Methodology

**Methodology**

**1. Research Design**

This research follows a quantitative experimental approach to evaluate the effectiveness of an AI-driven security framework for 5G network slicing. The study is structured into three main phases, focusing on simulation, anomaly detection, and real-time threat mitigation. A 5G testbed will be deployed using OpenAirInterface and srsRAN, and security vulnerabilities will be tested in a controlled environment.

This methodology is designed to:

* **Isolate 5G slices effectively** to prevent unauthorized access.
* **Deploy AI-based anomaly detection models** to identify cyber threats.
* **Implement real-time security mechanisms** to mitigate SS7-based and cross-slice attacks.

**2. Research Methods**

The project is divided into three phases:

**Phase 1: Security Analysis & Simulation Setup (Weeks 3-4)**

* **Simulating 5G network slicing** using OpenAirInterface and/or srsRAN.
* Deploying SDN(Software-Defined Networking)andNFV(Network Function Virtualization) to manage slices.
* Introducing SS7 vulnerabilities in a controlled testbed to study possible attack vectors.
* Capturing traffic logs using Wiresharkand/or Splunk for further analysis.

**Phase 2: AI-Based Threat Detection (Weeks 5-8)**

* Deploying AI/ML-based anomaly detection for real-time monitoring of slice traffic.
* Training ML models using Supervised Learning (Decision Trees, SVMs), Unsupervised Learning (Autoencoders, K-Means Clustering), Deep Learning (RNN, LSTM), and Reinforcement Learning.
* Processing captured network data to identify potential cyber threats.

**Phase 3: Automated Threat Mitigation (Weeks 9-10)**

* Deploying SDN controllers to implement slice-specific security policies.
* Implementing real-time mitigation techniques for SS7 threats and DoS attacks.
* Evaluating the security framework’s effectiveness under simulated attack conditions.

**3. Data Collection Procedures**

* Network traffic logs will be collected from 5G slices simulated in OpenAirInterface.
* AI models will be trained using attack scenarios including:
  + Cross-slice intrusions.
  + SS7-based location tracking and call hijacking.
  + SMS interception and DoS attacks.
* Anomaly detection results will be logged and analyzed for accuracy, precision, recall, and F1 score.

**4. Sampling Strategy**

Since this study is simulation-based, data sampling focuses on:

* **Attack datasets** generated in real-time.
* **Synthetic network logs** to train ML models.
* **Traffic pattern variations** across different slice types (eMBB, URLLC, mMTC).

**5. Data Analysis Techniques**

To evaluate the framework’s effectiveness:

* **Supervised models** (Decision Trees, SVMs) will classify attack types.
* **Unsupervised models** (Autoencoders, Clustering) will detect unknown anomalies.
* **Deep Learning models** (LSTM, RNN) will analyze attack patterns over time.
* **Reinforcement Learning (RL)** will optimize security responses dynamically.
* Performance metrics such as accuracy, false positive rate, and response time will be assessed.

**6. Justification of Methodological Choices**

* **Why ML-based security?**
  + Traditional rule-based security lacks adaptability to new threats.
  + AI-based detection improves real-time threat mitigation.
* **Why SDN/NFV?**
  + SDN enables dynamic security enforcement across slices.
  + NFV reduces dependency on rigid hardware-based security measures.

**7. Ethical Considerations**

* The study does not involve real user data; all experiments are conducted in a controlled 5G simulation.
* No personally identifiable information (PII) is collected.
* **Responsible AI use**: Models are trained to minimize bias and false positives.

**8. Limitations**

* **Simulation constraints**: Real-world deployments may introduce unpredictable security challenges.
* **Scalability**: AI-driven security must be tested for large-scale 5G networks.
* **False Positives**: ML-based detection systems may require fine-tuning for higher accuracy.

**Next Steps**

* Implement the **5G simulation and threat detection models**.
* Validate AI model performance with **realistic cyberattack scenarios**.
* Document results and refine security policies for better mitigation strategies.