**Context:**

**Industry 4.0:** This revolution integrates advanced manufacturing techniques with automation, minimizing human intervention and optimizing resource utilization.

**Predictive Maintenance (PdM):** Industry 4.0 application, using machine learning (ML) algorithms and Internet-of-Things (IoT) sensors to predict when equipment will need maintenance pre-failure.

**Cybersecurity Concerns:** The integration of IoT and DL in PdM systems, introduces vulnerabilities to cyber-attacks, particularly FDIA (False Data Injection Attacks), which can compromise the system's integrity.

**Research Project Breakdown:**

*The objective of the research project is to demonstrate the vulnerability of PdM systems to FDIA and exploring how different DL algorithms can be robust and mitigate these risks.*

**Initial Setup and Familiarization**

* Set up the coding development environment, understand the code structure, and get familiar with the data handling and DL model implementation processes.

**Literature Review and Data Preparation**

* Conduct a deep dive into existing research on DL techniques for PdM and prepare the dataset.
* Explore current DL applications in PdM, focusing on their effectiveness, challenges, and how FDIA impacts them.
* Obtain the Australian dataset or generate an IoT dataset that can be manipulated to simulate FDIA this has been provided.
* Alternative: Use the NSAS dataset and implement a state-of-the-art FDIA on it
* Collect relevant papers regarding the PdM based on the NASA dataset

**Experimentation with DL Techniques**

* Propose and experiment with new or existing DL techniques to predict the Remaining Useful Life (RUL) of equipment, initially without FDIA.
* LSTM, GRU, CNN, other state-of-the-art approaches, and hybrid approaches to predict RUL based on the dataset.
* Establish the performance benchmark of these models in predicting RUL under normal conditions.

**Application and Analysis of FDIA**

* Apply FDIA to the dataset and analyze how it affects the performance of the DL models in predicting RUL.
* Introduce continuous and interim FDIA to the sensor data.
* Evaluate the DL models' accuracy post-attack, focusing on the quantitative degradation of their predictive capabilities.

**Comparative Analysis and Conclusions**

* Compare the resilience of the DL models against FDIA and determine which model(s) maintain predictive accuracy despite the attacks.
* Analyze the models' performance, pre and post-attack, to identify which models are most resilient to FDIA.
* Identify the DL model or combination of models (hybrid) that offers the best balance between predictive accuracy and resilience to FDIA.

**Scope:**

**Integration of DL in PdM Systems:**

*Explore and implement advanced DL algorithms to predict the Remaining Useful Life (RUL) of machinery, specifically a turbofan engine, using the C-MAPSS dataset provided by NASA.*

Long Short-Term Memory (LSTM): Ability to remember long-term dependencies.

Gated Recurrent Unit (GRU): simple compared to LSTM.

Convolutional Neural Network (CNN): Processing time-series data only when structured as 1D convolution.

Hybrid Deep Learning (HDL) Models: Experiment with combinations like CNN-LSTM and LSTM-CNN to assess if they offer better predictions by capturing both spatial and temporal dependencies.

Other DL methods: transformer, recurrent neural networks, temporal neural networks

**Cybersecurity Vulnerabilities of IoT and DL in PdM**

*FDIA attacks introduce false data into the system, potentially leading to incorrect predictions about machinery health and RUL.*

Continuous FDIA: Persistent false data injection that could mimic gradual wear or fault development.

Interim FDIA: Sporadic injections that might simulate intermittent faults or sensor errors.

**Dataset Manipulation and FDIA Simulation**

*Generate or manipulate IoT datasets to simulate FDIA, providing a testing ground for assessing DL models' resilience.*

Collect or generate datasets representative of real-world IoT sensor data from turbofan engines. This dataset has been provided.

Alternative dataset: health of state monitoring data for battery

Apply continuous and interim FDIAs to this data, altering readings in a way that mimics potential cyber-attacks.

**Evaluation and Comparison of DL Models**

*Assess and compare the performance of various DL models in predicting RUL under normal and after the data injection attack has occurred.*

Resilience to FDIA: The ability of models to maintain accuracy despite data manipulation and its magnitude.

Performance Metrics: Utilize metrics such as Mean Squared Error (MSE), Mean Absolute Error (MAE), and others relevant to RUL prediction.

**Proposing Improvements**

*Propose improvements or new DL techniques that enhance resilience to FDIA without significantly compromising prediction accuracy.*

A comprehensive literature review of existing DL techniques in PdM and their vulnerabilities to cyber-attacks.

An analysis and comparison report detailing each DL model's performance, both in normal and compromised scenarios.

**Timeline:**

**Semester 1 (Weeks 1-13)**

**Week 2: Initial Setup**

*Establish a productive work environment and gain a thorough understanding of the tools, datasets, and project repository.*

**Install and Configure Necessary Software**

* Identify all required software for the project (Python, any specific IDES).
* Download and install Python.
* Download and install Git from its official website.
* Verify installations by opening the terminal (or command prompt) and typing python --version, git --version, and opening the IDE.

**Clone the GitHub Repository**

* Create a GitHub account.
* Locate the relevant GitHub repository URL.
* Clone the repository.
* Check the contents of the cloned directory to ensure the cloning process was successful.

**Explore the Repository**

* Open the cloned repository folder in the IDE.
* Review the README file for an overview of the project structure and setup instructions.
* Identify any setup or configuration files (e.g., requirements.txt for Python dependencies).

**Familiarize with the C-MAPSS Dataset**

* Locate the C-MAPSS dataset within the repository or download it if necessary.
* Read any accompanying documentation or publications related to the C-MAPSS dataset to understand its origin, structure, and usage.
* Open the dataset using a tool or library capable of handling its format.
* Perform a preliminary exploration, noting the types of data, the number of features, and any immediately visible patterns or anomalies.

**Begin Preliminary Exploration of Python Libraries**

* Identify the Python libraries used
* Install required Python libraries using pip. For example, pip install tensorflow pytorch pandas.
* Browse through the official documentation or tutorials for these libraries to understand their purposes and basic functionalities.
* Execute simple code snippets to test the installation and get a feel for the syntax and capabilities of each library.

**Week 3: Ethics Training and Literature Review Start**

*Complete ethics training and initiate literature review.*

Complete Ethics online training and quiz.

Define the literature review scope on DL in PdM, cybersecurity vulnerabilities, and FDIA.

Begin a collection of articles, papers, and resources.

Organize findings and notes.

Start summarizing key literature on DL applications in PdM and cybersecurity issues, especially for the same dataset.

**Week 4: Literature Review Deep Dive**

*Extend literature review focusing on deep learning techniques and IoT sensor vulnerabilities.*

Search for sources discussing DL techniques (LSTM, GRU, CNN, HDL and other state-of-the-art methods) in the PdM context.

Identify case studies or examples of DL technique applications, noting results and limitations.

Include research on IoT sensor vulnerabilities, with a focus on FDIA.

Begin drafting literature review sections, categorizing findings by DL technique, application in PdM, and cybersecurity vulnerabilities.

**Week 5: Data Collection and Initial Analysis**

*Start dataset collection and perform initial analysis.*

Collect or generate a dataset, which can also be from battery or wind turbine health monitoring data, if not using an existing one (e.g., C-MAPSS).

Analyze the structure, variables, and preprocessing needs of the C-MAPSS dataset.

Experiment with basic data visualization techniques for sensor data pattern recognition.

Document insights and questions from data exploration.

Consider methods for simulating FDIA on the dataset, including continuous and intermittent attack scenarios.

**Week 6: Data Preprocessing and Model Familiarization**

*Prepare a dataset for DL model implementation and understand DL models.*

Perform data cleaning and preprocessing for DL model use.

Explore architectures of DL models (LSTM, GRU, CNN, HDL) and review tutorials/documentation.

Establish a basic framework for model implementation, ensuring all libraries and dependencies are prepared.

**Week 7: Initial Model Implementation and Testing**

*Implement and test initial DL models.*

Code DL models using the pre-processed dataset, starting with simpler implementations.

Test models on dataset portions to evaluate RUL prediction performance without FDIA.

Document model performance using metrics such as accuracy, precision, and recall.

**Week 8: Refinement and FDIA Simulation Preparation**

*Refine models and prepare for FDIA simulation.*

Analyze initial test results and refine models for improved performance.

Design FDIA simulations, defining attack characteristics and expected impact.

Begin coding FDIA simulation scripts for controlled dataset manipulation.

**Week 9: FDIA Simulation and Impact Analysis**

*Conduct FDIA simulation and analyze the impact on model performance.*

Execute FDIA simulations, creating dataset versions with simulated cyber-attacks.

Test DL models on altered datasets to evaluate the impact of FDIA on performance.

Document results, noting significant performance metric changes.

**Week 10: Interim Report and VIVA Preparation**

*Compile findings for the interim report and prepare for VIVA presentation.*

Draft interim report incorporating literature review, methodology, findings, and FDIA impact analysis.

Develop VIVA presentation, summarizing objectives, progress, findings, and future steps.

Rehearse presentation, seeking feedback to refine delivery and content.

**Week 11: Finalizing the Interim Report**

*Complete and refine interim report for submission.*

Finalize interim report drafting, ensuring all sections are comprehensive and well-presented.

Proofread the report for clarity, coherence, and accuracy.

Incorporate illustrative figures, tables, or graphs.

Ensure correct citation of all references.

Submit the interim report for feedback to enhance quality.

**Week 12: VIVA Preparation and Presentation**

*Thorough preparation for VIVA presentation.*

Refine presentation based on feedback and report.

Prepare for potential VIVA questions with well-thought-out answers.

Practice presentation multiple times, ideally with an audience.

Prepare additional materials for VIVA as needed.

**Week 13: VIVA Presentation and Feedback Reflection**

*Deliver the VIVA presentation and utilize feedback for future planning.*

Present VIVA confidently, engaging with the examination panel and addressing queries.

Note feedback and questions for refinement.

Reflect on the VIVA experience to identify improvements.

Plan for next semester based on feedback and assessment.

**Recommendations:**

**Programming and Development Tools:**

* Jupyter Notebooks
* Visual Studio Code (VS Code) + Jupyter
* GitHub

**Data Analysis and Machine Learning Libraries:**

* TensorFlow and PyTorch
* Pandas and NumPy
* Matplotlib and Seaborn

**Project Management and Collaboration Tools:**

* Trello or Asana
* Microsoft Teams

**Study and Research Tools:**

* Mendeley or Zotero: Reference management software to organize research papers and articles. They can help manage bibliographies and references.
* Google Scholar Alerts

**Miscellaneous Tools**

* Grammarly or Hemingway
* Figshare or Zenodo

**Research Project extensions:**

**Semester 1 Extensions**

**Comparative Analysis of Additional DL Models:**

* Transformer models or attention mechanisms. This could provide insights into even more effective or efficient predictive models.

**Dataset Enrichment**:

* Enhance the C-MAPSS dataset with additional data sources, including real-world operational data from different machinery or environments, to test the models' generalizability and robustness across various scenarios. For example, there is increasing interest for the health monitoring data of battery, wind turbine and other critical assets.

**Preliminary Cybersecurity Framework Development:**

* Draft a cybersecurity framework tailored explicitly for PdM systems in IoT environments.
* Identifying key vulnerabilities
* Proposing data integrity verification mechanisms
* Developing preliminary guidelines for secure data transmission and processing.

**Semester 2 Extensions**

**Advanced FDIA Simulation and Resilience Testing**:

* Sophisticated attack patterns that mimic real-world cyber threats more closely.

**Integration of Anomaly Detection Techniques:**

* Incorporate anomaly detection techniques to identify unusual data patterns that could indicate a cyber-attack.