**Slide 1:**

Good Morning, my name is Harrison Faure, and today I will be presenting my research on 'False Data Injection Attacks on the Internet of Things and Deep Learning-Enabled Predictive Analytics.'"  
  
**Slide 2:**

Industry 4.0 merges automation with advanced manufacturing, aiming to reduce human effort and resources. A key component of Industry 4.0 is Predictive Maintenance, which uses machine learning algorithms and IoT sensors to predict equipment failures before they occur, enhancing operational efficiency and reducing maintenance costs.

**Slide 3:**

Main Research Question:

How do IoT sensor attacks, specifically False Data Injection Attacks, impact the performance of deep learning (DL) models used in Predictive Maintenance systems for predicting the Remaining Useful Life of turbofan engines?

Objectives:

Implement various DL models including LSTM, GRU, CNN, RNN, and Transformer.

Predict RUL using NASA’s C-MAPSS dataset.

Evaluate these models under FDIA scenarios.

Propose a cybersecurity framework to enhance the resilience of Predictive Maintenance systems against FDIA attacks.

**Slide 4:**

The literature review highlights the importance of Industry 4.0 and Predictive Maintenance, having devices connected to the IoT exposes industrial networks to a variety of cybersecurity attacks. The majority of the published literature focuses on the accuracy of IoT and DL-enabled Predictive Maintenance systems and often ignores the effect of these attacks.

There is a significant gap in understanding how cyber-attacks, specifically FDIA, impact the reliability and accuracy of Predictive Maintenance systems. Existing studies predominantly emphasize enhancing model accuracy and predictive capabilities without addressing the susceptibility to data integrity attack. Research is needed to develop robust Predictive Maintenance systems that maintain high predictive accuracy even in the presence of cyber threats.

In terms of deep learning models, LSTM and GRU are effective in handling sequential data and long-term dependencies. CNNs are useful for extracting spatial hierarchies from time series data. RNNs are beneficial for dynamic and complex fault detection scenarios common in Predictive Maintenance applications. Transformer models offer better performance in situations where long-range dependencies are crucial.

My research addresses these gaps by evaluating the impact of FDIA on various DL models used in Predictive Maintenance systems for predicting the Remaining Useful Life with The goal to propose a cybersecurity framework that enhances the resilience of these systems against FDIA attacks.

**Slide 4 (1.5 Minute):**

"The methodology of my research involves several key steps to ensure a thorough investigation and robust results.

First, model selection and training. I chose CNN, RNN, LSTM, GRU, and Transformers for their proven capabilities in handling time series data.

Next, data preparation. I utilized the NASA C-MAPSS dataset, which includes various sensor data and operational settings from a turbofan engine. Key steps in data preparation include normalization, feature engineering, and handling missing values to ensure the dataset is ready for analysis.

Then, the implementation of advanced models. CNNs are used for extracting spatial hierarchies, LSTM and GRU for their ability to handle long-term dependencies, RNN for sequential data processing, and Transformers for managing long-range interactions without constant recurrence.

FDIA attack simulation is a critical part of the methodology. I simulate the models under both normal operation environments and various simulated FDIA attack scenarios to test their feasibility and robustness.

For performance evaluation, I use metrics such as RMSE, MSE, and accuracy to RUL. Additionally, I conduct resilience tests under FDIA scenarios to compare robustness across models.

The iterative improvement and feedback phase focuses on optimization and refinement of the algorithms. This involves a continuous feedback loop to make iterative improvements based on performance results.

Finally, I work on drafting recommendations and framework. The goal is to develop practical recommendations for enhancing Predictive Maintenance systems and draft a preliminary cybersecurity framework to safeguard against FDIA attacks.

Each step in this methodology is crucial for ensuring the models are not only accurate but also resilient to cyber-attacks, which is essential for reliable Predictive Maintenance systems in Industry 4.0 environments."

**Slide 5 (1.5 Minute):**  
"In this section, I'll discuss the data collection and analysis process for my research.

First, the dataset. I utilized the NASA’s C-MAPSS dataset, which includes various sensor data and operational settings from a NASA turbofan engine. This dataset is essential for predicting the Remaining Useful Life (RUL) of the engine components.

For data preprocessing, I performed several key steps:

Normalization to ensure the data is on a consistent scale.

Feature engineering to extract relevant features that improve model performance.

Handling missing values to maintain data integrity.

Next, the preliminary results of the CNN implementation. The CNN model achieved a Mean Absolute Error (MAE) of 11.03 and an R² value of 0.8314. These results indicate a good fit, but there's room for improvement.

However, there were issues with the LSTM and GRU models. Both models are predicting a constant RUL, which is incorrect. To address this, I plan to adjust the model parameters and re-evaluate the training processes to enhance their predictive accuracy.

Looking ahead, the future data collection and analysis steps include:

Simulating False Data Injection Attacks (FDIA) to test model resilience.

Evaluating model performance under these attack scenarios to ensure robustness.

Each of these steps is crucial for developing reliable Predictive Maintenance systems that can withstand cyber-attacks and maintain accurate predictions, which is essential for Industry 4.0 environments."

**Slide 6 (1 Minute):**

"Let's take a look at the preliminary results from the CNN model implementation.

CNN Performance: The CNN model achieved a Mean Absolute Error (MAE) of 11.03 and an R² value of 0.8314. This graph shows the predicted vs. actual Remaining Useful Life (RUL), demonstrating the model's effectiveness in capturing complex patterns in the data.

Significance of Preliminary Results: These results highlight the potential of CNN for accurate RUL prediction in Predictive Maintenance systems. The relatively high R² value indicates that the model explains a significant portion of the variance in the data, which is promising for future development.

Areas for Improvement: While the CNN model shows good performance, there's still room to enhance its accuracy. Additionally, we need to resolve the issues with the LSTM and GRU models, which are currently predicting constant RUL values. Finally, implementing FDIA resilience testing will be crucial to ensure the robustness of the models against cyber-attacks.

These preliminary results provide a solid foundation for further improvements and testing."

**Slide 7 (1 Minute):**

Moving forward, here's the timeline for the remaining work in my project.

Timeline:

Week 1-2: Finalize semester one work and present the VIVA.

Week 3-4: Refine data collection and improve initial results.

Week 5-6: Implement transformer models and continue model training.

Week 7-8: Conduct FDIA simulations and evaluate model performance.

Week 9-10: Optimize models and prepare the first draft of the final report.

Week 11: Submit the final report and prepare for the presentation.

Key Milestones include the implementation of transformer models, conducting FDIA attack simulations, and preparing for the final report and presentation.

There are also several possible extensions to enhance the research further:

Implementing real-time data simulation to continuously test models and provide insights into their performance in real-world scenarios.

Developing advanced anomaly detection techniques to improve resilience against various forms of FDIA attacks.

Creating a comprehensive cybersecurity framework aimed at enhancing the resilience of Predictive Maintenance systems to FDIA attacks.

These steps will ensure that the research not only advances our understanding of Predictive Maintenance systems but also contributes to their robustness and reliability in the face of cyber threats.

**Slide 8 (50 seconds):**

In conclusion, my research investigates the impact of False Data Injection Attacks (FDIA) on Deep Learning (DL)-enabled Predictive Maintenance (Predictive Maintenance) systems. Using NASA’s C-MAPSS dataset, I implemented various DL models, including CNN, RNN, LSTM, GRU, and Transformers, to predict the Remaining Useful Life (RUL) of turbofan engines.

The importance of this work lies in enhancing the reliability and accuracy of Predictive Maintenance systems while addressing the critical vulnerabilities posed by FDIA in IoT environments. By doing so, we aim to improve the resilience of Predictive Maintenance systems to cyber-attacks and develop a robust cybersecurity framework for Industry 4.0 applications.

The expected impact of this research includes more reliable Predictive Maintenance systems, reduced maintenance costs, and enhanced operational efficiency across various industries.