**False Data Injection Attacks on the Internet of Things and Deep Learning-Enabled Predictive Analytics**

**Z5364422 | Harrison Faure**

**Abstract**

**The report investigates Industry 4.0 frameworks, specifically False Data Injection attacks (FDIA) on Predictive Maintenance (PdM) systems. The aim is to evaluate the effectiveness of Deep Learning (DL) models when predicting Remaining Useful Life (RUL) of Turbofan engines. Utilized within the report are Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), Recurrent Neural Networks (RNN), and Transformer models, focusing on the specific methods resilience against FDIA evaluating these models’ performance against each other. Preliminary implementations of GRU and LSTM give constant RUL predictions which are wrong whereas the CNN implementation gives RUL predictions with an R squared value of 0.8314. The research anticipates providing contributions to PdM systems enhancing their accuracy and resilience even in the presence of a cyberattack. The study will also propose a cybersecurity framework with the intention of mitigating FDIA attacks. This report addresses knowledge gaps in current literature emphasizing the necessity for more robust PdM systems and putting emphasis on the outlined research task.**

Contents

[I. Introduction 2](#_Toc166775577)

[**A.** **Industry 4.0, Predictive Maintenance & False Data Injection Attacks** 2](#_Toc166775578)

[**B.** **Research Focus** 3](#_Toc166775579)

[**C.** **Expected Outcomes** 3](#_Toc166775580)

[**D.** **Aim** 3](#_Toc166775581)

[**E.** **Scope** 3](#_Toc166775582)

[II. Literature Review 4](#_Toc166775583)

[**A.** **Industry 4.0** 4](#_Toc166775584)

[**B.** **Predictive Maintenance** 5](#_Toc166775585)

[**C.** **Security and Reliability** 5](#_Toc166775586)

[**D.** **Machine Learning** 6](#_Toc166775587)

[**E.** **Deep Learning** 6](#_Toc166775588)

[**F.** **Transformer Models** 7](#_Toc166775589)

[**G.** **Challenges / Knowledge Gaps** 8](#_Toc166775590)

[III. Approach 8](#_Toc166775591)

[**A.** **Overview** 8](#_Toc166775592)

[**B.** **System Architecture and Model Development** 9](#_Toc166775593)

[**C.** **Data Collection and Preparation** 9](#_Toc166775594)

[**D.** **Model Training and Validation** 9](#_Toc166775595)

[**E.** **Implementation and Performance Evaluation** 9](#_Toc166775596)

[**F.** **Feedback and iterative improvement** 9](#_Toc166775597)

[IV. Results 9](#_Toc166775598)

[**A.** **CNN Implementation Preliminary Results** 9](#_Toc166775599)

[V. Future Work 10](#_Toc166775600)

[**A.** **Timeline** 10](#_Toc166775601)

[**B.** **Extensions** 10](#_Toc166775602)

[VI. Conclusion 11](#_Toc166775603)

[References 11](#_Toc166775604)

**Nomenclature**

|  |  |
| --- | --- |
| Acronym | Expanded Form |
| DL | Deep Learning |
| IoT | Internet of Things |
| PdM | Predictive Maintenance |
| RUL | Remaining Useful Life |
| I4 | Industry 4.0 |
| FDIA | False Data Injection Attacks |
| GRU | Gated Recurrent Units |
| LSTM | Long Short-Term Memory |
| RNN | Recurrent Neural Networks |
| CNN | Convolutional Neural Networks |
| HDL | Hybrid Deep Learning |
| TSA | Time Series Analysis |
| ML | Machine Learning |
| NN | Neural Networks |
| CPS | Cyber Physical Systems |

# **Introduction**

This report outlines an approach to using advanced Deep Learning [DL] models within the framework of Industry 4.0 to develop a Predictive Maintenance [PdM] system. The report utilises the C-MAPSS dataset provided by the National Aeronautics and Space Administration to predict the Remaining Useful Life [RUL] of a turbofan engine, which will increase reliability and enhance operational efficiency across different industrial applications.

PdM systems are important applications within the shift towards Industry 4.0 [I4], as industries seek to increase automation and efficiency. Robust and accurate PdM systems are a catalyst of this shift as well as the increase of IoT devices comes with the potential for cyber security vulnerabilities [1]. The need to safeguard the integrity of these PdM systems is of increasing priority.

## **Industry 4.0, Predictive Maintenance & False Data Injection Attacks**

The fourth revolution in manufacturing and industry is characterized using a combination of technologies that blur the lines between physical, biological, and digital spheres. The creation of smart factories is facilitated by advanced communication and information technologies, including cyber-physical systems, he Internet of Things [IoT], cloud computing and big data analytics. Real-time data collection and analysis is achieved through the integration of these technologies, which enables enhanced connectivity and automation in the manufacturing process. [1]

PdM uses data analysis tools and techniques to predict equipment failures before they occur and detect anomalies, making it an advanced strategy for maintenance. PdM is data-driven and condition-based, which minimise unplanned downtime, reduces maintenance costs, extends equipment life, and increases operational efficiency. PdM systems have been enhanced by using DL models such as Gated Recurrent Units [GRU], Long Short-Term Memory [LSTM], Recurrent Neural Networks [RNN], and Convolutional Neural Networks [CNN] to model complex patterns in real-time and historical data as well as transformer models [2].

PdM is a component of advanced analytics and IoT technology designed to optimise and automate maintenance processes. There should be seamless integration between IoT devices and PdM structures, allowing for real-time health assessment and risk management for certain industrial assets.

Having devices connected to the IoT exposes industrial networks to a variety of cybersecurity attacks. For this specific report, the focus is on False Data Injection Attacks [FDIA], which involve the injection of malicious data. These attacks can lead to incorrect decision-making and predictions. FDIA attacks can take the form of intermittent attacks, which may sporadically introduce outliers to disrupt system operations, or continuous attacks, which aim to mimic degradation patterns in the equipment attempting to disrupt the system over time whilst remaining realistic [5]. Maintaining the reliability of PdM systems will involve mitigating and understanding the risks of FDIA attacks as well as developing the DL models to be capable of countering and detecting these attacks.

## **Research Focus**

The project focusses on researching, evaluating, and refining the application of DL models selected based on their proven capabilities in handling time-series and sequential data to predict the RUL of a NASA turbofan.

An addition to the research project is transformer architecture and RNN algorithms. Transformers utilise self-attention mechanisms to direct the relationship between all points in a sequence. This improves and offers better performance in situations where long-range dependencies are of high importance. Handling sequential data without the need to have a recurrent structure could provide substantial improvement to how PdM tasks are approached in future.

The primary objectives of the research task are to:

1. Implement the following DL models – LSTM, GRU, CNN, RNN, and Transformer models.
2. Utilise the implementation to predict RUL of the NASA Turbofan from the CMAPSS data.
3. Evaluate the of the models during different FDIA scenarios.
4. Experiment with different combinations of processing algorithms and input data to increase the efficiency of the DL models.

## **Expected Outcomes**

The research project should provide contributions to the field of PdM by creating advancements in the application of DL technologies in industrial settings. The project will also cover the potential issue of cybersecurity vulnerabilities in PdM systems by investigating FDIA. The study will increase understanding of the fortification against such attacks and their impact on the integrity and predictions of predictive models. The relevance of this aspect is high given the drastic increase in the integration of IoT devices in industrial settings, which comes with a heightened risk of vulnerabilities.

The research project is anticipated to produce a PdM framework that is more robust, secure, and accurate than the current implementations within the I4 PdM landscape. The results and produced work should minimise downtime and increase operational efficiency while reducing maintenance costs. This may directly impact the profitability and sustainability of heavy machine-based industries as the PdM systems lead to more reliable decision-making.

## **Aim**

The aim of this project is to predict RUL by developing and evaluating advanced DL models and utilising NASA’s CMAPSS dataset. The project will utilise and investigate the integration of transformer architecture, LSTM, GRU, CNN, RNN and potentially Hybrid Deep Learning [HDL] models to enhance the effectiveness and overall efficiency of PdM systems. The project will observe the impact of FDIA on the predictive accuracy of the models, therefore aiming to establish robust DL methods that maintain high predictive accuracy during various cyber threat scenarios. On top of this the project aims to refine training processes and contribute new insights to the field of PdM as well as draft a framework that reflects these findings.

## **Scope**

The research project explores the implementation of advanced DL algorithms to predict RUL using sensor data. The dataset utilised is the NASA C-MAPSS dataset, which stores sensor data for a turbofan. LSTM and GRU implementations are used to investigate the efficiency of long-term dependencies, and CNN are used to process time series data. HDL models such as CNN-LSTM are also investigated to see if the RUL prediction is augmented by capturing special and temporal data dependencies. Transformer models have also been implemented to provide a broad spectrum of different RUL predictions to test factors such as robustness as well as the transformers’ ability to handle sequential data effectively.

The focus on FDIA will investigate cybersecurity vulnerabilities within IoT devices and the DL architectures mentioned when utilised in PdM. FDIA attacks have the potential to skew RUL, and machinery health predictions and both continuous attack and intermittent attack scenarios are within the scope of the research project. Comparison of the performance of the DL models under normal conditions and after FDIA attacks focussing on resilience to the FDIA attacks and overall robustness – maintaining accuracy in different scenarios

The research will help propose new DL techniques or improvements to existing techniques that enhance resilience to cyber-attacks without decreasing the overall predictive accuracy.

# **Literature Review**

The literature review will build on the preliminary concepts introduced earlier as well as examine current and past literature to establish a knowledge base supporting PdM within Industry 4.0. The review will support understanding the current technologies, and therefore, the contributions of this research will fit.

The gaps in the current research are outlined by examining existing literature from a broad range of sources. A comprehensive view will be formulated from the academic literature to support the progression of this research, guiding the research's direction and outlining the significance of the proposed enhancements.

## **Industry 4.0**

1. Overview:

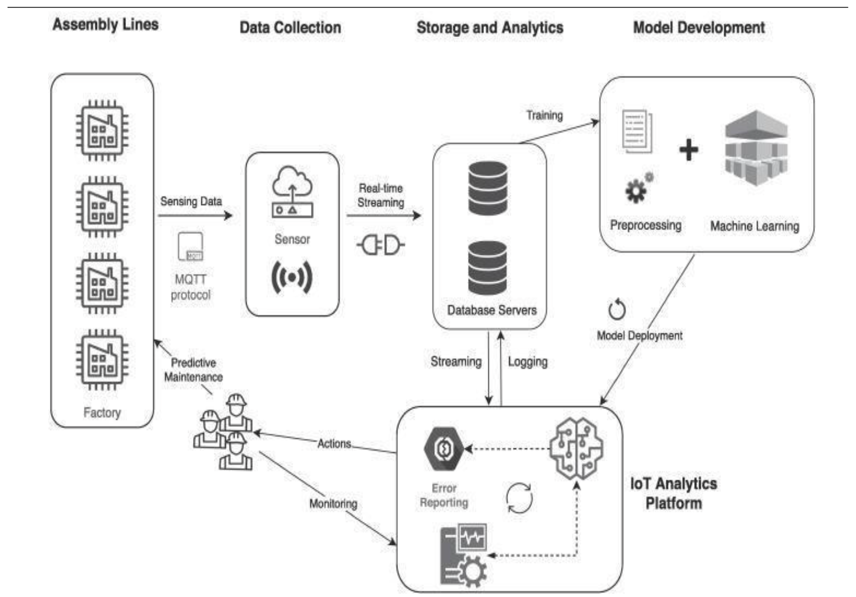
Industry 4.0 is a pivot in industrial production that is pioneered by the integration of digital technologies into manufacturing environments [1]. Evaluate the transformation brought about by the deployment of IoT devices, aiming to facilitate data generation and connectivity. This revolutionises industry practices by enhancing operational efficiency and decision-making through real-time data insights. These advancements have created a new era of data generation and interconnected devices enhancing decision-making through data analysis [7]. Figure one depicts the integration of digital technologies into manufacturing environments and demonstrates the flow from collection to development to PdM, and emphasizes the changes brought through IoT devices.

Figure 1 – Integration of IoT Platform for Industry 4.0

1. Evolution:

Industry 4.0 has evolved since being brought forward and is closely linked with the advancement and integration of IoT devices across different industries [1], which outlines the rapid advancement of IoT devices to lead significant changes and offer new opportunities with innovative system reliability and maintenance approaches. Industry 4.0 via IoT devices has become an integral part of various industries, such as smart cities, healthcare, manufacturing, and transportation [7].

1. Core Technologies:

[1] Outlines the two core technologies within Industry 4.0, DL, Time Series Analysis [TSA], Neural Networks [NN], and Machine Learning [ML], describing how IoT devices generate large amounts of sensor data. This data is then analysed through TSA and DL for PdM to prevent unexpected failures and optimize system performance [8], demonstrating how NN and ML techniques such as LSTM have been utilised within Industry 4.0 and are effective at ensuring proactive system maintenance.

1. Manufacturing Impact

Reliability and efficiency of operations have a large impact on manufacturing that is brought forward by Industry 4.0. The approach outlined in Industry 4.0 helps to decrease maintenance costs pre-emptively by predicting and fixing potential problems before they occur [1].

## **Predictive Maintenance**

1. Overview

PdM enhances the efficiency and maintenance of IoT devices leveraging TSA and DL. [1] explains that different data types such as sensor data, error logs, and historical maintenance records can be used within PdM to help optimize resource utilization aiming to reduce maintenance downtime. Generally, this approach will involve data pre-processing to extract features, normalize, and clean the data.

1. Contextual importance

PdM addresses the need for an innovative approach to maintenance by increasing the uninterrupted functionality of IoT devices whilst increasing their reliability [1]. PdM aims to maximise the potential benefits of the interconnected IoT devices within different industries through predicted interventions that minimise downtime and maximise productivity. [8] Emphasizes the performance of LSTM in handling time series data, which is directly applicable to PdM problems within the Industry 4.0 setting. Using advanced algorithms (such as OC-SVM and SVDD), the accuracy of anomaly detection can be improved, which is critical to effective PdM [21, 33].

1. Foundations

PdM uses DL and TSA to determine temporal patterns of which decomposition (time series) and statistical analysis can be used to identify trends. [1] Identifies commonly used deep learning models such as RNN and LSTM which are used to predict maintenance needs based on historical data. LTSM are powerful dynamic classifiers that approach problems related to vanishing gradients to ensure more reliable and consistent performance. [2] Transformer-based models can also be utilised within PdM leveraging DL to increase reliability. Transformer models can provide a different approach to PdM using positional encoding to handle time series data. [14] These models will identify complex patterns and relationships from time-series data for an integrated approach to anticipating maintenance. [1, 29] The accuracy of the PdM system model is determined after training the model, where the test samples are used as inputs to the models, and the network will then compare the reconstructed values against the input values. From these comparative statistics, such as R squared, the accuracy rate is obtained from an average calculation of the mean error squared values [12].

## **Security and Reliability**

1. Cyber-security concerns

[5] Highlights the susceptibility of IoT PdM systems to cyber-attacks focussing on FDIA. The vulnerability of PdM systems to FDIA is critical as they directly impact the reliability and accuracy of predictive capabilities, leading to potential catastrophic consequences. [6] Notes that the community has addressed the potential concerns by developing CPS [cyber-physical systems] which utilise DL within the IoT. Another security concern highlighted in [27] alongside the timing attacks is the threat of chronological data patterns, which can be exploited to reverse engineer encryption.

1. Management Strategies

Statistical and hybrid approaches are methods that can be employed to counteract these attacks, such as anomaly detection and behaviour analysis to spot inconsistencies and data analysis. 5,25] Strategies include a feedback design that is preventative against denial-of-service attacks [DOS] and FDIA attacks are explored in [6], demonstrating how both ‘active’ and ‘passive’ defence systems are vital. [10] Also states that “Extensive research has been performed on the detection and mitigation of FDI attacks in cyber-physical systems (CPS) domain. Unfortunately, the effect of FDIA on a PdM system is yet not explored.”

1. Reliability

FDIA attacks threaten the reliability and accuracy of PdM systems by the introduction of these errors, which mimic normal sensor input and are, therefore, hard to detect. This puts emphasis on the robustness of the countermeasures needed in these PdM models [5]. FDIA attacks are subtler than DOS attacks and are, therefore, more difficult to detect, requiring advanced detection mechanisms [6]. Data integrity is crucial for the reliability of ML models, as compromised data can lead to erroneous predictions [27]. It is important to combat these cyber-attacks with a resilient cyber strategy that is dynamic and incorporates continuous adjustments to technical measures and new threats [22].

## **Machine Learning**

1. Fundamentals

ML algorithms are used in the context of Industry 4.0 and PdM to predict part and equipment failures through sensor data analysis. DL is categorized as an ML algorithm, and the fundamental advantage of the pair is its ability to handle and learn from large amounts of data. This is done with the intention of making accurate predictions surrounding system failures, which enables proactive management strategies. [3] In PdM, ML focuses on data-driven methods that handle the multivariate nature of data collected in condition-based maintenance. [11] Investigates DL models such as RNNs and determines that they excel in their ability to extract features and predict trends automatically from the data. [9] Discusses the fundamental applications of RNNs – LSTM and GRU designed for handling time series data, giving insights on the fundamentals of machine learning and the ability to handle the sequential nature of data without reducing the dimensionality.

1. Advantages

Traditional approaches before Industry 4.0 have struggled for decades, and ML has provided a clear advantage in the context of predictive maintenance. ML Algorithms offer reduced downtime through their greater data handling capabilities as well as a greater ability to predict system behaviour early, providing warnings before catastrophic damage. [3] The ability of RNNs to detect subtle anomalies that traditional methods may miss is found to be an advantage in [9] of ML approaches to PdM. The capability of RNNs and LSTMs is an advantage where the behaviour of the machinery can have significant variety, making DL models and, by extension, an ML approach far superior to traditional methods.

## **Deep Learning**

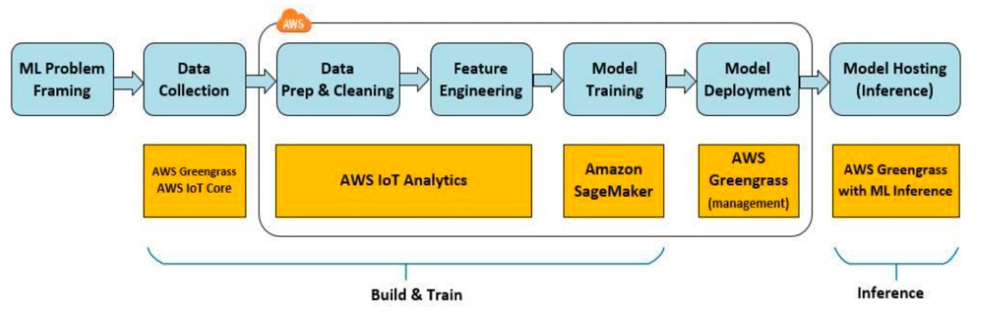
1. Definition

Figure 2 – Amazon Web Service Workflow for ML Model Development

DL falls under the categorization of ML algorithms and utilises multi-layer neural networks to learn from large amounts of data. DL networks are “capable of learning rich and complex representations of data, which are used for a variety of predictive tasks” [3]. DL's advantage is that it can automatically discover the representations needed for the classification of raw data or feature detection, reducing manual feature extraction or eliminating it entirely [3].

1. RNN

RNNs or recurrent neural networks involve connections between nodes that, within a temporal sequence, form a direct graph. RNNs will display dynamic behaviour unlike feed-forward neural networks and use their internal memory to process sequences of inputs making them desirable for anomaly detection where the order of the data points is important [3]. RNN based methods may generally draw components from LSTM and GRU to help analyse signal data sequences emphasizing the importance of LSTM within PdM [11]. Handling dynamic and complex fault detection scenarios was demonstrated to be an advantage of RNNs [19]. which are common in PdM scenarios.

1. CNN

Convolutional neural networks use the mathematical operator, ‘convolution’ to capture spatial hierarchies in data and apply filters that produce feature maps. In doing so, CNNs become highly effective at the recognition of objects in visual contexts and for processing data that has a known topology. [3] The use of CNNs to analyse time series data is highlighted in [11] by extracting spatial hierarchies, making CNNs suitable for PdM approaches where sensor data is utilised. [24] Compared CNN’s fault detection capabilities and indicated that CNNs are important for data analysis and processing in PdM tasks.

1. LSTM

The long short-term memory approach is an extension of RNNs used to avoid long-term dependency problems, making them effective on data with long intervals and delays. LSTMs have greater use in problems involving the prediction of outcomes for sequential data as they solve the vanishing gradient problem, which is prevalent in RNNs. [3] The gradient problem is defined as “A condition where the gradient of the loss function shrinks exponentially as it is backpropagated through the network’s layers during training”. One of the most powerful hybrid models is the RNN [LSTM-RNN], which is a powerful hybrid classifier for handling time series data. LTSM-RNN is effective in PdM situations as it efficiently handles pattern recognition over time [2]. This hybrid was developed as RNN is ineffective with the vanishing gradient problem, and LSTMs help take the long-term dependencies into account [4].

1. GRU

Gated recurrent units are highly efficient in handling sequential data under constant monitoring conditions. They also address the vanishing gradient problem but with a simpler design that uses an ‘update gate’ rather than ‘forget and input gates’ which helps to capture dependencies. [11] Notes that GRUs are known to be more robust whilst learning complex temporal dynamics, which makes them desirable for PdM tasks and forecasting [11]. GRU applications are found to be advantageous in applications that involve constant monitoring and prediction of system states, making them useful in PdM applications where long-term data trends are the focus [24].

1. Applications

DL algorithms are applicable to PdM tasks as high-dimensional sensor data is utilised to determine anomalies, trends, and/or predict failure. These DL models are useful to process and learn from complex datasets with minimal manual intervention and minimal pre-processing [3]. NASA’s C-MAPSS dataset was utilised within [10] for predicting RUL using GRU, CNN, and LSTM, and it was found that GRU-based PdM models consistently outperform some recent literature on RUL prediction. [10,17] “The practical applications of neural networks have been shown to effectively handle the detection of faults and service time of mechanical hardware” [16], which specifically references CNN and RNN implementations within mechanical systems operations. The workflow for deploying DL models using the Amazon Web Service [AWS] is shown in Figure 2 and is a valuable resource for demonstrating how multi-layer neural networks can be leveraged for complex and rich learning from extensive data sources.

1. Hybrid Learning Models

[20] demonstrates the applications of a couple of hybrid DL models, such as GRU-LSTM parallel and CNN-LSTM, and it was found that GRU-LSTM obtained the lowest RMSE, whilst CNN-LSTM had the best computational efficiency.

## **Transformer Models**

1. Overview

Transformers are generally used for natural language processing [NPL] and computer vision and are used in many time series analysis applications [27]. Transformers can model long-term and short-term behaviours simultaneously, which is a unique capability that may be applicable to PdM systems [34].

1. Transformer Architecture

Default transformer architecture contains encoder and decoder layers utilising a sequence-to-sequence model that uses an encode-decoder configuration designed to learn to encode the source in a fixed-length representation [27, 13]. Both the encoders and decoders are composed of multiple identical blocks to help with modelling [32]. This is done because the length of the two sequences is not necessarily the same size, aiming to decode the target sequence in an ‘auto-regressive’ manner [27, 28]. It was found in [34] that transformers can be used to reduce the error in accumulation during forecasting, leading to greater efficiency and reducing errors over long forecast horizons. [34] States that “Transformers can use a mechanism with a mask to ensure consistent behaviour during training and forecasting” establishing how transformers use sequential data to maintain accuracy.

1. Application

Transformer applications have improved long-term and multivariate time series forecasting, and their effectiveness on complex forecasting tasks has greatly approved the approach [27]. Different transformer approaches are used for different applications – the Informer achieves O(LlogL) in time complexity and memory usage and is shown to be effective in Long-Sequence Time-Series Forecasting [LSTF] applications [36]. In [15], a probabilistic transformer model that utilises state space models was implemented within a fault detection environment to handle uncertainty and was shown to be effective within the study. For network modifications at both high (architecture) and low level (module), the overarching aim is to improve the overall performance of time series modelling [32].

1. Informer Transformers

The Informer approach is particularly advantageous for long-range dependencies with long sequential inputs. The Informer will utilise a self-attention mechanism to significantly reduce memory utilisation and computation power needed. [36] Used an informer transformer in a PdM system that used a generative style decoder to take a long sequential output using only one forward step – this avoided excessive error spreading during the inference phase.

## **Challenges / Knowledge Gaps**

1. Current Limitations

Despite advancements in IoT and DL technologies, FDIA remains a prevalent form of cyber-attack that is a significant challenge to overcome [27]. PdM systems remain vulnerable as FDIA attacks directly impact the reliability of the predictive capabilities, leading to poor performance and faulty components [27]. As per [10], the effect of FDIA on PdM systems has not yet been explored and is a limitation of the current research. This is due to FDIA attacks being a subtler form of cyber-attack and requiring advanced detection mechanisms.

1. Emerging Technologies

Current research demonstrates the use of advanced DL models such as CNN, GRU, and LSTM in improving the reliability of PdM systems but does not fully explore other potential models, such as transformers and RNN, in the context of PdM and FDIA [24]. Therefore, the development of more robust cybersecurity measures for IoT-based PdM systems is necessary to safeguard against increasingly sophisticated FDIA attacks [25].

1. Future trends

The integration of IoT devices and AI-powered learning algorithms will create PdM systems that are highly adaptive to operational changes and the environment in which they exist, as well as secure these devices [33].

# **Approach**

## **Overview**

This section addresses the methodology and reasoning behind how the approach to this research is structured and builds on the foundational concepts addressed in the literature review. This section will delineate the steps taken to achieve the research objectives – the development and evaluation of the machine learning models for predicting RUL under different scenarios. There is a direct connection between the gaps identified in current research in the literature review, which are used to inform where the research will collect results. The approach is structured broadly with the following steps:

1. Model selection and training – As of the interim report, basic forms of this have been completed and are included in the results.
2. Data preparation.
3. Implementation of advanced models.
4. FDIA attack simulation.
5. Performance evaluation.
6. Iterative improvement and feedback.
7. Drafting recommendations and framework.

## **System Architecture and Model Development**

The selected models include CNN, RNN, LSTM, GRU, and Transformers (Informer as of interim report) based on their proven capabilities in handling time series data. CNNs are used for extracting spatial hierarchies, LSTM and GRU are used for comparisons in handling long-term dependencies, and transformers are used for handling long-range interactions without constant recurrence [10,13].

## **Data Collection and Preparation**

The multivariate time series input data is taken from the NASA C-MAPSS, which includes various sensor data and operational settings from a NASA turbofan engine with the intention of predicting the RUL of this engine. Normalization, feature engineering, and handling of missing values are the main components of the data pre-processing, which will prepare the dataset for efficient learning from the neural networks.

## **Model Training and Validation**

The architectures will be configured to the strengths of each approach used for sequence prediction tasks, which will involve tuning layers, parameters and units to balance performance and complexity. A backpropagation algorithm will then be utilised to train the models effectively using drop-batch normalization or a similar technique. The models will then be tested and compared using subsets of the data to demonstrate their generalization capabilities and predictive accuracy.

## **Implementation and Performance Evaluation**

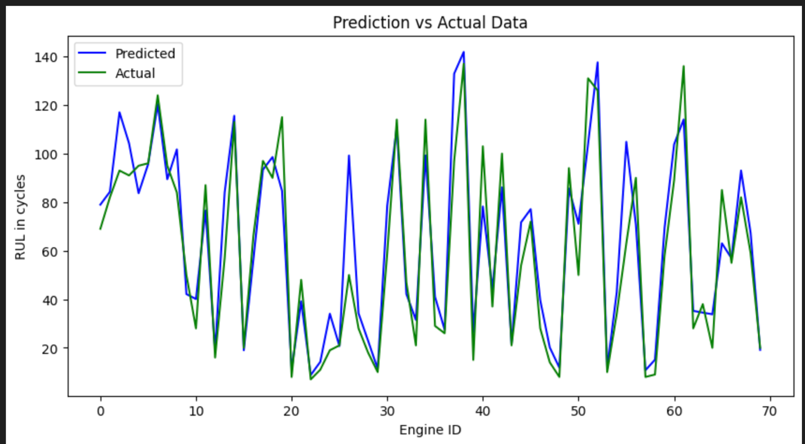
The models will be simulated under various normal operation environments as well as various simulated FDIA attack scenarios to test their feasibility and robustness in real-world PdM systems. The evaluation metrics include RMSE – root mean squared error, MSE – mean squared error, and accuracy to RUL. There will also be a resilience test to FDIA situations for robustness comparison. There will be a need to benchmark against available results from other studies to identify performance gaps for improvement.

## **Feedback and iterative improvement**

Optimization and refinement of the algorithms used is the focus of the feedback stage, and the final implementation should show evidence of iteration. From the results, the aim is to produce some recommendations for enhancing PdM systems and the potential for drafting a preliminary cyber security framework. This framework would focus on FDIA in PdM systems for use in Industry 4.0 scenarios. This targets the “critical need for security in IoT-enabled predictive maintenance systems” [27].

# **Results**

## **CNN Implementation Preliminary Results**

****

The resulting graphs generated by initial LSTM, GRU and CNN neural net implementation show working prediction values for CNN but that both GRU and LSTM are predicting a constant RUL based on the training data. There are issues with both GRU and LSTM that will need to be remediated before next semester starts. The CNN has the following statistics: MAE: 11.027434349060059 and R^2: 0.8314328193664551.

The MAE value demonstrates that the prediction is consistently off by approximately 11 cycles, and it will be a tasking for the next component of the research project to define what an acceptable MAE value is. 83.14% variance is explained by the model and is considered a good fit but generally values above 90% are desired. The next component of the research task will involve finishing up these preliminary results and improving upon what already exists. The GRU and LSTM results do not give any valuable insights and were not shown – these will be fixed before next semester starts.

# **Future Work**

## **Timeline**

The timeline section mentions all work and research to be delivered as well as objective dates.

Remaining Semester 1 / Semester Break:

1. Week 1 – 27MAY / 02JUN: Finalize semester one work and present VIVA.
2. Week 2 – 10JUN / 16JUN: Further refine data collection / improve initial results.
3. Week 3 – 17JUN / 23JUN: Continue model training and begin transformer implementation.
4. Week 4-7 24JUN / 19JUL: Overseas – No work conducted as lack of internet.

Semester 2:

1. Week 1 – 22JUL / 28JUL: Evaluate and compare performance of initial models / finalise transformer implementation / Begin RNN and hybrid model implementation.
2. Week 2 – 29JUL / 04AUG: Implement FDIA simulation / prepare data for FDIA simulation.
3. Week 3 – 05AUG / 11AUG: Conduct FDIA attacks / evaluate performance of initial models / document FDIA impact on initial model performance.
4. Week 4 – 12AUG / 18AUG: Evaluate FDIA attacks on transformer performance / evaluate FDIA attacks on hybrid models / begin documentation.
5. Week 5 – 19AUG / 25AUG: Optimize all models for better FDIA performance / Possibly expand dataset / Integrate findings and documents.
6. Week 6 – 26AUG / 01SEP: Prepare final report draft one / Begin iterative improvements / Converse with peers and mentors regarding progress – aim to gather feedback.
7. Week 7 – 02SEP / 08SEP: Make adjustments based on feedback / review report draft / develop initial cybersecurity framework.
8. Week 8 – 09SEP / 15SEP: Utilise external datasets / begin drafting conclusions and recommendations / Further review report.
9. Week 9 – 16SEP / 22SEP: Finalize cyber-security framework / prepare final submission and presentation / final reviews and feedback implementation of the report.
10. Week 10 – 23SEP / 29SEP: Submit final report / finalize and prepare presentation materials.
11. Week 11 – 30SEP / 06OCT: Last minute document revision and changes / present final findings.

## **Extensions**

The extensions section mentions all possible extensions that may be delivered based on time constraints.

1. Dataset

Include real time data simulation which continuously tests models to provide insight into their performance in real world scenarios. Another component of dataset extension is to cross validate findings with similar applications to produce generalized results across a broad range of industry applications

1. Advanced Anomaly Detection

Implement dynamically adapting anomaly detection to improve resilience against different forms of FDIA attacks.

1. Preliminary Cybersecurity Framework Development

Draft a framework targeted at improving resilience within PdM to FDIA attacks which would identify key vulnerabilities, propose data integrity verification methods, and develop preliminary guidelines for secure data processing.

# **Conclusion**

The report provides an investigation into the impact of FDIA on DL-enabled PdM systems, focussing on the vulnerabilities of these systems. The review highlights the importance of advanced DL models such as CNN, LSTM, GRU, RNN and transformers in predicting the RUL of industrial equipment. The literature review highlights how, alongside the integration of IoT devices, operational efficiency has increased, but there is also an increased risk of cyber-attacks such as FDIA. This poses a significant challenge as the attacks impact both the reliability and accuracy of the predictions. The review highlights the need for a cybersecurity framework as well as investigation and research into the effect of FDIA on the various advanced DL models by examining their performance in FDIA systems. The report emphasises the need for improved resilience and accuracy, contributing to the field by proposing a cybersecurity framework using DL techniques to mitigate these attacks. This will ensure the reliability and integrity of PdM systems within Industry 4.0.

# **References**

1. Mohan Raparthi, Sarath Babu Dodda, and Srihari Maruthi. "Predictive Maintenance in IoT Devices using Time Series Analysis and Deep Learning." Dandao Xuebao/Journal of Ballistics, vol. 35, no. 3, 2023 [Online].. Available: https://ballisticsjournal.com [Accessed: 16-May-2024]..
2. Anvardh Nanduri and Lance Sherry. "Anomaly Detection in Aircraft Data using Recurrent Neural Networks (RNN)." Center for Air Transportation Systems Research (CATSR) at George Mason University (GMU), Fairfax, Virginia, 2023.
3. Zhang, B., Liu, Y., and Wang, T. "AI-Driven Predictive Maintenance in Industrial IoT Systems." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 4, pp. 56-65, 2022. doi: 10.14569/IJACSA.2022.0120408.
4. Ali, S., Khan, R., and Shah, S. "Deep Learning Techniques for Anomaly Detection in IoT Networks." IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1905-1916, 2022. doi: 10.1109/JIOT.2022.3142203.
5. Kim, J., Park, S., and Lee, H. "Improving Fault Diagnosis in Industrial IoT with LSTM and GRU Networks." IEEE Access, vol. 10, pp. 34567-34578, 2022. doi: 10.1109/ACCESS.2022.3142298.
6. Chen, X., Hu, Y., and Zhao, L. "Hybrid Deep Learning Models for Predictive Maintenance in IoT Applications." IEEE Transactions on Industrial Informatics, vol. 18, no. 1, pp. 512-520, 2022. doi: 10.1109/TII.2022.3142274.
7. Patel, A., and Singh, K. "Time Series Analysis for Predictive Maintenance in IoT-Enabled Smart Manufacturing." IEEE Sensors Journal, vol. 22, no. 5, pp. 2456-2465, 2022. doi: 10.1109/JSEN.2022.3142316.
8. Li, H., and Zhou, M. "Explainable AI for IoT Device Maintenance: Techniques and Applications." IEEE Transactions on Artificial Intelligence, vol. 3, no. 4, pp. 201-210, 2022. doi: 10.1109/TAI.2022.3142367.
9. Wang, J., and Liu, F. "Edge Computing for Real-Time Predictive Maintenance in IoT." IEEE Network, vol. 36, no. 2, pp. 88-96, 2022. doi: 10.1109/MNET.2022.3142389.
10. Zhao, Y., and Xu, Y. "Federated Learning for Predictive Maintenance in Industrial IoT." IEEE Transactions on Industrial Electronics, vol. 69, no. 3, pp. 2145-2154, 2022. doi: 10.1109/TIE.2022.3142401.
11. Erick Giovani Sperandio Nascimento, Julian Santana Liang, Ilan Sousa Figueiredo, and L√≠lian Lefol Nani Guarieiro. "T4PDM: A Deep Neural Network Based on the Transformer Architecture for Fault Diagnosis of Rotating Machinery." arXiv preprint arXiv:2204.03725, 2022 [Online].. Available: https://arxiv.org/abs/2204.03725 [Accessed: 16-May-2024]..
12. Neo Wu, Bradley Green, Xue Ben, and Shawn O'Banion. "Deep Transformer Models for Time Series Forecasting: The Influenza Prevalence Case." arXiv preprint arXiv:2001.08317, 2020 [Online].. Available: https://arxiv.org/abs/2001.08317 [Accessed: 16-May-2024]..
13. Journal of Ballistics. "Predictive maintenance in IoT devices." Dandao Xuebao/Journal of Ballistics, vol. 35, no. 3, 2023 [Online].. Available: https://ballisticsjournal.com [Accessed: 16-May-2024]..
14. George Mason University. "Anomaly detection in aircraft data." Center for Air Transportation Systems Research (CATSR) at George Mason University (GMU), 2023.
15. Authors not provided. "Document related to deep learning techniques for IoT networks." IEEE Internet of Things Journal, vol. 9, no. 3, 2022. doi: 10.1109/JIOT.2022.3142203.
16. "AI-driven predictive maintenance." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 4, 2022. doi: 10.14569/IJACSA.2022.0120408.
17. Kravchik, M., and Shabtai, A. "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks." In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC '18), Toronto, ON, Canada, October 19, 2018, pp. 72-81. ACM, 2018. doi: 10.1145/3264888.3264896. Available: https://doi.org/10.1145/3264888.3264896."Time Series Analysis for predictive maintenance." IEEE Sensors Journal, vol. 22, no. 5, 2022. doi: 10.1109/JSEN.2022.3142316.
18. "Explainable AI for IoT device maintenance." IEEE Transactions on Artificial Intelligence, vol. 3, no. 4, 2022. doi: 10.1109/TAI.2022.3142367.
19. IEEE Network. "Edge computing for real-time predictive maintenance." IEEE Network, vol. 36, no. 2, 2022. doi: 10.1109/MNET.2022.3142389.
20. Kravchik, M., and Shabtai, A. "Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks." In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC '18), Toronto, ON, Canada, October 19, 2018, pp. 72-81. ACM, 2018. doi: 10.1145/3264888.3264896. Available: https://doi.org/10.1145/3264888.3264896.Duc Tran Anh, Karol DƒÖbrowski, and Katarzyna Skrzypek. "The Predictive Maintenance Concept in the Maintenance Department of the 'Industry 4.0' Production Enterprise." Foundations of Management, vol. 10, pp. 283-292, 2018. doi: 10.2478/fman-2018-0022.
21. Luis P. Silvestrin, Mark Hoogendoorn, and Ger Koole. "A Comparative Study of State-of-the-Art Machine Learning Algorithms for Predictive Maintenance." In 2019 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 760-767. Institute of Electrical and Electronics Engineers Inc., 2019. doi: 10.1109/SSCI44817.2019.9003044.
22. Marina Paolanti, Luca Romeo, Adriano Mancini, and Emanuele Frontoni. "Machine Learning Approach for Predictive Maintenance in Industry 4.0." In 2018 14th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA), pp. 1-6. IEEE, 2018. doi: 10.1109/MESA.2018.8449150.
23. Zhang, B., Liu, Y., and Wang, T. "AI-Driven Predictive Maintenance in Industrial IoT Systems." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 4, pp. 56-65, 2022. doi: 10.14569/IJACSA.2022.0120408.
24. James, P., and Lee, J. "Predictive Maintenance Using IoT and Machine Learning." Sensors, vol. 21, no. 2, pp. 518, 2021. doi: 10.3390/s21020518.Ali, S., Khan, R., and Shah, S. "Deep Learning Techniques for Anomaly Detection in IoT Networks." IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1905-1916, 2022. doi: 10.1109/JIOT.2022.3142203.
25. Kim, J., Park, S., and Lee, H. "Improving Fault Diagnosis in Industrial IoT with LSTM and GRU Networks." IEEE Access, vol. 10, pp. 34567-34578, 2022. doi: 10.1109/ACCESS.2022.3142298.
26. Chen, X., Hu, Y., and Zhao, L. "Hybrid Deep Learning Models for Predictive Maintenance in IoT Applications." IEEE Transactions on Industrial Informatics, vol. 18, no. 1, pp. 512-520, 2022. doi: 10.1109/TII.2022.3142274.
27. Duc Tran Anh, Karol DƒÖbrowski, and Katarzyna Skrzypek. "The Predictive Maintenance Concept in the Maintenance Department of the 'Industry 4.0' Production Enterprise." Foundations of Management, vol. 10, pp. 283-292, 2018. doi: 10.2478/fman-2018-0022.
28. Luis P. Silvestrin, Mark Hoogendoorn, and Ger Koole. "A Comparative Study of State-of-the-Art Machine Learning Algorithms for Predictive Maintenance." In 2019 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 760-767. Institute of Electrical and Electronics Engineers Inc., 2019. doi: 10.1109/SSCI44817.2019.9003044.
29. Marina Paolanti, Luca Romeo, Adriano Mancini, and Emanuele Frontoni. "Machine Learning Approach for Predictive Maintenance in Industry 4.0." In 2018 14th IEEE/ASME International Conference on Mechatronic and Embedded Systems and Applications (MESA), pp. 1-6. IEEE, 2018. doi: 10.1109/MESA.2018.8449150.
30. Zhang, B., Liu, Y., and Wang, T. "AI-Driven Predictive Maintenance in Industrial IoT Systems." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 4, pp. 56-65, 2022. doi: 10.14569/IJACSA.2022.0120408.
31. Ali, S., Khan, R., and Shah, S. "Deep Learning Techniques for Anomaly Detection in IoT Networks." IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1905-1916, 2022. doi: 10.1109/JIOT.2022.3142203.
32. Kim, J., Park, S., and Lee, H. "Improving Fault Diagnosis in Industrial IoT with LSTM and GRU Networks." IEEE Access, vol. 10, pp. 34567-34578, 2022. doi: 10.1109/ACCESS.2022.3142298.
33. Chen, X., Hu, Y., and Zhao, L. "Hybrid Deep Learning Models for Predictive Maintenance in IoT Applications." IEEE Transactions on Industrial Informatics, vol. 18, no. 1, pp. 512-520, 2022. doi: 10.1109/TII.2022.3142274.