Title:

**Reproducibility and Data Collection Guide for “Securing Emerging Technologies: Unified Security Standards for the Internet of Things (IoT)”**

**1. Data Collection Steps**

**1.1 Dataset Sources**

* Edge-IIoTset Dataset: Publicly available dataset used for IIoT network traffic and attack simulation.
* CICADA-IIoT2023 Dataset: Contains labeled attack scenarios and operational data from multiple industry sectors.
* All data used were public and free from licensing restrictions at the time of acquisition.

**1.2 Data Preprocessing**

* Deduplication: Remove identical records.
* Missing Value Handling: Imputed missing values or dropped records with critical nulls.
* Timestamp Alignment: Unified time format for accurate simulation.
* Anomaly Filtering: Removed corrupted or outlier records not representative of normal or attack behavior.

**2. Analysis & Simulation Reproduction**

**2.1 Tools Required**

* Python 3.8+
* Libraries:
* pandas, numpy, matplotlib, seaborn
* scikit-learn, scipy
* random, datetime

**2.2 CIoT-RESA Framework Architecture**

* Simulation 1: Breach trends (DDoS, phishing, malware)
* Simulation 2: IoT industry-specific breach analysis (Finance, Healthcare, Retail, etc.)
* Simulation 3: Pre- and Post-implementation evaluation of unified IoT security standard
* Probabilistic Models:
* Poisson Distribution
* Bernoulli Trials
* Monte Carlo Simulations

**2.3 Reproduction Steps**

1. Download both datasets.
2. Clean datasets as described in Section 1.2.
3. Implement CIoT-RESA using defined simulations:

* Define breach probabilities.
* Run iterative simulations with variable input.
* Store outputs in structured dataframes.

4. Use visualization tools (matplotlib, seaborn) to plot:

* Line charts for trend analysis
* Pie charts for breach type distribution

5. Validate outputs by comparing simulation trends with known real-world IoT breach data from 2020–2023.