Dissertation Proposal

Mitigating Temperature-Based Side-Channel Attacks in Data Centers

**Supervisor**: Ruth Lennon  
**Candidate**: Sumathi Dhanasekaran  
**Program**: MSc in DevOps  
**Credits**: 30

**1. Introduction**

Data centers face understudied physical security risks: minute temperature fluctuations (e.g., door openings cause transient drops/rises) can leak sensitive access patterns. Attackers monitoring heat probe data could infer unauthorized physical intrusions. This research develops a **software-driven pipeline** to obfuscate these thermal side-channels while preserving operational monitoring capabilities.

**2. Research Aims & Objectives**

**Primary Aim**: Design a Python-based framework to secure temperature data against inference attacks.  
**Objectives**:

1. Prevent reconstruction of physical access events (e.g., door openings) via data obfuscation.
2. Maintain ±2°C accuracy for critical operational alerts (e.g., overheating).
3. Achieve ≥90% detection rate for adversarial tampering.
4. Ensure real-time processing (<1s latency).

**Research Questions**

1. How can differential privacy parameters balance noise injection to mask door events while retaining thermal integrity?
2. Does multi-sensor fusion (18 probes) improve attack resilience vs. single-sensor configurations?
3. What computational trade-offs enable real-time privacy without disrupting operations?

**4. Methodology**

**Software Artefact**:

A **Python pipeline** with:

* **Input**: Simulated/live data from 18 probes (CSV/MQTT).
* **Processing**:
  + *Obfuscation*: Laplace noise (PyDP) + temporal aggregation.
  + *Sensor Fusion*: Outlier rejection via cross-correlation (SciPy).
  + *Anomaly Detection*: Isolation Forest model (Scikit-learn).
* **Output**: Sanitized data streams + security alerts.

**Evaluation**:

| **Test** | **Method** | **Target Metric** |
| --- | --- | --- |
| **Privacy** | Inject 100 door events; measure reconstruction rate | ≤10% success rate |
| **Utility** | Simulate overheating; compute MAE vs. raw data | ≤2°C error |
| **Adversarial Robustness** | Stress-test with rapid door events/spoofed data | ≥90% attack detection |
| **Performance** | Benchmark latency for 1h data (18 probes) | <1s processing |

**5. Novelty & Differentiation**

**Beyond Existing Work**:

* Prior studies detect thermal leaks (*IEEE 2019*) or apply generic privacy to sensors (*ACM 2020*).
* **This research**:
  + First framework combining **multi-sensor fusion**, **adaptive noise injection**, and **ML-based attack detection** for thermal side-channels.
  + Delivers an **open-source Python tool** (not just theoretical models).
  + Solves the privacy-utility trade-off for operational data centers.

**6. Ethical Considerations**

* **No human participants or confidential data**.
* Uses **synthetic datasets** (publicly available or programmatically generated).
* Real probe data (if used) will be anonymized/non-sensitive.

**7. Conclusion**

This proposal addresses a critical gap in data center physical security by developing a reproducible, software-driven solution to thermal side-channel leaks. The artefact will empower operators to protect against access inference attacks while maintaining NIST/ISO-compliant monitoring.