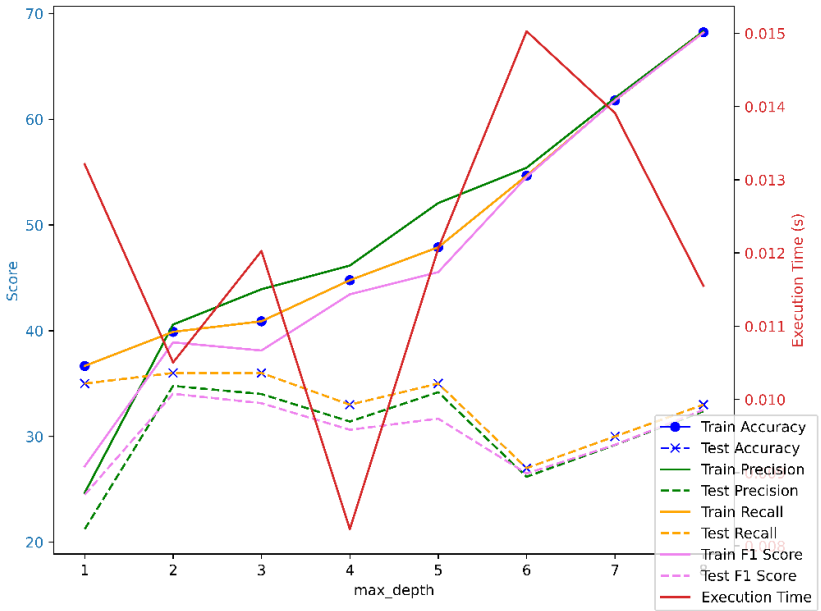

Figure 5. Graph of Accuracy, Precision, Recall, F1 Score, and Execution Time for DecisionTreeClassifier

E. Graph of Accuracy, Precision, Recall, F1 Score, and Execution Time for RandomForestClassifier

In this case, we have used 10% of the data as test data, and the remaining data were classified as trained data. From Figure 6 as depth increases, train accuracy curve (solid circle blue) flat rises, approaching 99.98% at depth 20. This indicates how well the model fits the training with dataset. At all depths, the test accuracy (dashed x blue) ranges from 36.5% to 37%. Even though the tree is getting deeper, there isn't any noticeable improvement. With depth increases, Train Precision, Recall, and F1 Score are overlap each other (solid green, orange, and pink) and gradually approach perfect scores (>0.98). This demonstrates that the model is retaining the training data. With nearly no upward trend,

test precision, recall, and F1 (dashed green, orange, and pink) remain flat and very near 0.35 to 0.37. At depths 19-20, Execution Time (red) peaks at about 0.21 seconds, increasing with depth (Table 1).

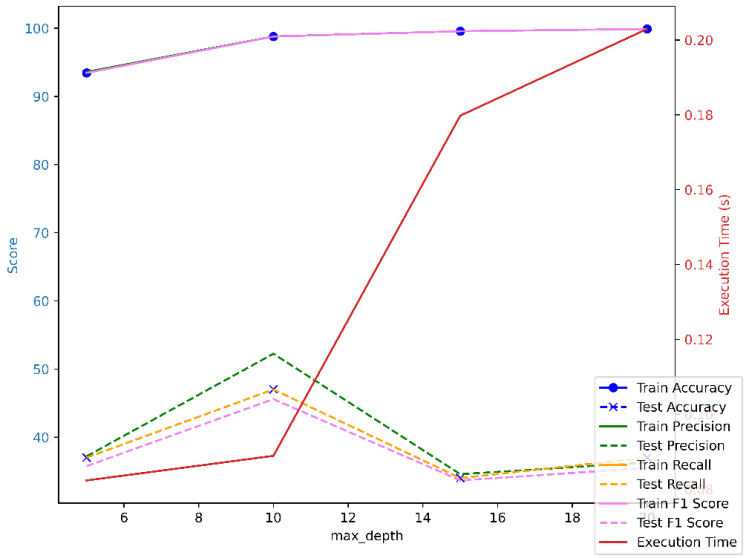

Figure 6. Graph of Accuracy, Precision, Recall, F1 Score, and Execution Time for RandomForestClassifier

Table 1. Performance Evaluation of ML Models with Execution Time

Model Name	Train Accuracy	Test Accuracy	Train Precision	Test Precision	Train Recall	Test Recall	Train F1 Score	Test F1 Score	Execution Time
DecisionTreeClassifier	68.22%	33.00%	68.32%	32.38%	68.22%	33.00%	68.18%	32.50%	0.0116 seconds
RandomForestClassifier	99.89%	37.00%	99.89%	36.29%	99.89%	37.00%	99.89%	35.49%	0.2029 seconds

Overall, the results demonstrate that AI-based attack detection models hold strong potential for enhancing the security of 6G network slices. Our study also reinforces the importance of security slice architecture, where slice isolation, policy enforcement, and continuous monitoring are essential for ensuring confidentiality, integrity, and availability. However, to achieve truly scalable and adaptive solutions, future research must focus on optimizing AI models for real-world 6G deployments while balancing security with system performance.

5. Conclusion

As the 6G network turns into reality, network slicing is playing an important role in ensuring the best distribution of resources for various applications. However, this slope requires a sophisticated, adaptive protection system for its complexity and fragility. AI-based attack identification arrangements will provide extraordinary possibilities to address these disadvantages. Through the attack type classification and evaluation in several AI models, our research emphasizes the AI's strength, error, and future guidance in protecting the 6G network. Specifically, this study contributes a slice-specific attack classification framework that establishes a baseline for secure 6G slice architectures and outlines a roadmap for developing adaptive, AI-driven defense systems capable of mitigating emerging cyber-attacks.

References

Asensio-Garriga, R., Alemany, P., Zarca, A. M., Sedar, R., Kalalas, C., Ortiz, J., ... & Skarmeta, A.: Zsm-based e2e Attacks, challenges, solutions and research directions. *IEEE Communications Surveys & Tutorials*, *26*(1), 534-570, 2023.

B. B. Gupta, K. T. Chui, A. Gaurav and V. Arya, "Deep Learning Based Cyber Attack Detection in 6G Wireless

Cáceres-Hidalgo, J., & Avila-Pesantez, D.: Cybersecurity study in 5G network slicing technology: A systematic

De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M.: A survey on network slicing security:

Eziama, E.U., Okochi, P., Ibe, B.O., Esiowu, U.: 6G Network Slicing Attack Detection Using AI-Driven Mechanism.

Kukliński, S., Tomaszewski, L., Kołakowski, R., & Chemouil, P.: 6G-LEGO: A framework for 6G network

M. M. Saeed, R. A. Saeed, A. S. A. Gaid, R. A. Mokhtar, O. O. Khalifa and Z. E. Ahmed, "Attacks Detection in 6G

mapping review. In *2021, IEEE Fifth Ecuador Technical Chapters Meeting (ETCM)* (pp. 1-6). IEEE, 2021.

Moreira, R., & Silva, F. D. O.: Towards 6G network slicing. *arXiv preprint arXiv:2412.11366*, 2024.

Networks," *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, Hong Kong, Hong Kong, 2023, pp. 1-5, doi: 10.1109/VTC2023-Fall60731.2023.10333795.

Ren, Z., Li, X., Jiang, Q., Wang, Y., Ma, J., & Miao, C.: Network slicing in 6G: An authentication framework for

ResearchGate, 2025.

security slice management for DDoS attack protection in mec-enabled v2x environments. *IEEE Open Journal of Vehicular Technology*, *5*, 485-495, 2024.

Wireless Networks using Machine Learning," 2023 9th International Conference on Computer and Communication

Engineering (ICCCE), Kuala Lumpur, Malaysia, 2023, pp. 6-11, doi: 10.1109/ICCCE58854.2023.10246078.