IoTAI 2025

The Second International Conference on IoT-AI

ISBN: 978-1-68558-286-9

July 6th– 10th, 2025

Venice, Italy

IoTAI 2025 Editors

Alexander Lawall, IU International University of Applied Science, Germany

Przemyslaw Pochec, University of New Brunswick, Canada

IoTAI 2025

Forward

The Second International Conference on IoT-AI (IoTAI 2025), held on July 6th – 10th, 2025 focused on blending AI and IoT (Applied intelligence) to various domains.

Joining Artificial Intelligence (AI) and Internet of Thinks (IoT) is a technical convenience of complementary capabilities. IoT deals with devices interacting using the Internet, while AI makes the devices learn from their data and experience. Almost all domains are greatly benefiting from the marriage IoT-AI for processing high volumes of real-time data. The myriad of IoTs deserves a careful data selection, data patterns identification, controlled frequency for data gathering, high data quality, and appropriate filtering mechanisms.

In essence, by using AI principles and AI-based tools, IoT networks and devices can learn from past decisions, predict future activity, and continuously improve performance and decision-making capabilities. The successful combination of AI and IoT leverages the quality of real data to benefit system customers.

We take here the opportunity to warmly thank all the members of the IoTAI 2025 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to IoTAI 2025. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

We also thank the members of the IoTAI 2025 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that IoTAI 2025 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the area of AI and IoT. We also hope that Venice provided a pleasant environment during the conference and everyone saved some time to enjoy the historic charm of the city.

IoTAI 2025 Chairs

IoTAI 2025 Steering Committee

Narito Kurata, Tsukuba University of Technology, Japan
Yasushi Kambayashi, Sanyo-Onoda City University, Japan
Bharath Sudharsan, General Motors, Ireland
Christoph P. Neumann, Ostbayerische Technische Hochschule Amberg-Weiden, Germany
Young-Joo Suh, POSTECH, South Korea
Marko Jäntti, University of Eastern Finland, Finland

IoTAI 2025

Committee

IoTAI 2025 Steering Committee
Narito Kurata, Tsukuba University of Technology, Japan
Yasushi Kambayashi, Sanyo-Onoda City University, Japan
Bharath Sudharsan, General Motors, Ireland
Christoph P. Neumann, Ostbayerische Technische Hochschule Amberg-Weiden, Germany
Young-Joo Suh, POSTECH, South Korea
Marko Jäntti, University of Eastern Finland, Finland
Alexander Lawall, IU International University of Applied Science, Germany

IoTAI 2025 Technical Program Committee

Zainab Abouelhassan, Kuwait College of Science and Technology (KCST), Kuwait
Assiya Akli, National School of Applied Sciences | Ibn Tofail University, Kenitra, Morocco
Jameela Al-Jaroodi, Robert Morris University, USA
Abdullah Al-Khatib, Technical University Chemnitz, Germany
Prashant Anantharaman, Narf Industries, USA
Yang Bai, University of Maryland College Park, USA
Grigorios N. Beligiannis, University of Patras - Agrinio Campus, Greece
Zoran Bojkovic, University of Belgrade, Serbia
Yi Chen, National Sun Yat-sen University, Taiwan
Hongmei Chi, Florida A&M University, USA
Kuan-Lin Chiu, Columbia University, USA
Giulia Cisotto, University of Trieste, Italy
Volkan Dedeoglu, CSIRO, Australia
Declan Delaney, University College Dublin, Ireland
Raffaele Della Corte, Federico II University of Naples, Italy
Shakib Mahmud Dipto, Old Dominion University, USA / University of Liberal Arts Bangladesh, Bangladesh
Smain Femmam, UHA University France, France
Vasileios Gkioulos, NTNU, Normay
Myriam Guedey, University of Applied Sciences Stuttgart, Germany
Hariyanto Gunawan, Chung Yuan Christian University, Taiwan
Rahul Kumar Hindustani, Government Engineering College, Sheikhpura, India
Mauro Iacono, Università degli Studi della Campania "Luigi Vanvitelli", Italy
Murat Isik, Stanford University, USA
Essa Imhmed, Eastern New Mexico University, USA
Razib Iqbal, Missouri State University, USA
Yasser Ismail, Southern University and A&M College, USA
Rossitza Ivanova Goleva, New Bulgarian University, Bulgaria
Marko Jäntti, University of Eastern Finland, Finland
Bhargavi K, Siddaganga Institute of Technology, Tumakuru, India
Yasushi Kambayashi, Sanyo-Onoda City University, Japan
Alvi Ataur Khalil, Florida International University, USA

Xiangchen Zhao, Pure Storage Inc., USA
Zeljko Zilic, McGill University, Canada

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Enhancing Bike-sharing Demand Forecasting: Anomaly Detection and Feature Selection in LSTM Networks

Pedro Nunes
School of Design, Management and Production Technologies Northern Aveiro
University of Aveiro Oliveira de Azeméis, Portugal
e-mail: pnunes@ua.pt
José Paulo Santos
Department of Mechanical Engineering,
University of Aveiro Aveiro, Portugal
e-mail: jps@ua.pt

***Abstract*—Accurate forecasting of casual bike-sharing demand is crucial for optimizing operations and resource allocation. This study employs a Long Short-Term Memory (LSTM) network to predict hourly bike rentals, incorporating temporal, meteorological, and categorical features. To enhance the model, we integrate an anomaly detection step using the Local Outlier Factor (LOF) method, treating its output as an additional feature. The initial LSTM model achieved a Root Mean Squared Error (RMSE) of 34.26. Incorporating anomaly detection based on weather-related data, such as temperature and humidity, and subsequently removing those features, led to an improved RMSE of 30.86. Feature permutation analysis was then used to assess variable importance. The most critical predictors were whether the day was a working day and which working day it was, highlighting clear behavioral patterns in casual bike-sharing demand. By combining anomaly detection with feature selection, we enhance the interpretability of LSTM-based forecasting models, which are often considered black boxes. Removing redundant features simplifies the model while potentially improving accuracy, making it more transparent and efficient. These findings provide valuable insights for bike-sharing system operators, enabling data-driven decision-making for demand management and operational planning.**

Keywords-LSTM; Bike-Sharing; Feature permutation; Anomaly detection; Interpretability.

I. INTRODUCTION

Accurate forecasting of the demand for bike sharing is essential to optimize operations and improve urban mobility [1]. Various factors influence bike-sharing demand, including built environment characteristics, weather conditions, and temporal trends [2][3]. For example, the authors in [2] demonstrated the impact of urban infrastructure and land use on ridership levels, while [4] investigated the operational challenges associated with bike redistribution to balance demand across stations. Additionally, event detection techniques have been utilized to identify anomalies in bike-sharing data, enhancing forecasting accuracy by accounting for unexpected fluctuations in usage [5].

Recent advancements in Machine Learning (ML) have enabled the development of sophisticated predictive models, such as Deep Learning (DL) approaches, to capture the complex temporal and spatial dependencies inherent in bike-sharing usage patterns [3]. Among these, Long Short-Term Memory (LSTM) networks have shown promise in time-series forecasting due to their ability to model long-term dependencies in sequential data [1]. The authors in [6] conducted a comparative study between multiple linear regression and LSTM models, finding that LSTM significantly outperformed traditional regression techniques in predicting bike-sharing demand when considering time and weather factors.

Recent studies have demonstrated the effectiveness of ML techniques in capturing the complex, non-linear relationships inherent in bike-sharing data. For instance, [7] employed an artificial immune system combined with an Artificial Neural Network (ANN), to predict bike-sharing demand. Similarly, [8] proposed a Spatial-Temporal Graph Attentional LSTM approach that integrates multi-source data, including historical trip records and weather information, to enhance short-term demand predictions. On the other hand, [9] emphasized the importance of analyzing and visualizing bike-sharing demand with outliers, proposing methodologies to model baseline temporal usage patterns and detect significant deviations.

In this study, we employ an LSTM-based approach to predict hourly bike rentals, incorporating temporal, meteorological, and categorical features. To enhance model performance, we integrate an anomaly detection step using the Local Outlier Factor (LOF) method, treating its output as an additional feature. This approach aligns with previous research that highlights the importance of addressing demand variability through advanced modeling techniques [4]. Furthermore, we implement a feature permutation analysis to assess the importance of variables in order to understand the most influential parameters on bike-sharing demand.

One of the key features of the proposed solution is the improvement of the interpretability of LSTM-based forecasting models, which are often seen as black boxes. In realistic contexts, it is of utmost importance to have transparent predictions and to understand the main parameters under the predicted values to optimize operations and decision-making.

The remainder of this document is organized as follows: Section II presents the problem being addressed and describes the dataset used. Section III outlines the proposed combination of anomaly detection and an LSTM network for forecasting bike-sharing demand. Section IV presents and discusses the obtained results. Finally, section V concludes the work.

 ISBN: 978-1-68558-286-9

II. Dataset and problem description

The dataset used in this study originates from the Capital Bikeshare system in Washington, D.C., covering a two-year period from 2011 to 2012. This dataset, originally compiled by Fanaee-T and Gama [5], includes rental data aggregated hourly, and integrates multiple sources of information, including weather data and calendar-based attributes, to provide a comprehensive view of bike rental patterns. The dataset attributes include:

- Temporal attributes: Date (dteday), season (season), year (yr), month (mnth), hour (hr for the hourly dataset), weekday (weekday), and working day (workingday).
- Weather conditions: Weather situation (weathersit), temperature (temp), apparent temperature (atemp), humidity (hum), and wind speed (windspeed).
- Rental information: Count of casual users (casual), registered users (registered), and the total count of rented bikes (cnt).

The primary objective of this study is to develop an accurate model to forecast the hourly bike rental demand for casual users, using an LSTM-based approach. Since this demand is influenced by several factors, such as weather conditions, holidays, and special events, it is intended to incorporate a method for feature importance, in order to assess the factors that most contribute to the model's prediction, thus mitigating the black box nature of most DL models.

III. Methodology

The proposed methodology, depicted in Figure 1, encompasses a preprocessing step that structures the raw data for training the LSTM model. After training, a feature importance analysis is conducted to identify the most relevant features. This process yields a predictive model that forecasts hourly bike-sharing demand while providing insights into the most significant contributing factors.

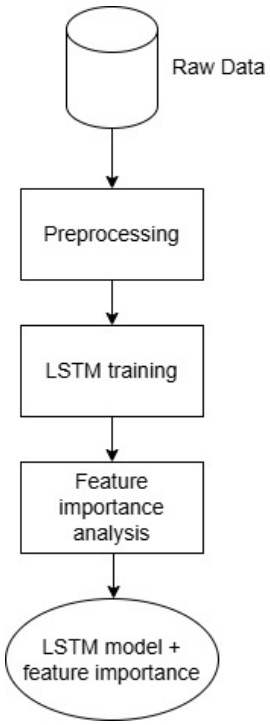


Figure 1. Overview of the proposed methodology.

A. Preprocessing

The preprocessing stage encompasses several steps, as depicted in Figure 2. The dataset includes both numerical and categorical variables. To prepare the data for training the LSTM model, one-hot encoding was applied to transform all categorical variables into numerical representations. Note that the numerical variables are already normalized, and for this reason, there was no need to scale them.

Anomalies and event-driven variations, such as unusual spikes or drops in bike rentals, may arise due to special events or extreme weather conditions [1] [2]. Considering this, the LOF algorithm [10] was employed to identify anomalies in the weather-related data (temperature, humidity, perceived temperature, and windspeed). LOF is an unsupervised anomaly detection method that identifies outliers based on local density variations relative to their neighbors. It quantifies how isolated a data point is by comparing its density to that of surrounding points. The variables used for anomaly detection included:

- *temp:* Normalized temperature;
- *atemp:* Normalized apparent temperature;
- *hum:* Normalized humidity;
- *windspeed:* Normalized wind speed.

In this study, a neighborhood size of 24 points was selected, corresponding to the time window used in the LSTM model, as will be further discussed. The method was implemented using the Scikit-learn library, with a contamination ratio of 0.05.

The LSTMs are a type of Recurrent Neural Networks (RNNs) designed to capture long-range dependencies in sequential data, making it well-suited for time-series forecasting tasks. Unlike traditional RNNs, which suffer from vanishing gradient problems when learning long-term dependencies, LSTMs incorporate specialized gating mechanisms to regulate the flow of information [11].

In this study, the input to the model consists of time-ordered sequences of features extracted from the dataset, including weather conditions, temporal attributes. Each training instance is structured as a rolling window of 24 consecutive hourly observations, where the model uses data from the previous 24 hours to forecast the bike demand for the next hour.

After structured, the dataset was divided in training, validation, and testing instances, maintaining the temporal order, as illustrated in Figure 3. The proportion used was 68-12-20 for training, validation, and test, respectively. By maintaining the temporal order we want to ensure that no data leakage occurs during the training process.

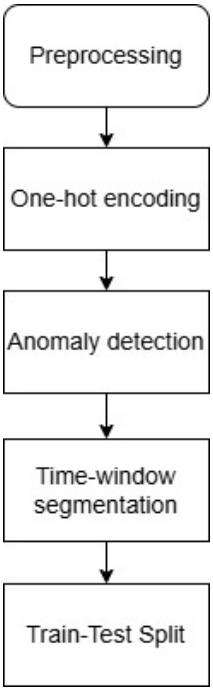


Figure 2. Overview of the proposed methodology.

Figure 3. Overview of the data split, maintaining the temporal order. 68% training data, 12% validation data, and 20% test data.

B. LSTM model training

The time-window size, N_W, for the LSTM was set has 24, since it is reasonable to assume time dependencies of the last day, to forecast casual users of bike-sharing. Figure 4 depicts the structure of the proposed LSTM model. It uses temporal and weather features from the current hour and from the last 24 hours. The output of anomaly detection is also used as feature, but in this scenario, the weather-related features used to compute it, were removed. The LSTM network has one layer with 25 cells, and it is followed by three dense layers with 50,20, and 1 neurons, respectively. After the,e first LSTM, and dense layers, a dropout of 0.1 was used. This model was implemented using Keras and TensorFlow, Python libraries.

We use the Adam optimizer and mini-batch of 32 samples, to optimize the weights and bias of the DL model. The adopted learning rate was 0.001 if the number of epochs was lower than 10, and then decreased according to $l_r(i) = l_r(i-1) * e^{-0.01}$, where $l_r(i)$ is the learning rate of the current epoch. This strategy was chosen to stabilize the training process, leading to better fine-tuning of the model. The maximum number of epochs was set to 100. Note that, to avoid overfitting, the early stop is applied after 10 consecutive epochs with no improvement in the validation score.

C. Feature importance analysis

The feature importance analysis quantifies the contribution of each feature to the LSTM model's predictive performance. We employ the permutation importance technique, which assesses feature relevance by randomly shuffling the values of a given feature and measuring the resulting decline in model performance. The greater the degradation, the more critical the feature is to the model.

One advantage of this method is its model-agnostic nature, meaning it can be applied to any trained estimator. Additionally, by performing multiple permutations, we obtain a measure of variance in the importance scores, enhancing result reliability.

Feature importance is computed by (1), where i_j is the importance of feature j, s is the reference score for the model (e.g., F1-score for classification or RMSE for regression), and K denotes the number of permutations. In this work, we set $K = 5$.

$$i_j = \frac{1}{K} \sum_{k=1}^{K} s_{k,j} - s. \quad (1)$$

IV. Results and Discussion

After obtaining the first LSTM model, by using all features except the anomaly detection output, we evaluated its performance on the test dataset using Root Mean Square Error (RMSE) as the primary metric. Figure 5 displays the predicted and actual values for the number of casual bike-sharing users over the first 10 days of the test period. To enhance visualization, only 240 hours of the test data are shown. The RMSE for the full test set is 34.25, which is reasonable given the range of values observed for casual user counts.

To assess the impact of incorporating anomaly detection, we removed the weather-related features originally used to train the LOF model and instead included the anomaly detection output as an input feature. The model was then retrained. As shown in Figure 5, this revised approach improved the model's performance, reducing the RMSE to 30.86. Additionally, it lowered computational complexity by using fewer input features.

Accurately predicting bike-sharing demand is crucial for optimizing urban mobility decisions. However, beyond predictive accuracy, understanding which factors most influence predictions is essential for informed decision-making. To achieve this, we applied the conditional feature permutation method to evaluate the importance of each input variable. First the correlation matrix was computed for the features, and then features with a correlation higher than 0.75 were shuffled conditionally, to assure that dependencies between features are not broken during the process.

As depicted in Figure 6, the most influential features in the trained model are $workingday$ (indicating whether a day is a weekday or weekend) and the features $weekday\_n$, which identify the day of the week. The seasons of the year

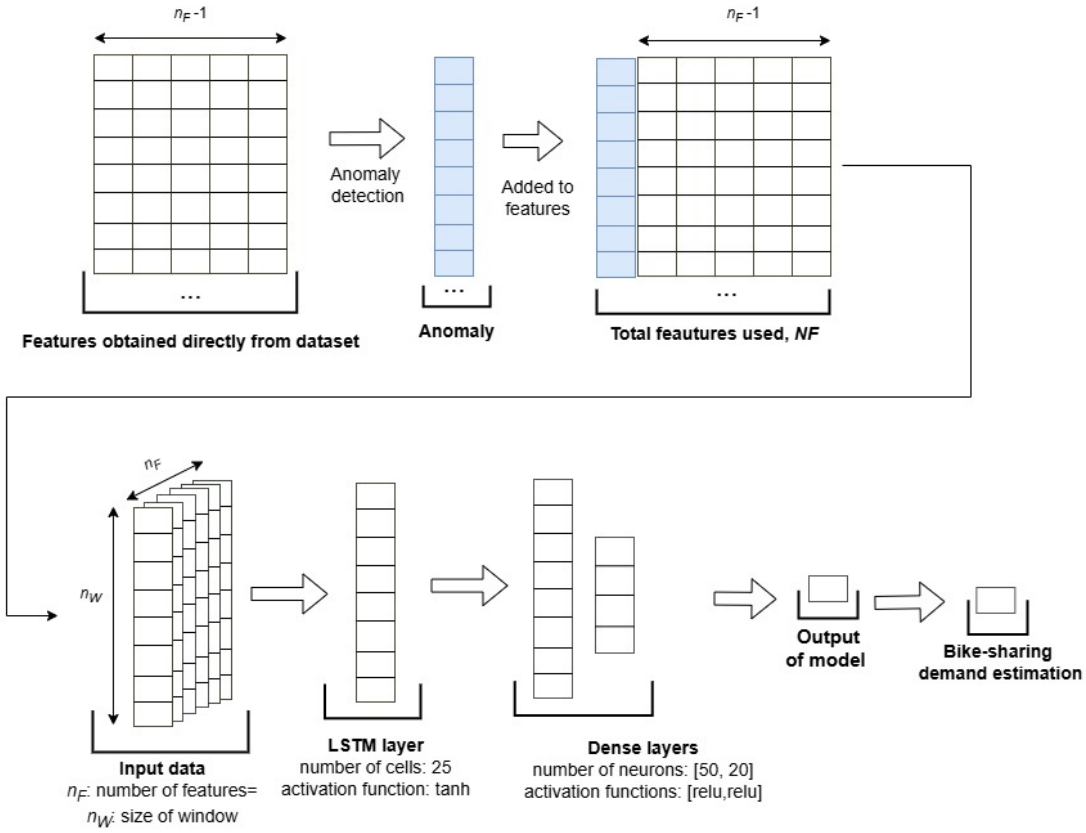


Figure 4. Proposed LSTM architecture.

and general weather conditions $weathersit$ appear to be less significant.

It is interesting to note the features such as temperature (tem), perceived temperature ($atemp$), and wind speed ($windspeed$) have very low importance, since anomaly detection also has low importance, however the anomalies detected using these features as basis have a reduce the computational complexity of the model, while improving its performance. This suggests that instead of absolute weather values, what matters most is whether the weather conditions at a given hour deviate significantly from recent patterns.

Following the initial evaluation, we removed four features (temperature, perceived temperature, humidity, and windspeed), and replaced them by the anomaly detection output. The refined model achieved an improved performance, with an RMSE of 30.86 (compared to 34.26), as depicted in Figure IV. This indicates that combining DL with feature importance analysis and anomaly detection allows us to:

- Identify the most influential features driving the predictions.
- Reduce model complexity by eliminating less relevant variables.
- Maintain comparable predictive performance while using fewer features.

V. CONCLUSION AND FUTURE WORK

This study proposed an LSTM-based approach to forecast hourly bike-sharing demand, incorporating anomaly detection and feature importance analysis. Integrating the LOF method allowed the model to account for unexpected variations in demand, while the feature permutation analysis enabled the identification of the most influential predictors. Results demonstrated that the most critical features were related to the day of the week and whether it was a working day, confirming clear behavioral patterns in casual bike-sharing usage.

Furthermore, the feature selection step reduced model complexity while improving predictive accuracy. This highlights the potential of combining deep learning with explainability techniques to enhance both performance and interpretability in time-series forecasting tasks.

Future work could explore advanced interpretability methods for deep learning models, such as SHAP (Shapley Additive Explanations) and Integrated Gradients, to provide deeper insights into feature contributions. Additionally, investigating attention mechanisms in LSTM or Transformer-based models could improve both transparency and predictive accuracy. Expanding the methodology to different bike-sharing systems and urban contexts would also help validate its applicability and robustness.

Another promising line of research involves the integration

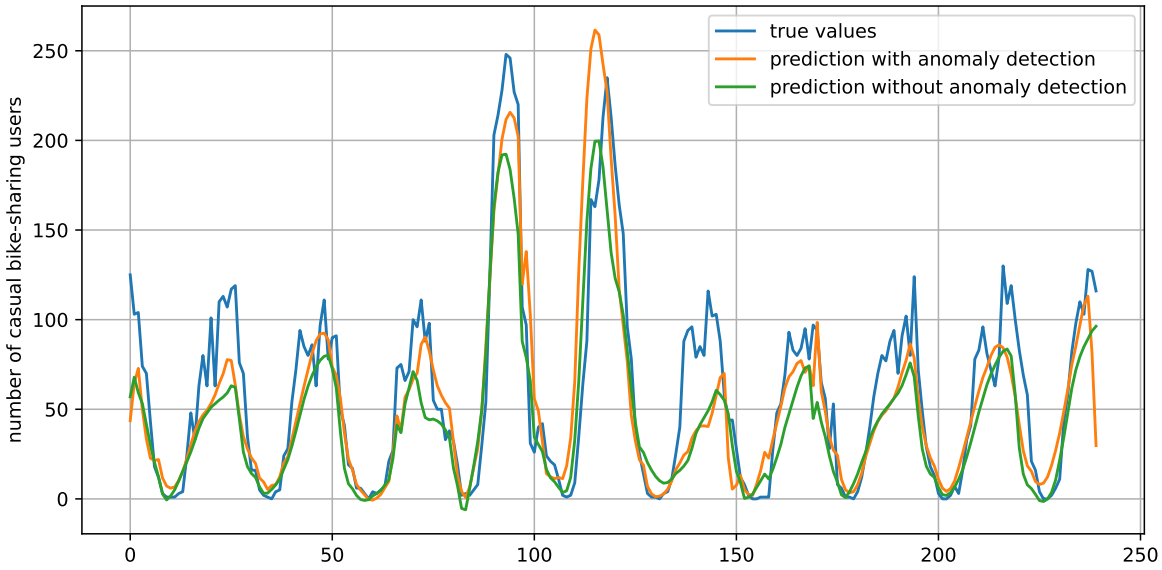


Figure 5. Comparison between prediction scenarios with anomaly detection, and with no anomaly detection for the first 10 days of test data (240 hours).

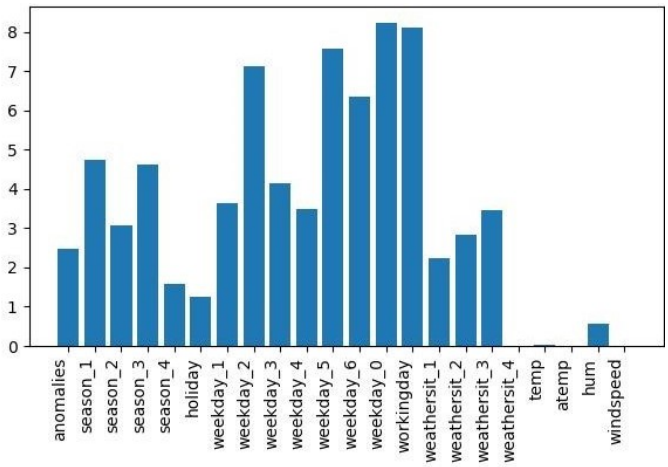


Figure 6. Feature importance obtained through conditional feature permutation.

of IoT modules directly into bike-sharing systems, enabling the real-time collection of weather-related data, such as temperature and humidity, as well as automated user counting, as proposed by [12]. Combined with additional sensors like accelerometers and GPS, this setup could offer valuable insights into user preferences and mobility patterns. Such data could support the development of real-time, context-aware route recommendation systems for cyclists, as explored in [13].

ACKNOWLEDGMENTS

This study was developed within the scope of Project AM2R [C644866475-00000012 – Project No. 15], funded by the PRR – Recovery and Resilience Plan under the Next Generation EU from the European Union. Laboratory support was provided by the projects UIDB/00481/2020 and UIDP/00481/2020, financed by FCT – Fundação para a Ciência e a Tecnologia (DOI: 10.54499/UIDB/00481/2020 and DOI: 10.54499/UIDP/00481/2020).

REFERENCES

[1] "Predicting station-level hourly demand in a large-scale bike-sharing network: A graph convolutional neural network approach," *Transportation Research Part C: Emerging Technologies*, vol. 97, pp. 258–276, Dec. 2018, ISSN: 0968090X. DOI: 10.1016/j.trc.2018.10.011.

[2] W. El-Assi, M. S. Mahmoud, and K. N. Habib, "Effects of built environment and weather on bike sharing demand: A station level analysis of commercial bike sharing in toronto," *Transportation*, vol. 44, pp. 589–613, 3 May 2017, ISSN: 15729435. DOI: 10.1007/s11116-015-9669-z.

[3] E. Eren and V. E. Uz, "A review on bike-sharing: The factors affecting bike-sharing demand," *Sustainable Cities and Society*, vol. 54, p. 101 882, Mar. 2020, ISSN: 22106707. DOI: 10.1016/j.scs.2019.101882.

[4] T. Raviv, M. Tzur, and I. A. Forma, "Static repositioning in a bike-sharing system: Models and solution approaches," *EURO Journal on Transportation and Logistics*, vol. 2, pp. 187–229, 3 Aug. 2013, ISSN: 21924376. DOI: 10.1007/s13676-012-0017-6.

[5] H. Fanaee-T and J. Gama, "Event labeling combining ensemble detectors and background knowledge," *Progress in Artificial Intelligence*, vol. 2, pp. 113–127, 2-3 Jun. 2014, ISSN: 2192-6352. DOI: 10.1007/s13748-013-0040-3.

[6] X. Zhang, Z. Yu, and C. Xie, "Optimizing bike sharing demand prediction: A comparative study of multiple linear regression and lstm models based on time and weather factors," *Journal of Education, Humanities and Social Sciences*, vol. 42, pp. 353–359, Dec. 2024, ISSN: 2771-2907. DOI: 10.54097/c2934z45.

[7] P.-C. Chang, J.-L. Wu, Y. Xu, M. Zhang, and X.-Y. Lu, "Bike sharing demand prediction using artificial immune system and artificial neural network," *Soft Computing*, vol. 23, pp. 613–626, 2 Jan. 2019, ISSN: 1432-7643. DOI: 10.1007/s00500-017-2909-8.

[8] X. Ma, Y. Yin, Y. Jin, M. He, and M. Zhu, "Short-term prediction of bike-sharing demand using multi-source data: A spatial-temporal graph attentional lstm approach," *Applied Sciences (Switzerland)*, vol. 12, p. 1161, 3 Feb. 2022, ISSN: 20763417. DOI: 10.3390/app12031161.

[9] N. Rennie, C. Cleophas, A. M. Sykulski, and F. Dost, "Analysing and visualising bike-sharing demand with outliers," *Discover Data*, vol. 1, p. 1, 1 Mar. 2023, ISSN: 2731-6955. DOI: 10.1007/s44248-023-00001-z.

[10] M. M. Breuniq, H.-P. Kriegel, R. T. Ng, and J. Sander, "Lof: Identifying density-based local outliers," *SIGMOD Record (ACM Special Interest Group on Management of Data)*, vol. 29, no. 2, pp. 93–104, 2000. DOI: 10.1145/335191.335388.

[11] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, ISSN: 08997667. DOI: 10.1162/NECO.1997.9.8.1735.

[12] P. Nunes, C. Nicolau, J. Santos, and A. Completo, "From a traditional bicycle to a mobile sensor in the cities," SCITEPRESS - Science and Technology Publications, Jul. 2020, pp. 81–88, ISBN: 978-989-758-419-0. DOI: 10.5220/0009349700810088.

[13] P. Nunes, A. Moura, and J. Santos, "Solving the multi-objective bike routing problem by meta-heuristic algorithms," *International Transactions in Operational Research*, vol. 30, pp. 717–741, 2 Mar. 2023, ISSN: 0969-6016. DOI: 10.1111/itor.13114.

Private LoRaWAN Network Deployment in Kuopio, Finland: A Case Study on AI-Based Water-Level Monitoring and Urban Flood Prediction

Markus Aho
UEF Business School, University of Eastern Finland, Yliopistokatu 2, 80100, Joensuu, Finland, markus.aho@uef.fi
Funlus Oy, Sepontie 15, 73300, Nilsiä, Finland, markus.aho@funlus.fi

Marko Jäntti
School of Computing, University of Eastern Finland, Microkatu 1, 70210 Kuopio, Finland,, marko.jantti@uef.fi

Aki Happonen
Savonia University Of Applied Sciences
Microkatu 1, 70210 Kuopio, Finland,
aki.happonen@savonia.fi

Kaapo Pehkonen
Kajaani University of Applied Sciences
Ketunpolku 1, 87100 Kajaani Finland,
Funlus Oy, Sepontie 15, 73300, Nilsiä, Finland,
kaapo@funlus.fi

***Abstract*—This paper addresses the overarching research problem: How can an Artificial Intelligence(AI)-based water-level monitoring service be implemented and deployed for effective flood prediction in an urban environment? To explore this, three research questions are posed: RQ1—What type of network architecture can be used in AI-based monitoring of water levels? RQ2—How can the AI-based water-level monitoring service be implemented regarding devices, components, and AI models? and RQ3—Which challenges are related to the implementation and deployment of the AI-based water-level monitoring service? A private LoRaWAN network was set up in Kuopio, Finland, integrating 16 Elsys ELT Ultrasonic sensors with Kerlink and RAK gateways to monitor stormwater wells despite structural obstacles. The study spanned from Fall 2023 to Spring 2025, employing iterative field tests, AI model comparisons (linear regression, decision trees, random forest), and Information Technology Infrastructure Library (ITIL)-based pattern matching. The findings demonstrate the feasibility and robustness of a tailored IoT network, highlighting best practices for sensor placement, gateway configuration, and predictive analytics. These insights provide a blueprint for other cities aiming to harness low-power technologies and AI for early flood warnings and data-driven urban water management.**

Keywords: LoRaWAN; IoT; Environmental Monitoring; Predictive Maintenance; Artificial Intelligence; Sensor Networks; Gateway Configuration; Field Testing; Kuopio; Random Forest; Implementation; ITIL 4; Pattern Matching

I. INTRODUCTION

The rapid evolution of the Internet of Things (IoT) has led to the emergence of wireless communication technologies designed for low-power, long-range applications. Among these, LoRa (Long Range) and its associated LoRaWAN protocol have attracted significant attention due to their extended coverage, minimal energy requirements, and cost effectiveness [1][2]. In many regions, including Kuopio, commercial networks may be either expensive, unavailable, or unsuitable for specific monitoring needs. In response, deploying a dedicated private LoRaWAN network becomes a viable alternative.

Climate change and urbanization are anticipated to cause more urban floods due to changing precipitation patterns. This necessitates a review of current design practices and the incorporation of climate change impacts into urban drainage systems [3]. In built-up areas where new design methods cannot be fully implemented, focus should shift to early warning and prediction systems based on IoT solutions. IoT refers to systems in which devices automatically transmit data used for monitoring or control over the internet. Wireless communication is typically essential, often relying on Low-Power Wide-Area Networks (LPWAN) [4]. Some of these networks utilize 3GPP-based 5G standards enabling massive Machine Type Communications (mMTC) [5].

Now in the era of Artificial Intelligence (AI), data serve as the foundation for warning and prediction models. In particular, data aggregation and appropriate latency considerations—edge or cloud processing—are crucial to achieving reliable and timely predictions [15]. This paper introduces an AI-assisted IoT system for urban flood prediction built on a private LoRaWAN network in Kuopio, Finland. The system employs three RAK7289 V2 WisGate Edge Pro Gateways with Elsys ELT Ultrasonic Industrial Distance Sensors installed in stormwater wells. Additionally, the Loriot platform was incorporated for network management, and the Tulvia.ai application was developed to provide real-time visualization and alerting services for water-level changes. The paper is organized as follows. Section II describes the theoretical framework. Section III explains the methodology. Section IV discusses the results and analysis, and Section V includes further discussion. Finally, Section VI presents conclusions.

II. THEORETICAL FRAMEWORK

LoRaWAN has gained prominence within the broader ecosystem of low-power wide-area networks (LPWAN) due to its capacity for energy-efficient, long-range data communications in Internet of Things (IoT) applications [1],

[2]. Competing LPWAN architectures (e.g., NB-IoT, Sigfox) also prioritize low power consumption and extended coverage, but LoRaWAN's unique attributes—including license-free frequency operation, adaptable spreading factors, and a star-of-stars topology—make it a compelling choice in challenging urban environments. Finland, for instance, experiences frequent snowfall and sub-zero temperatures that accelerate battery depletion, so the network design must ensure both robust signal propagation and reliable sensor operation. LoRaWAN's ability to support different Classes (A, B, and C) of end devices further enhances flexibility, enabling developers to balance factors, such as latency, power consumption, and communication patterns in varied use cases.

In the context of water-level monitoring, LoRaWAN devices, often placed underground in stormwater wells or obstructed by metal covers, must maintain connectivity despite physical barriers. Chirp Spread Spectrum (CSS) modulation underpins LoRaWAN's robustness, allowing signals to remain intelligible across relatively long distances and through moderate interference [7][16]. Moreover, Adaptive Data Rate (ADR) can automatically adjust a node's spreading factor, power settings, and bandwidth to optimize transmission based on real-world conditions. This adaptability helps preserve device battery life, an essential concern when sensors cannot be easily retrieved for replacement or recharging. Alongside these connectivity advantages, LoRaWAN employs a network server for packet handling, encryption, and device authentication. When environmental monitoring expands to dozens or hundreds of sensors, centralized management enables administrators to handle large volumes of traffic with relative ease.

Despite the importance of reliable data transmission, mere connectivity is not enough in applications where timely interventions, such as flood warnings are critical. Integrating Artificial Intelligence (AI) into environmental monitoring frameworks addresses this gap. Linear regression models, for example, are straightforward to implement but assume direct proportionality between input features (rainfall or temperature) and output (water levels). While suitable for quick or basic predictions, such models can be inadequate when water-level fluctuations exhibit non-linear patterns. Decision trees capture these complexities more effectively, yet they risk overfitting unless carefully tuned. Random forest ensembles, by contrast, aggregate multiple decision trees to produce more robust, accurate forecasts in noisy, real-world data settings [6]. Given the variability of precipitation, runoff, and well infrastructure across city districts, ensemble methods often offer superior performance for short-term water-level prediction.

In line with recent urban flood management studies, such as Kostopoulos et al. [11] and Keung et al. [12], effective solutions often hinge on combining IoT-based sensing networks with sophisticated data analytics pipelines. Recent applications include AI-driven flood depth sensors and real-time dashboards for urban drainage monitoring [12][13][14]. Moreover, Chang and Chang [15] underscore how advanced machine-learning methods and time-series modeling can further refine water-level forecasting, enabling targeted warnings that mitigate flood-related impacts. Together, these studies reinforce the importance of integrated approaches—merging hardware resilience with algorithmic intelligence—to address the multifaceted challenges of urban flooding.

Effective AI-based water-level monitoring also hinges on an appropriate balance between edge and cloud analytics. In many LoRaWAN setups, gateways forward sensor data to network and application servers located in the cloud, leveraging extensive computing and storage capacities for model training and large-scale analytics [4][5]. This configuration is generally sufficient for daily or hourly forecasts, but certain mission-critical scenarios—such as sudden flood events—may demand edge analytics to mitigate latency or manage intermittent connectivity. Whether fully cloud-based or employing a hybrid approach, the final design must consider the computational cost of AI models, sensor data volume, and reliability of internet backhaul.

An additional layer of complexity emerges from the human and organizational factors surrounding IoT deployments. Technical execution alone does not guarantee long-term success. The ITIL 4 framework emphasizes the interplay of multiple dimensions—Information and Technology, People and Processes, Value Streams and Processes, and Partners and Suppliers—to guide service management [8]. For water-level monitoring, "Information and Technology" challenges might include selecting gateways robust enough for harsh conditions. "People and Processes" could manifest in training requirements for field technicians who manage sensor installation and for data scientists who refine AI models. "Value Streams and Processes" directs focus to how data flows from sensor to predictive model, ensuring that insights are delivered to relevant stakeholders in time to prevent or mitigate flooding events. Finally, "Partners and Suppliers" become critical when firmware updates, hardware end-of-life, or differing service-level agreements can undermine a well-designed system. A practical strategy for coping with these variables is the pattern matching technique [9], where observed challenges such as a high sensor failure rate are systematically compared to theoretical predictions from existing literature or known constraints, confirming or refuting underlying assumptions.

By synthesizing the technical benefits of LoRaWAN with AI-driven analytics and structured service management, water-level monitoring systems can transcend basic data collection to achieve near real-time environmental intelligence and situational awareness. LoRaWAN's extended coverage, battery-friendly design, and flexible MAC-layer controls facilitate data acquisition in obstructed urban environments, while AI models transform these data into actionable alerts and forecasts. Simultaneously, frameworks like ITIL 4 ensure that human factors, partner dynamics, and operational workflows receive due attention, creating a holistic service that is both technologically sound and sustainably managed. This integrated view encompassing resilient low-power communication, adaptive AI analytics, and a multidimensional approach to service orchestration—underpins the feasibility of deploying robust,

AI-enhanced water-level monitoring solutions in Kuopio's city area.

III. METHODOLOGY

The methodology of this study was structured around an explorative single case study approach [9] spanning from Fall 2023 to Spring 2025 in Kuopio's city area. In alignment with Yin's definition of a single-case design, the case can be framed as the deployment project of a LoRaWAN-based urban flood prediction system in Kuopio. This approach allowed for an in-depth, context-rich examination of how the network architecture, AI models, and stakeholder processes interact within a real-world setting. Within-case analysis, as described by Eisenhardt [10], was adopted to deepen the understanding of the dynamics at play in this specific municipal context. During the first phase in Fall 2023, sixteen ultrasonic sensors were acquired (Elsys ELT Ultrasonic) and placed in designated stormwater wells. Preliminary site surveys identified each well's physical constraints, such as metal covers and limited space, guiding decisions on sensor mounting and gateway installation. A Kerlink Wirnet iFemtoCell LoRaWAN Gateway served as the core node. Trial runs were performed to verify sensor connectivity and data transmission intervals, after which battery drain studies commenced. Results indicated that sensors operating at high transmission frequency could deplete batteries in roughly 9 months under winter conditions, aligning with the local data logs. Figure 1 illustrates the daily fluctuations in link-quality indicators (RSSI, SNR) and gateway reach, highlighting why adaptive data-rate and multi-gateway diversity are essential for a resilient smart-city LoRaWAN network.

Figure 1. Understanding signal variability helps in designing more resilient networks for smart cities.

In Spring 2024, additional RAK7289 gateways were deployed in strategic locations across Kuopio, aiming to improve coverage in areas where high-rise buildings or underground infrastructure attenuated signals. Antenna orientations and power settings were systematically tested. Network management during this phase was facilitated by the Loriot platform, which provided real-time oversight of gateway status, packet routing, and sensor activations. The Tulvia.ai application was also conceptualized to eventually deliver front-end visualizations and alerts based on aggregated data. The Tulvia.ai application—conceptualised and developed within this project—offers an interactive dashboard for real-time situational awareness (see Figure 2) During these pilot tests, each sensor reported ultrasonic distance measurements at set intervals, enabling near real-time monitoring of water levels alongside signal quality indices like RSSI and SNR.

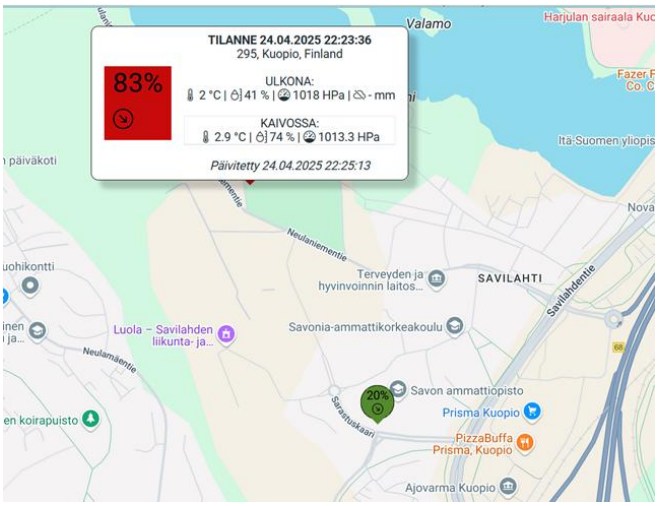


Figure 2. Screenshot of the Tulvia.ai web dashboard (site 295, Kuopio)

From Fall 2024 to Spring 2025, the project shifted toward optimization and AI model integration. Different antenna types, including 5.8 dBi fiberglass antennas and smaller 2 dBi SubG versions, were tested to identify the most effective configuration under Kuopio's urban conditions. Two AI models were then developed: an initial model trained on approximately 10,000 sensor readings, which compared linear regression, decision trees, and random forests for short-term water-level forecasting; and a subsequent model that integrated precipitation and temperature data. As illustrated in Figure 3, the random forest approach consistently demonstrated the highest predictive performance, particularly for the two-hour horizon. The internal structure of the Random-Forest ensemble is illustrated in Figure 4, where the Pythagorean-forest view depicts key splits across the 1 000 constituent trees, revealing heterogeneous yet complementary decision patterns. Maintenance staff feedback led to refined procedures for sensor inspections, especially under winter conditions when snow accumulation, ice, or wind could disturb gateway enclosures.

Model	MSE	RMSE	MAE	MAPE	R2
Linear Regression	142112.666	376.978	115.150	0.050	0.901
Random Forest	9676.905	98.371	20.762	0.007	0.993
Tree	22580.684	150.269	23.685	0.008	0.984

Figure 3. Comparative performance of the AI models

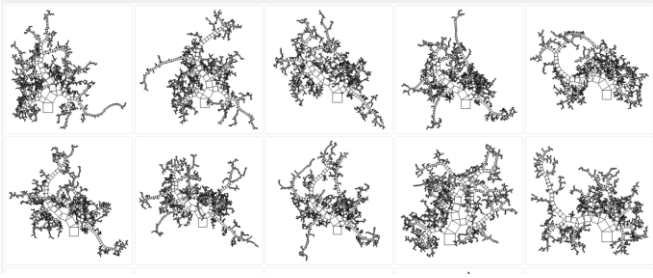


Figure 4. Pythagorean Forest Visualization of Random Forest Models in Orange Data Mining Software

Throughout these phases, both quantitative and qualitative data were collected, reflecting Yin's emphasis on multiple sources of evidence [9] to build a comprehensive case study database. Sensors continuously logged water-level readings, while gateway telemetry captured battery performance, signal strength, and firmware health. Supplementary stakeholder interviews with maintenance technicians, data scientists, and city officials offered perspectives on device calibration, mag-mount reliability, and the complexities of scheduling on-site inspections. Participant observation further enriched the dataset, as researchers took part in the physical tasks of installing gateways, opening wells, and retrieving sensors. Physical artifacts (e.g., sensor mounting hardware, gateway enclosures) also provided tangible evidence for understanding real-world constraints.

The within-case analysis approach advocated by Eisenhardt [10] allowed researchers to delve deeply into the specific operational, technical, and organizational factors shaping the project's outcomes. Data were triangulated across different sources—sensor logs, interviews, field notes, and artifacts—to identify emerging themes and refine implementation practices. A pattern matching analysis [9] systematically compared observed challenges—such as disruptions from metal well covers or sensor detachments—to establish theoretical constraints, confirming the importance of organizational readiness and robust hardware selection for stable LoRaWAN-based monitoring. By incorporating iterative feedback loops, the methodology ensured that insights from each phase informed subsequent optimization, culminating in a data-driven framework for AI-based flood prediction in Kuopio's urban environment.

IV. Results and Analysis

A. *Research Question 1 (RQ1): Network Architecture*

RQ1 asks: What type of network architecture can be used in AI-based monitoring of water levels? In Kuopio's city context, the LoRaWAN-based architecture proved effective due to its low power needs, modular design, and adaptability to various obstructions. Table I summarizes key findings regarding coverage improvement, antenna orientation, power optimization, and the importance of gateway placement near tall buildings.

TABLE I. Findings Related to Network Architecture

Finding	***Data Source***
Multiple gateways improved coverage and reliability.	Field tests, coverage logs
Proper antenna orientation reduced signal degradation in urban areas.	Pilot test measurements
Adjusting transmit power optimized energy consumption	Battery discharge records
Gateway placement was critical for line-of-sight near tall buildings.	GPS-based signal mapping
Well covers and sensor magnetic mounts can impede signal transmission, especially below ground.	Field notes, pilot test results
Strong above-ground signal coverage does not guarantee adequate underground coverage (LoRaWAN signals attenuate quickly); NB-IoT could be tested as an alternative.	Winter field observations
Routers (gateways) and their antennas should be placed as high as possible, ideally with clear line-of-sight, to maximize coverage.	Implementation logs
Changing sensor antenna orientation (vertical vs. horizontal) can modestly improve transmission quality.	Pilot test measurements
Different antenna types feature varying coverage patterns; certain models "hear" better from all directions but with a smaller range, which can be advantageous for underground reception.	Lab and field testing
Building a private LoRaWAN network can be an effective solution in areas with many sensors or lacking a commercial network.	Stakeholder interviews

Through iterative testing, positioning gateways at elevated points and experimenting with different antennas proved beneficial in mitigating coverage blind spots in Kuopio's dense city environment.

B. *Research Question 2 (RQ2): Implementation of the AI-based Service*

RQ2 asks: How can the AI-based water level monitoring service be implemented regarding devices, components, and AI models? A combination of hardware and software components was employed, including resilient LoRaWAN sensors, multiple gateways, the Loriot network server for device authentication and packet forwarding, and an application server that hosted AI-based analytics and the

Tulvia.ai interface. Table II highlights the main implementation aspects, findings, and data sources.

TABLE II. IMPLEMENTATION ASPECTS, FINDINGS, AND DATA SOURCES

Implementation Aspect	*Finding*	*Data Source*
Data Network	5.8 dBi antennas provided adequate coverage in open areas	Interviews, physical artifacts
Sensor Deployment	Magnetic mounts interfered with signal in certain wells.	Field notes, pilot test results
AI Model	Random forest outperformed linear regression & decision trees for short-term forecasting.	Model training logs, local dataset
Maintenance Scheduling	Battery drain rate required adjustments in transmission intervals (~9 months when sending data every two minutes).	Testing data, system logs
Well Access	Stormwater well covers may be buried and not opened for a long time; GPS data can be inaccurate, so extra tools (e.g., shovels, manual searches) are needed to locate and expose the well.	Field notes, additional observations
Mount Reliability	Magnetic sensor mounts do not always hold under winter conditions; two sensors fell into the well, yet one continued to transmit despite immersion.	Winter pilot test results
Weather Conditions	Strong winds, freezing temperatures, and snow accumulation can complicate outdoor gateway installation and affect sensor placement feasibility.	Implementation logs
Private Network Feasibility	Setting up a self-managed LoRaWAN network can be advantageous if there is no commercial LoRaWAN or if a large number of sensors are concentrated in one location.	Stakeholder interviews
Network Management	Platforms like Loriot, WisGate support remote gateway updates, device authentication, and encryption key management, but require technical expertise and adherence to frequency/duty cycle regulations.	Network server logs, vendor docs
AI Model Complexity	If large volumes of sensor data are collected, training AI models (e.g., random forests) can become resource-intensive; cloud computing resources may be required.	Model training logs, interviews
Algorithm Comparison	Lighter models (e.g., linear regression) may be faster to run, while more complex models (e.g., random forest) offer higher accuracy, so balancing speed vs. accuracy is crucial.	Model evaluations

By combining robust network hardware with advanced AI models, the solution ensures both continuous data capture and accurate water-level forecasting, enabling effective early urban flood warning mechanisms. The Tulvia.ai application leverages this data to display real-time water levels, issue alerts, and provide predictive insights to municipal authorities.

C. Research Question 3 (RQ3): Challenges and Pattern Matching

RQ3 asks: Which challenges are related to the implementation and deployment of the AI-based water level monitoring service? Numerous challenges arose, ranging from physical obstructions like metal well covers to organizational factors, such as firmware updates and staff training. These were categorized using a pattern matching technique [9] aligned with ITIL 4 service management dimensions [8]. Table III illustrates the primary findings.

TABLE III. CHALLENGES BY ITIL 4 SERVICE MANAGEMENT DIMENSIONS

Dimension	*Finding*	*Data Source*
Information and Technology	Metal well covers and magnetic mounts disrupted signals; hardware selection proved critical.	Interviews, field notes
People and Processes	Technicians needed re-training on sensors and updated software tools.	Interviews, documentation
Value Streams and Processes	Delays in data flow due to suboptimal network routes impacted real-time analytics.	Network server logs
Partners and Suppliers	Third-party gateway firmware updates occasionally caused minor downtime for gateways. Also misscommunication caused minor delays for logistics (antennas delivery time).	Vendor communication
Information and Technology	Surface-level coverage does not guarantee underground connectivity; thorough on-site testing is required to mitigate well cover interference.	Field notes, pilot tests
People and Processes	Multiple stakeholders in the installation process can delay schedules; staff must coordinate to handle well openings, seasonal conditions, and sensor calibrations.	Maintenance logs, interviews
Value Streams and Processes	Strict duty cycle and frequency regulations must be followed to avoid network congestion and data loss, requiring updated processes for device configuration.	Vendor documentation, local regs
People and Processes	Maintaining a private network demands specialized knowledge of gateway configuration, encryption key management, and sensor troubleshooting.	Stakeholder interviews
Information and Technology	Winter weather can damage or dislodge gateways and sensors, necessitating adjustments to both hardware selection and maintenance schedules.	Field notes, pilot test results

By systematically aligning observed issues with theoretical patterns, the project team was able to implement targeted improvements. This approach confirmed that both technological and human factors must be addressed throughout the entire service lifecycle.

V. DISCUSSION

The findings validate the premise that integrating a private LoRaWAN network with AI-driven analytics can enhance water-level monitoring and urban flood prediction in Kuopio's city area. Early in the research, theoretical arguments emphasized LoRaWAN's adaptability and coverage potential, particularly if antennas and gateways were strategically positioned to overcome obstacles like metal stormwater covers and tall buildings. Empirical results backed these claims; field tests revealed that coverage reliability improved markedly when multiple gateways were installed at higher vantage points, and when antenna power settings were tuned based on real-world signal measurements.

On the AI front, experimental comparisons confirmed that random forests excel in handling non-linear and rapidly changing hydrological data. These findings underscore the value of ensemble methods, particularly when aided by contextual information, such as precipitation and temperature logs. The two-hour forecast window aligns well with the need for timely interventions, granting local authorities enough lead time to respond to imminent surges in well levels or potential flood events. By incorporating these predictive tools into the Tulvia.ai application, city personnel receive actionable updates capable of prompting proactive drainage checks or other preventative measures.

From an organizational standpoint, pattern matching revealed that sensor calibration, firmware updates, and staff training often dictated the project's day-to-day success as much as the underlying technology. Metal well covers, for instance, necessitated repeated on-site adjustments to ensure signals could penetrate effectively. Firmware updates from hardware vendors occasionally introduced compatibility issues, demanding swift responses from the technical team to maintain continuity. Coupled with winter conditions that tested battery performance and sensor stability, these factors reaffirmed the importance of an integrated service management framework (ITIL 4). Ensuring that all stakeholders—maintenance crews, data analysts, municipal decision-makers—operated with a coherent workflow helped preserve the system's overall reliability.

Lastly, the study's results hint at promising avenues for future exploration. Although LoRaWAN proved effective in Kuopio's urban environment, alternative LPWAN technologies, such as NB-IoT, may offer better underground penetration under certain conditions. On the AI side, advanced ensemble or deep-learning models could prove even more accurate given larger datasets that incorporate seasonality and extended climate patterns. Enhanced security measures, including advanced encryption methods and anomaly detection, are also increasingly relevant as IoT data sensitivity grows.

VI. CONCLUSIONS

This study demonstrated the feasibility of deploying a private LoRaWAN network, augmented by AI-based prediction models, to monitor and forecast water levels in Kuopio's city environment. Systematic refinement of network architecture—through gateway placement, antenna configuration, and iterative transmit power adjustments—addressed key challenges linked to metal well covers, tall buildings, and subzero temperatures. The project's phased approach, from sensor installation in Fall 2023 to comprehensive field tests and AI integration by Spring 2025, effectively resolved practical obstacles tied to hardware setup, coverage blind spots, and battery limitations.

Empirical comparisons of AI models indicated that ensemble learning methods, especially random forests, delivered robust short-term forecasts when coupled with local sensor data and environmental metrics. These predictive enhancements can significantly improve municipal responses to sudden well-level changes or urban flooding. At the same time, incorporating an ITIL 4-inspired pattern matching technique confirmed that human factors—ranging from technician retraining to vendor firmware compatibility—must be integrated into planning and operations for the system to remain durable.

Overall, the alignment of low-power IoT infrastructure with AI-driven analytics shows strong potential for proactively managing stormwater wells in Kuopio. In addition to improving local flood preparedness, the results illuminate how future studies might delve deeper into alternative LPWAN technologies, develop advanced machine learning architectures, and strengthen IoT security protocols. By balancing innovative technical solutions with consistent service management practices, this project provides a replicable model for cities seeking to harness IoT data in mitigating flood risks.

ACKNOWLEDGMENT

This work was partially supported by Advanced CoMputing Continuum Solutions for Boosting DigITalization acrOss EUropean RegionS, Grant Agreement: 101115116, funded by the European Union. The views and opinions expressed in this paper are solely those of the author(s) and do not necessarily reflect the official policies or positions of the European Union, the European Innovation Council, or the SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for any use that may be made of the information contained herein.

REFERENCES

[1] Semtech Corporation, "LoRa Technology Overview," 2024. [Online]. https://www.semtech.com/lora [retrieved: April 2025]

[2] LoRa Alliance, "LoRaWAN Specification," 2017. [Online]. https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 [retrieved: April 2025]

[3] Kang, N.; Kim, S.; Kim, Y.; Noh, H.; Hong, S. J.; Kim, H. S. Urban Drainage System Improvement for Climate Change Adaptation. Water 2016, 8, 268. https://doi.org/10.3390/w8070268

[4] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855 – 873, 2017, http://dx.doi.org/10.1109/COMST.2017.2652320

[5] N-N. Dao *et al.*, "A review on new technologies in 3GPP standards for 5G access and beyond," *Computer Networks*, vol. 245, art. no. 110370, 2024. https://doi.org/10.1016/j.comnet.2024.110370

[6] Breiman, L. Random Forests. Machine Learning 2001, 45, 5 – 32. https://doi.org/10.1023/A:1010933404324

[7] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016. http://dx.doi.org/10.1109/MWC.2016.7721743

[8] AXELOS, *ITIL Foundation ITIL 4 Edition*, TSO, 2019.

[9] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th ed. Thousand Oaks, CA: SAGE Publications, 2018.

[10] K. M. Eisenhardt, "Building Theories from Case Study Research," Academy of Management Review, vol. 14, no. 4, pp. 532–550, 1989.

[11] A. Kostopoulos et al., "Boosting Digitalization Across European Regions: The AMBITIOUS Approach," in Artificial Intelligence Applications and Innovations. AIAI 2024 IFIP WG 12.5 International Workshops. AIAI 2024. IFIP Advances in Information and Communication Technology, vol. 715, I. Maglogiannis, L. Iliadis, I. Karydis, A. Papaleonidas, and I. Chochliouros, Eds. Cham: Springer, 2024. https://doi.org/10.1007/978-3-031-63227-3_4

[12] K. L. Keung, C. K. M. Lee, K. K. H. Ng and C. K. Yeung, "Smart City Application and Analysis: Real-time Urban Drainage Monitoring by IoT Sensors: A Case Study of Hong Kong," 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 2018, pp. 521-525 https://doi:10.1109/IEEM.2018.8607303

[13] Chang, L.-C. and Chang, "IoT-based Flood Depth Sensors in Artificial Intelligent Urban Flood Warning Systems," EGU General Assembly 2020, EGU2020-12523, https://doi.org/10.5194/egusphere-egu2020-12523

[14] R. Dhaya, T. A. Ahanger, G. R. Asha, E. A. Ahmed, V. Tripathi, R. Kanthavel, and H. K. Atiglah, "Cloud-Based IoE Enabled an Urban Flooding Surveillance System," Security and Communication Networks, vol. 2022, pp. 1–16, May 2022, https://doi:10.1155/2022/8470496

[15] F.-J. Chang, K. Hsu, and L.-C. Chang, Eds., Flood Forecasting Using Machine Learning Methods. MDPI, 2019, https://doi:10.3390/books978-3-03897-549-6, ISBN: 978-3-03897-5

[16] Reynders, B.; Pollin, S. Chirp Spread Spectrum as a Modulation Technique for Long-Range Communication. In Proceedings of the 2016 Symposium on Communications and Vehicular Technologies (SCVT), Mons, Belgium, 22 Nov 2016; IEEE, pp. 1–5. https://doi.org/10.1109/SCVT.2016.7797659

Predicting Surface Roughness in Titanium Alloy Milling Machining Through Tool Wear Images

Hariyanto Gunawan
Department of Mechanical Engineering
Chung Yuan Christian University
Taoyuan, Taiwan
e-mail: harrywey@cycu.edu.tw

AM Mufarrih
Department of Mechanical Engineering
Chung Yuan Christian University
Taoyuan, Taiwan
e-mail: mufarrih@polinema.ac.id

Chi-Min Chang
Department of Mechanical Engineering
Chung Yuan Christian University
Taoyuan, Taiwan
e-mail: jimmy21262353122385@gmail.com

Zheng-Xin Su
Department of Mechanical Engineering
Chung Yuan Christian University
Taoyuan, Taiwan
e-mail: aa891119@gmail.com

***Abstract*—This study presents a deep learning-based approach to predict surface roughness in the Computer Numeric Control (CNC) milling of Ti-6Al-4V, integrating You Only Look Once (YOLO)v7 for tool wear detection with Long Short-Term Memory/Bidirectional Long Short-Term Memory (LSTM/BiLSTM) for time-series prediction. Images of tool wear are analyzed to extract wear features, which are combined with machining parameters to forecast surface roughness. Experiments were conducted on a vertical milling machine to confirm the effectiveness of the model. YOLOv7 achieved a wear detection accuracy of 92.4%, while BiLSTM attained a prediction of 82.61%, outperforming traditional LSTM. The proposed system offers a reliable solution for intelligent tool condition monitoring and machining quality control.**

Keywords-YOLOv7; BiLSTM; tool wear; surface roughness.

I. INTRODUCTION

In modern manufacturing industries, titanium alloys are widely used in aerospace, biomedical, and marine engineering due to its strength and corrosion resistance [1]. Machining Titanium alloy (Ti-6Al-4V) poses significant challenges, including rapid tool wear because its high hardness, low thermal conductivity, and chemical reactivity. Tool wear significantly impacts surface roughness, influencing dimensional accuracy and production costs [2-4]. Traditional methods to monitor tool wear and surface roughness are offline, time-consuming, and lack predictive capabilities [5]. In recent years, incorporating Artificial Intelligence (AI) and Internet of Things (IoT) has further enhanced the intelligence system of CNC [6]

To address these challenges, this study proposes a hybrid approach that combines vision-based tool wear detection using YOLOv7 with LSTM/BiLSTM based time-series prediction of surface roughness. By integrating machine vision and deep learning, the system aims to provide real-time monitoring and prediction, ultimately supporting process optimization in smart manufacturing.

The structure of this paper is as follows: In section 2, we describe the methodology used, including data collection, preprocessing, and model design. Section 3 presents the experiment design and results. Also, the discussion of the findings and comparative analysis with prior work. Finally, Section 4 concludes the paper and outlines future directions.

II. METHODOLOGY

The proposed framework consists of image acquisition, wear detection, data preprocessing, predictive modeling, and performance evaluation. (1) Tool wear detection. TiAlN-coated tungsten carbide end mills are used for milling Ti-6Al-4V under eight combinations of process parameters (defined via Taguchi L8 orthogonal array). After each trial, the tool wear is examined using a SUPEREYES B008 digital microscope. (2) YOLOv7 model [7]. Tool wear images are annotated into wear and tool regions. YOLOv7 is trained to detect and classify wear into five levels based on the wear area ratio. The tool wear score is calculated as the wear area percentage of the total tool face. (3) Surface roughness measurement. Surface roughness (Ra) is measured at five fixed points on each machined surface using a FBT-650 surface roughness tester. The average Ra is used for model training. (4) Data integration and modeling. The wear scores, tool diameters, spindle speeds, feed rates, and cutting depths form the input features. LSTM and BiLSTM models are trained using 80% of the dataset, while the remaining 20% is used for testing. (5) Model evaluation. Performance is assessed using Mean Absolute Percentage Error (MAPE), accuracy rate, and model loss.

III. EXPERIMENTAL RESULTS AND DISCUSSION

The experimental framework of this study is illustrated in Figure 1. The experiment is structured using the Taguchi L_8 orthogonal array to test four factors at two levels: tool

diameter 3 and 4 mm; spindle speed 3000 and 5000 rpm; feed rate 247 and 300 mm/min; depth of cut 0.5 and 1 mm. Each condition is repeated three times, producing 24 samples. Tool wear image and surface roughness values are recorded for each trial. Figure 2 shows the bounding box and label of the tool and Not Good (NG) for wear characteristics.

The trained YOLOv7 model successfully identifies tool and wear regions with an overall classification accuracy of 92.4%. Five wear grades were established based on wear score distribution (2.1 to 4.9%). Figure 3 shows an example of tool wear level 5 (4.9%). The confusion matrix showed high performance with a precision of 95% and a recall of 93%.

The LSTM model achieved a peak test accuracy of 77.12%, while BiLSTM outperformed it with an accuracy of 82.61%. Figures 4 and 5 show the LSTM and BiLSTM prediction accuracy. The BiLSTM model also exhibited better convergence with a smoother loss curve and lower final error (MSE ≈ 0.005) as shown in Figure 6. The use of bidirectional processing helps capture temporal dependencies more effectively. Taguchi analysis of signal-to-noise (S/N) ratios revealed that feed rate and tool diameter have the greatest impact on Ra. Lower feed (247 mm/min) and smaller tool diameter (3 mm) result in lower surface roughness, as shown in Figure 7.

The results affirm the efficacy of combining vision-based tool wear detection with time-series prediction. BiLSTM is notably superior due to its dual-directional processing, making it suitable for capturing complex temporal features in tool wear evolution. Lower feed rate and shallow depth of cut help maintain surface quality. The approach reduces reliance on offline inspection and enhances adaptive process control.

IV. CONCLUSIONS

This study presents a hybrid intelligent framework that integrates computer vision and deep learning for predictive surface roughness analysis in CNC milling of Ti-6Al-4V. The YOLOv7 model effectively detects and quantifies tool wear, while BiLSTM excels in forecasting surface quality using historical and real-time data. The results validate the models' capability in capturing temporal dependencies and supporting data-driven decision-making in manufacturing. Future work may explore adaptive control and real-time integration with CNC systems.

REFERENCES

[1] Q. Zhao and Q. Sun, "High-strength titanium alloys for aerospace engineering applications: A review on melting-forging process," Mater. Sci. Eng. Vol. 845, pp. 143260-1432642, 2022.

[2] P. M. Huang and C. H. Lee, "Estimation of tool wear and surface roughness development using deep learning and sensors fusion," Sensors. Vol 21(16), pp. 5338-5359, 2021.

[3] R. Kang, H. Ma, Z. Wang, Z. Dong, and Y. Bao, "Effect of tool wear on machining quality in milling Cf/SiC composites with PCD tool," J. Manuf. Process. Vol. 105, pp. 370-385, 2023.

[4] H. Demirpolat, R. Binali, A. D. Patange, S. S. Pardeshi, and S. Gnanasekaran, "Comparison of tool wear, surface roughness, cutting forces, tool tip temperature, and chip shape during sustainable turning of bearing steel," Materials. Vol. 16(12), pp. 4408-4421, 2023.

[5] Q. Wang, H. Wang, L. Hou, and S. Yi, "Overview of tool wear monitoring methods based on convolutional neural network," Appl. Sci. Vol. 11(24), pp. 12041-12063, 2021.

[6] S. Du, "Analysis of the application of intelligent CNC technology in machinery manufacturing," J. Phys. Conf. Ser. Vol. 2649, pp. 012010-012014, 2023.

[7] L. Zhao and M. Zhu, "MS-YOLOv7: YOLOv7 based on multi-scale for object detection on UAV aerial photography," Drones Vol. 7(3), pp. 188-205, 2023.

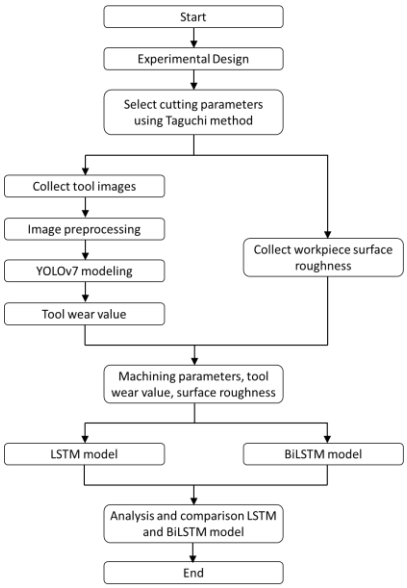


Figure 1. Research workflow

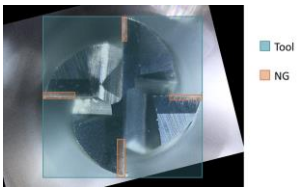


Figure 2. YOLOv7

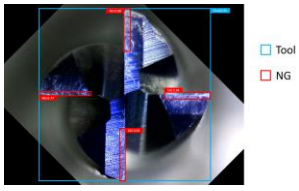


Figure 3. Tool wear level 5 (4.9%)

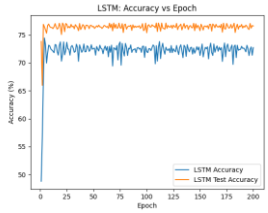


Figure 4. LSTM model accuracy

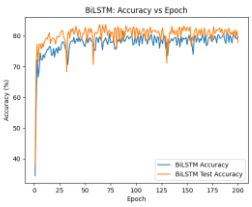


Figure 5. BiLSTM model accuracy

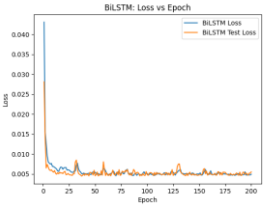


Figure 6. BiLSTM model loss

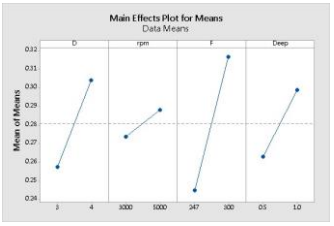


Figure 7. Main effect of surface roughness

Cybersecurity in Civil Aviation – Threat Landscape and Vulnerability Assessment of Attack Vectors

Alexander Lawall
IU International University of Applied Science
Erfurt, Thüringen, Germany
alexander.lawall@iu.org

***Abstract*—The digital transformation of civil aviation has introduced significant cybersecurity risks across interconnected systems such as avionics, air traffic control, and airport infrastructure. This paper examines the evolving threat landscape by identifying key threat actors, attack vectors, and system vulnerabilities. Using a qualitative approach based on expert interviews, the study reveals critical weaknesses in satellite communications, Automatic Dependent Surveillance–Broadcast (ADS-B), and legacy ground infrastructure. Results indicate high susceptibility to cyberattacks due to insufficient encryption, system fragmentation, and outdated protocols. The findings highlight the need for targeted risk assessments, standardized cybersecurity frameworks, and international collaboration to enhance aviation resilience.**

Keywords-Civil Aviation; Cybersecurity; Threat Landscape; Vulnerability Assessment; Attack Vectors; Critical Infrastructure.

I. Introduction

Digital transformation in civil aviation broadens the cyber threat landscape by exposing critical systems to significant vulnerabilities. Ten studies document that key aviation components—including communication, navigation, surveillance, and IT networks—lack robust security measures. For example, researchers report that wireless communication systems are inherently insecure [1] and that aeronautical communication standards rarely incorporate cybersecurity requirements [2]. Authors examining aircraft IT systems note substantial gaps in secure software design and communication practices [3], while studies targeting air traffic management (ATM) propose extended threat models to capture interdependent risks [4]. An analysis of ten identified attack vectors indicates that seven bear high potential impact (e.g., Global Navigation Satellite Systems (GNSS) spoofing, malware injection, ransomware, and ADS-B exploitation) and that detection capabilities mostly remain limited or moderate. Complementary approaches — such as novel risk assessment frameworks [5] and threat taxonomies [6] — illustrate efforts to systematically assess evolving challenges, including those emerging with urban air mobility and unmanned aerial systems [7].

This paper addresses three core research questions:

RQ1 *"Who are the relevant threat actors targeting civil aviation?"*

RQ2 *"What are the critical attack vectors exploited in this domain?"*

RQ3 *"How vulnerable are current aviation systems to these evolving threats?"*

This systematic review examines cybersecurity challenges across commercial aviation systems, encompassing both airborne and ground-based infrastructures [3], [8]. The analysis covers critical aviation components including Communication, Navigation, and Surveillance (CNS) systems, air-ground communication, radio navigation aids, and aeronautical surveillance systems [5]. The research methodology combines systematic reviews with both theoretical and empirical approaches [1], incorporating qualitative analysis through expert perspectives [9] and comprehensive threat assessments [4]. This multi-faceted approach enables a thorough examination of cybersecurity vulnerabilities in modern aviation systems, from aircraft information technology to ATM infrastructure [3], [10].

The paper is structured as follows: Section I introduces the cybersecurity challenges in civil aviation and formulates the key research questions. Section II presents the qualitative research methodology based on expert interviews. In Section III, we analyze the threat landscape by identifying prominent threat actors and their motivations. Section IV categorizes and evaluates the most relevant attack vectors and system vulnerabilities. Section V synthesizes expert insights and identifies key technical and organizational security gaps. Finally, Section VI concludes with the main findings, answers the research questions, and offers recommendations and future research directions.

II. Methodology

This research employs a qualitative methodology to investigate the cybersecurity threat landscape and vulnerabilities in civil aviation systems. The approach was chosen due to the complexity and sensitivity of the topic, which benefits from expert-based insights rather than purely quantitative data.

A. Research Design

The study follows an exploratory and descriptive design. The primary objective was to gather structured knowledge about realistic cyber threats, system vulnerabilities, and the expert perception of risk within the aviation domain. Given the limited publicly available data and operational sensitivity of aviation systems, expert interviews were deemed the most suitable method for data collection.

 ISBN: 978-1-68558-286-9

B. Expert Selection and Sampling

A purposive sampling strategy was employed to identify individuals with relevant professional expertise. Selection criteria included:

- Professional background in civil aviation, ATM, or aircraft systems.
- Specific experience in cybersecurity, cyber risk assessment, or information security.
- Academic or consulting roles with publications or projects in the aviation cybersecurity field.

The experts represented organizations such as aviation authorities, cybersecurity consultancies, aviation software vendors, and research institutions. All participants had more than five years of relevant work experience.

C. Interview Design and Procedure

Semi-structured interviews were conducted to ensure comparability while allowing for flexible and in-depth discussion. The interview guide included thematic blocks related to:

- Identification of relevant threat actors.
- Perception of technical vulnerabilities in airborne and ground systems.
- Assessment of communication protocol security (e.g., ACARS, ADS-B).
- Evaluation of organizational cybersecurity challenges.

Interviews were conducted via video conferencing and lasted between 30 and 60 minutes. With consent, all sessions were recorded and transcribed.

The expert sample comprised five aviation professionals serving as pilots/copilots on aircraft such as the Airbus A320, A330/340, and the CRJ-900. These individuals possessed an average flight experience ranging from 6,000 to 9,000 hours, indicating a high level of operational expertise. All participants were employed by German commercial airlines, providing a consistent organizational backdrop. The interviews focused on critical aspects of aviation cybersecurity, specifically addressing airborne systems, ground infrastructure, and communication links. GNSS, avionics systems, the Aircraft Communications Addressing and Reporting System (ACARS), and threats related to Instrument Landing System (ILS) spoofing are examples.

D. Data Analysis

The transcribed material was analyzed using qualitative content analysis. An inductive coding scheme was developed to identify recurring themes. The analysis focused on clustering insights into threat types, attack feasibility, system weaknesses, and organizational practices. These categories informed the structure and content of the subsequent results and discussion sections.

While this study is grounded in qualitative analysis due to the domain's sensitivity and expert-driven nature, future extensions could explore quantitative methodologies such as the Common Vulnerability Scoring System (CVSS), probabilistic threat trees, or hybrid models in aviation. The assessed risks in this paper are based on preliminary efforts in this direction. The simplified versions (cf. Tables II, III, IV, and V) are related to pilot-centered studies using ICAO Doc 9859-compliant matrices [11], offering a valuable foundation for quantitative risk propagation modeling in aviation cybersecurity.

III. Threat Landscape

Understanding the diverse threat landscape is critical for developing effective cybersecurity strategies in civil aviation. Cybersecurity threats in aviation are evolving with the increasing digitization and integration of ICT tools [10], smart technologies and IoT devices in airports [4]. The aviation sector is confronted by a range of adversaries, each with different motives, capabilities, and targets. This section provides an overview of the primary threat actors and analyzes their motivations and technical capacities.

A. Overview of Threat Actors

Nation-state actors are considered among the most capable and persistent adversaries, pose significant risks to aviation systems, targeting communication networks and avionics for political influence and intelligence gathering [8], [12], [13]. Their motivations typically include political influence, economic disruption, and strategic intelligence gathering. These actors, often operating as Advanced Persistent Threat (APT) groups, have access to substantial resources and engage in long-term operations [10]. The complexity and interconnectedness of Communication, Navigation, and Surveillance (CNS) infrastructure amplify the potential scope of attacks [14]. This includes communication networks, air traffic control infrastructure, or avionics systems [10], [15].

Cybercriminals and hacktivists often exploit known vulnerabilities for financial gain or ideological purposes [4], [16]. Airports and airlines face various cyber risks, including potential loss of passenger information, disruption of operations, and damage to aircraft [17]. Ransomware attacks on airport IT systems and attempts to breach airline customer databases are common examples. Hacktivists may seek to disrupt flight operations or expose perceived injustices using defacement, denial-of-service (DoS) attacks, or information leaks [10], [18].

Insider threats pose a significant cybersecurity risk, often underestimated compared to external attacks [19]. These threats come from individuals with legitimate access, such as employees, contractors, or vendors, who may exploit their knowledge of internal systems and bypass perimeter defenses. The impact of insider attacks can be severe, as evidenced by high-profile cases at companies like Tesla and government agencies like the US Department of Defense [20]. Insiders are particularly dangerous due to their operational knowledge and ability to bypass conventional perimeter defenses [21].

B. Motivations and Capabilities

Threat actors targeting civil aviation operate with a broad spectrum of motivations:

- **Political motivations:** Aimed at destabilizing nations, projecting power, or coercing policy changes (nation-states) [22], [23].
- **Economic motivations:** Including theft of personal data, ransom payments, or illicit trade in sensitive information (cybercriminals) [4], [10].
- **Ideological motivations:** Related to activist agendas or grievances against the aviation industry (hacktivists) [15], [16].

Their capabilities vary widely. Nation-states can exploit zero-day vulnerabilities and conduct coordinated cyber-physical operations [24]. Cybercriminals often rely on off-the-shelf malware and social engineering, whereas insiders leverage their access privileges and domain familiarity to perform covert actions [21]. All actors are increasingly capable of targeting key aviation subsystems, including avionics, ground control centers, and satellite communication links [25].

Table I presents a summary of selected real-world aviation cybersecurity incidents that illustrate the feasibility and impact of documented vulnerabilities.

TABLE I
SELECTED CYBERSECURITY INCIDENTS IN CIVIL AVIATION

Year	Incident	Vector	Impact
2018	Brit. Airways breach	Customer DB	Data theft (£20M)
2020	Ransomware on ST Eng.	Airport MRO	Operations halt
2023	GNSS spoofing Iraq/Iran	GNSS	Position deviat.
2024	Hamburg airport cam. hack	IT system	Public data leak

IV. ATTACK VECTORS AND VULNERABILITIES

This section synthesizes the findings from expert interviews with a literature-based analysis, providing a structured overview of the main attack vectors in civil aviation. It follows the categories of airborne systems, ground infrastructure, and communication links. The complex interplay between airborne, ground, and communication subsystems is illustrated in Figure 1, which highlights how interdependencies across aviation infrastructure expand the cyber attack surface.

The tables (cf. Table II, III and IV) reflect the prioritization of threats as described by expert interviewees and supported by the literature review. In detail, the attack vectors discussed below are derived from a thematic synthesis of the expert interviews and the structured literature review. Key vulnerabilities were categorized where at least two interviewees identified similar risks, which were then cross-validated against peer-reviewed and industry literature. This integration follows principles of inductive qualitative coding and thematic saturation, ensuring methodological rigor in capturing domain knowledge. The likelihood and impact ratings are derived through a triangulated synthesis of literature and practitioner input. Attack vector tables are annotated with expert-based (E), literature-based (L), or combined evidence (E+L), to clarify the provenance of each rating.

A. Airborne Systems

Airborne systems include all onboard digital subsystems, such as avionics, navigation, and communication modules.

Figure 1. Interlinked Systems in Civil Aviation [26]

TABLE II
RISKS IN AIRBORNE SYSTEMS

Attack Vector	Likelihood	Impact	Evidence
Legacy avionics exploitation	Medium	High	E+L
SATCOM command injection	Medium	High	E+L
ADS-B ghost aircraft injection	High	High	E+L
GNSS spoofing/jamming	High	High	E+L

Experts emphasized the high dependency of modern aircraft on complex, interconnected technologies, many of which were not originally designed with cybersecurity in mind. The summary of the risks for airborne systems is shown in Table II.

1) Avionics and Flight Management Systems: Legacy avionics platforms often operate on proprietary or outdated software with limited patching capabilities due to certification constraints [27]. These systems are vulnerable to local and remote exploitation if attackers gain access to maintenance ports or use wireless vectors during pre-flight servicing [28], [29]. According to expert interviews and industry reports, exploitation is considered *moderately likely*, but the *impact is high* due to the proximity of these systems to flight-critical functions.

2) SATCOM and Data Links: SATCOM-based communication plays a central role in long-haul aviation [30]. Experts highlighted that many implementations lack strong encryption or robust authentication, exposing them to spoofing or hijacking attempts [31]. Attackers could theoretically disrupt the data integrity between cockpit and ground services or inject false control commands [30]–[32]. Although complex, such attacks are *technically feasible*, making the *likelihood medium* and the *impact high* due to the potential for operational disruption.

3) ADS-B and GNSS: The ADS-B protocol broadcasts aircraft position data in plaintext, without encryption or authentication [31], [32]. This allows attackers to eavesdrop or inject ghost aircraft into air traffic visualizations [31], [33]. GNSS signals are also weak and susceptible to jamming or spoofing, which can mislead navigation systems [34], [35].

TABLE III
RISKS IN GROUND INFRASTRUCTURE

Attack Vector	Likelihood	Impact	Evidence
Ransomware in airport IT	High	Medium	E+L
ATM network compromise	Medium	High	E+L
Third-party lateral movement	High	Medium	E
Manipulated maintenance records	Medium	High	E+L

TABLE IV
RISKS IN COMMUNICATION LINKS

Attack Vector	Likelihood	Impact	Evi.
ACARS interception	High	Medium	E+L
ACARS message manipulat.	Medium	High	E+L
SWIM data injection	Medium	Medium–High	E+L
VHF/UHF spoofing or jam.	Low–Medium	Medium	E+L

Several real-world incidents (Middle East) validate feasibility [15], [36], [37]. These attacks are *well-documented in research and red-teaming efforts*, making the *likelihood high* and the *impact high*.

B. Ground Infrastructure

Ground-based systems provide essential support for aircraft operations, including logistics, passenger processing, and air traffic control. The following subsystems were identified as critical and the summary of the risks for ground infrastructure is shown in Table III.

1) Airport IT Systems and Networks: Experts reported that airport IT systems are often heterogeneous and difficult to centrally manage [4]. Attack vectors include ransomware, spear-phishing, and lateral movement via third-party contractor access [15], [18]. Ransomware attacks have frequently occurred globally (e.g., ransomware at airport check-in systems) [38], [39], confirming the *high likelihood* also due to weak endpoint protection, though the *impact is considered medium* as the attacks typically affect business continuity rather than flight safety.

2) ATM Systems: Air traffic control environments rely on legacy architectures and software as well as centralized infrastructures [40]. Experts warned that insufficient network segmentation and outdated authentication mechanisms pose severe risks, especially when connected to supervisory control and data acquisition systems [41]. Experts cite complex vendor ecosystems [18]. Access is often poorly segmented, and attackers can escalate privileges across IT networks [42]. The *likelihood is medium* due to controlled access, while the *impact is high* because compromised ATM systems could disrupt national airspace by impacting flight routing, a safety-critical function. Operational disruption in ATM may lead to cascading scheduling effects that indirectly compromise flight safety and emergency response coordination.

3) Supply Chain and Maintenance Systems: Digital systems used for aircraft maintenance, such as electronic logbooks and maintenance management tools, were identified as vulnerable due to limited access control and shared interfaces [27], [42]. Digital systems are exposed via remote or wireless interfaces [43]. If exploited, could lead to incorrect repairs or overlooked issues that allow subtle manipulation of aircraft safety-related data [44]. The *likelihood is medium*, and the *impact is high* due to latent threats to airworthiness.

C. Communication Links

Cybersecurity vulnerabilities in communication links were a key concern across all interviews and the summary of the risks for communication links is shown in Table IV.

1) ACARS and Voice Communications: The ACARS transmits sensitive data like flight plans, fuel status and weather updates over plaintext VHF or SATCOM channels [45], [46]. Experts warned of the ease with which such messages can be intercepted or crafted valid messages can be injected into systems using low-cost software-defined radios [31], [33]. This results in a *high likelihood* for data interception, and a *medium impact* as the intercepted data could support more targeted or disruptive attacks.

2) SWIM and IP-based Protocols: The increasing adoption of System Wide Information Management (SWIM) introduces standardized interfaces for data exchange between aviation actors using standardized APIs over IP [40]. However, this integration also extends the attack surface, especially when IP-based protocols are used without end-to-end encryption [15], [47]. Improper authentication may allow false data exchange (e.g., flight status, weather) [31]. While no public exploitation is known to date, *expert opinion assessed the likelihood as medium* and the *impact as medium to high*, depending on the data affected.

D. Summary of Findings

The aggregated results from expert interviews and supporting literature indicate that cyber risks in civil aviation vary significantly across system categories in both likelihood and potential impact, cf. Table V.

Airborne systems — particularly those relying on outdated avionics or unauthenticated data broadcasts such as ADS-B — were consistently rated as having the highest impact, given their direct connection to flight safety and the limited ability to implement rapid updates due to certification constraints. However, due to more restricted physical and logical access, the likelihood of successful exploitation was generally considered medium to high.

Ground infrastructure, encompassing airport IT, ATM networks, and maintenance systems, presented a higher likelihood of exploitation. This was attributed to the widespread use of commercial off-the-shelf (COTS) components, heterogeneous networks, and extensive third-party integration. Although the immediate safety impact of attacks on ground systems may be lower, operational disruptions and indirect safety effects — such as delayed maintenance updates — elevate the risk severity.

Communication links were assessed to have a medium likelihood of exploitation due to known vulnerabilities in protocols like ACARS and the integration of IP-based systems like SWIM. Experts emphasized that while direct safety effects depend on the attack vector, compromised communication

integrity could result in degraded situational awareness or operational delays.

TABLE V
RISK OVERVIEW BY ATTACK VECTOR CATEGORY

Category	Likelihood	Impact	Evi.
Airborne Systems	Medium–High	High	E+L
Ground Infrastructure	Medium–High	Medium–High	E+L
Communication Links	Low–High	Medium–High	E+L

V. DISCUSSION

This study aimed to provide a comprehensive assessment of cybersecurity threats in civil aviation by combining expert insights with a structured vulnerability evaluation. Unlike prior studies, this paper introduces a layered risk prioritization based on operational pilots' judgment integrated with literature-based scoring. The findings confirm that the aviation sector is facing a complex, multi-dimensional threat landscape characterized by both well-understood and emerging attack vectors.

A. Expert Consensus and Divergences

Across the interviews, there was broad consensus regarding the most critical vulnerabilities: unauthenticated communication protocols (especially ADS-B and ACARS), outdated avionics platforms, and ransomware threats in ground infrastructure. Experts agreed that while the likelihood of attacking airborne systems may be lower due to restricted access and specialized knowledge requirements, the potential impact is significantly higher due to safety-critical dependencies. Conversely, ground systems are more exposed due to extensive third-party integration and reliance on legacy IT architectures.

A distinguishing contribution of this study lies in its triangulated risk synthesis, which not only validates known attack vectors such as ADS-B spoofing and ACARS plaintext but also stratifies their risk severity based on direct expert evaluation. Unlike prior literature reviews, this paper systematically ranks vulnerabilities across airborne, ground, and communication layers, reflecting real-world operator prioritization and threat perception.

Notably, the perception of risk around communication systems varied more significantly among experts. Some emphasized the high exploitability of ACARS and voice channels due to lack of encryption, while others viewed such channels as low-priority targets, arguing that operational redundancy limits their criticality. This divergence points to the need for scenario-based risk modeling to clarify the consequences of link-level compromises.

B. Identified Security Gaps

The results presented in Section IV highlight how cyber threats manifest across system layers. Rather than restating attack vectors, we group observed weaknesses into four overarching categories: (1) legacy systems lacking patchability, (2) insecure-by-design communication protocols, (3) unsegmented network architectures, and (4) limited visibility across operational technology (OT)/IT domains. These categories are not isolated — their interdependencies intensify systemic risk. For example, outdated avionics in airborne systems not only lack encryption but also interact with unverified ground data over ADS-B and SATCOM, compounding threat exposure.

- **Legacy technology**: Many components in avionics and air traffic systems remain unpatched or unsupported, yet are essential to certified aircraft and control operations.
- **Protocol weaknesses**: Unsecured communications (e.g., ADS-B, ACARS) are still in widespread use without industry-wide mandates for cryptographic protection.
- **Insufficient segmentation**: Airport and ATM networks often lack adequate isolation between OT and IT systems, allowing lateral movement in case of breach.
- **Limited situational awareness**: There is a notable gap in the deployment of real-time intrusion detection or anomaly recognition systems tailored for aviation environments.

Synthesizing the results reveals that many risks cannot be addressed at the subsystem level alone. Vulnerabilities in airborne platforms (e.g., legacy flight systems) are often mirrored by insecure communications (e.g., unencrypted ACARS) and exacerbated by permissive ground networks (e.g., shared maintenance IT). These layers form a tightly coupled threat surface where mitigation strategies must be holistic rather than component-specific.

C. Organizational and Regulatory Challenges

Beyond technical vulnerabilities, organizational barriers emerged as a dominant theme. Experts noted that aviation cybersecurity is hindered by inter-organizational complexity and unclear accountability across airline operators, airport authorities, OEMs, and regulators. This diffusion of responsibility contributes to delayed patch cycles, inconsistent incident reporting, and fragmented responses to shared threats.

From a regulatory perspective, initiatives such as the ICAO Cybersecurity Strategy and EASA's oversight programs have made progress in establishing a governance framework. However, practical enforcement and harmonized adoption across countries and actors remain lacking. Several interviewees stressed the importance of moving from voluntary guidance to enforceable minimum cybersecurity baselines, particularly for data integrity and access control in ground-air-ground communication.

D. Strategic Implications

Taken together, the results highlight the need for a layered and aviation-specific cybersecurity approach. Mitigation strategies must prioritize:

- Protection of safety-critical systems (e.g., navigation, control) through isolation and redundancy.
- Gradual deprecation of insecure communication protocols in favor of authenticated, encrypted alternatives.
- Continuous training and threat modeling across operational teams, IT personnel, and aircrew.
- Strengthening of information sharing platforms for threat intelligence between stakeholders.

The findings also support the adoption of advanced monitoring tools (e.g., AI-based intrusion detection) to detect anomalous patterns across OT and IT boundaries. While technical interventions are necessary, a cohesive security culture supported by policy and cross-organizational cooperation is essential to sustaining trust in civil aviation infrastructure.

VI. Conclusion and Future Work

A. Conclusion

This paper investigated the cybersecurity threat landscape in civil aviation by answering three guiding research questions. In addressing RQ1, the study identified nation-states, cybercriminals, and insiders as the principal threat actors. Nation-state adversaries were considered the most capable, often motivated by political or strategic objectives, while cybercriminals targeted economic assets through extortion or data theft. Insider threats, although less visible, remain dangerous due to their system knowledge and access privileges.

For RQ2, the study systematically categorized attack vectors across three critical domains: airborne systems, ground infrastructure, and communication links. Particular emphasis was placed on unauthenticated data links such as ADS-B and ACARS, insecure SATCOM implementations, and legacy airport IT systems. These vectors were identified through both expert elicitation and evidence from past incidents, supporting their relevance and severity.

Addressing RQ3, the research showed that civil aviation systems remain highly vulnerable to cyberattacks. Vulnerabilities were not limited to outdated technologies, but also to organizational fragmentation and limited situational awareness across stakeholders. While the impact of an attack on airborne systems is typically higher due to safety implications, ground and communication systems were found to be more accessible, increasing the likelihood of compromise.

B. Recommendations

Based on these results, the following recommendations are proposed. Each is explicitly linked to the corresponding research question (RQ) to ensure coherence and traceability:

RQ1 (Threat Actors): Aviation regulators and industry actors should establish mandatory information-sharing frameworks and joint cyber exercises to enhance situational awareness and resilience across organizational boundaries. These measures address the complex threat actor landscape — ranging from state-sponsored APTs to insider threats — by strengthening collaborative defense mechanisms and reducing organizational silos.

RQ2 (Attack Vectors): The adoption of secure communication protocols, such as encrypted ADS-B, IP-authenticated SWIM, and secure ACARS variants, must become mandatory. These steps directly mitigate attack vectors that exploit unauthenticated or plaintext messaging formats, which are prevalent in both airborne and ground-air communication systems.

RQ3 (System Vulnerability): Addressing systemic vulnerabilities requires both technical retrofitting and architectural modernization. Legacy avionics and airport IT systems must be upgraded using secure-by-design principles despite long certification cycles. In parallel, strict network segmentation and anomaly detection tailored to OT/IT hybrid environments should be deployed to detect and contain threats across domain boundaries. These controls improve visibility into lateral movements and cross-layer attacks, especially in supply chain and maintenance subsystems.

Strategic Roadmap for Mitigation: To operationalize the recommendations and support implementation across the aviation sector, a phased roadmap is proposed. This roadmap spans short-, mid-, and long-term actions, corresponding to technical, infrastructural, and governance domains:

In the short term, priority should be given to securing vulnerable communication protocols. This includes deploying encryption and authentication mechanisms for ADS-B and ACARS transmissions, as well as enforcing strict access control policies for SWIM interfaces.

In the mid term, focus must shift to infrastructure hardening. Key actions involve segmenting ATM and airport IT networks to reduce lateral movement risk, and upgrading airport systems that currently rely on outdated or unsupported software components.

In the long term, sustainable cybersecurity in civil aviation requires robust governance mechanisms. These include mandatory coordinated vulnerability disclosure programs, harmonized reporting obligations across national aviation authorities, and alignment with international cybersecurity baselines as advocated by ICAO and EASA.

C. Future Work

Quantitative modeling and simulation frameworks should be developed to better understand risk propagation and system dependencies across aviation domains. These models can support scenario-based planning and incident response.

Advanced machine learning techniques offer potential for anomaly detection in avionics and ATM environments. Research should explore real-time inference models that account for context, latency, and safety constraints.

Policy-oriented studies are needed to evaluate how regulatory mandates, certification policies, and governance frameworks influence cybersecurity readiness across aviation actors.

Lastly, comparative analyses across critical infrastructure sectors (e.g., rail, maritime, energy) can identify transferable best practices and highlight aviation-specific requirements for cybersecurity resilience.

In summary, this research confirms that civil aviation cybersecurity is a multi-dimensional challenge requiring coordinated technical, organizational, and regulatory responses. Mitigating these threats demands not only improvements in system design and risk detection, but also sustained governance, industry-wide collaboration, and a proactive security culture embedded across all aviation stakeholders.

References

[1] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE transactions on intelligent transportation systems*, vol. 18, no. 6, pp. 1338–1357, 2016.

[2] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022.

[3] M. Wolf, M. Minzlaff, and M. Moser, "Information technology security threats to modern e-enabled aircraft: A cautionary note," *Journal of Aerospace Information Systems*, vol. 11, no. 7, pp. 447–457, 2014.

[4] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, p. 19, 2018.

[5] A. A. Elmarady and K. Rahouma, "Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment," *IEEE access*, vol. 9, pp. 143 997–144 016, 2021.

[6] E. Habler, R. Bitton, and A. Shabtai, "Assessing aircraft security: A comprehensive survey and methodology for evaluation," *ACM Computing Surveys*, vol. 56, no. 4, pp. 1–40, 2023.

[7] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in *Aiaa scitech 2021 forum*, 2021, p. 0773.

[8] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K. R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," *Computers & Security*, vol. 112, p. 102516, 2022.

[9] C. A. P. Viveros, "Analysis of the cyber attacks against ads-b perspective of aviation experts," *Master's thesis, University of Tartu*, 2016.

[10] E. Ukwandu, M. A. Ben-Farah, H. Hindy, M. Bures, R. Atkinson, C. Tachtatzis, I. Andonovic, and X. Bellekens, "Cyber-security challenges in aviation industry: A review of current and future trends," p. 146, 2022.

[11] I. Doc, "ICAO Doc 9859 safety management manual," *Montreal: International Civil Aviation Organization*, 2018.

[12] A. Pawlicka, M. Choraś, and M. Pawlicki, "Cyberspace threats: not only hackers and criminals. raising the awareness of selected unusual cyberspace actors-cybersecurity researchers' perspective," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–11.

[13] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology innovation management review*, vol. 4, no. 10, 2014.

[14] Y. Xie, A. Gardi, and R. Sabatini, "Cybersecurity risks and threats in avionics and autonomous systems," in *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2023, pp. 0814–0819.

[15] A. Malatras, Z. Stanic, I. Lella, R. De Sousa Figueiredo, E. Tsekmezoglou, M. Theocharidou, R. Naydenov, and A. Drougkas, "Enisa threat landscape: Transport sector (january 2021 to october 2022)," 2023.

[16] J. Soldatos, J. Philpot, and G. Giunta, "Cyber-physical threat intelligence for critical infrastructures security: a guide to integrated cyber-physical protection of modern critical infrastructures," 2020.

[17] A. Alsaidi, A. Gutub, and T. Alkhodaidi, "Journal of forensic research," 2019.

[18] B. I. Scott, "Aviation cybersecurity: Regulatory approach in the european union," 2019.

[19] J. Predd, S. L. Pfleeger, J. Hunker, and C. Bulford, "Insiders behaving badly," *IEEE Security & Privacy*, vol. 6, no. 4, pp. 66–70, 2008.

[20] G. Mazzarolo and A. D. Jurcut, "Insider threats in cyber security: The enemy within the gates," *arXiv preprint arXiv:1911.09575*, 2019.

[21] B. Bean, "Mitigating insider threats in the domestic aviation system: Policy options for tsa," 2017.

[22] R. Abeyratne, "Cyber terrorism and aviation—national and international responses," pp. 337–349, 2011.

[23] A. F. Brantly, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 edited by Jason Healy: Arlington, VA: Cyber Conflict Studies Association*. Taylor & Francis, 2014.

[24] M. C. Libicki, *Conquest in cyberspace: national security and information warfare*. Cambridge University Press, 2007.

[25] K. Sampigethaya and R. Poovendran, "Aviation cyber-physical systems: Foundations for future aircraft and air transport," *Proceedings of the IEEE*, vol. 101, no. 8, pp. 1834–1855, 2013.

[26] P. Gontar, H. Homans, M. Rostalski, J. Behrend, F. Dehais, and K. Bengler, "Are pilots prepared for a cyber-attack? a human factors approach to the experimental evaluation of pilots' behavior," *Journal of Air Transport Management*, vol. 69, pp. 26–37, 2018.

[27] R. De Cerchio and C. Riley, "Aircraft systems cyber security," pp. 1C3–1, 2011.

[28] E. Habler, R. Bitton, and A. Shabtai, "Evaluating the security of aircraft systems," *arXiv preprint arXiv:2209.04028*, 2022.

[29] L. Bogoda, J. Mo, and C. Bil, "A systems engineering approach to appraise cybersecurity risks of cns/atm and avionics systems," in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2019, pp. 1–15.

[30] S. Khare and N. S. Talwandi, "Satellite communication vulnerabilities and threat landscape," in *2024 IEEE Silchar Subsection Conference (SILCON 2024)*. IEEE, 2024, pp. 1–6.

[31] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2014.

[32] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11*. Springer, 2013, pp. 253–271.

[33] A. Costin, A. Francillon *et al.*, "Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices," pp. 1–12, 2012.

[34] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012.

[35] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[36] D. Sullivan, "Above us only stars: Exposing gps spoofing in russia and syria," https://c4ads.org/publications/above-us-only-stars, 2019, c4ADS Report [retrieved: February, 2025].

[37] GPSJam.org, "Global gps interference map - crowdsourced gnss disruption data," https://gpsjam.org, 2024, [Retrieved: April, 2025].

[38] A. Lawall and P. Beenken, "A threat-led approach to mitigating ransomware attacks: Insights from a comprehensive analysis of the ransomware ecosystem," in *Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference*, ser. EICC '24, S. Li, K. Coopamootoo, and M. Sirivianos, Eds. New York, NY, USA: Association for Computing Machinery, 2024, p. 210–216. [Online]. Available: https://doi.org/10.1145/3655693.3661321

[39] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A holistic review of cybersecurity and reliability perspectives in smart airports," *IEEE Access*, vol. 8, pp. 209 802–209 834, 2020.

[40] R. Medina, "Air traffic management (atm)," Cairn/Cairn, pp. 22–27, 2024.

[41] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "Guide to industrial control systems (ics) security," National Institute of Standards and Technology, Tech. Rep. 82, 2011.

[42] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, and T. Baker, "Security threats to critical infrastructure: the human factor," *The Journal of Supercomputing*, vol. 74, pp. 4986–5002, 2018.

[43] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.

[44] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[45] X. Lu, "Research on the security of communication addressing and reporting system of civil aircraft," in *IOP Conference Series: Earth and Environmental Science*, vol. 295, no. 3. IOP Publishing, 2019, p. 032026.

[46] A. Roy, "Secure aircraft communications addressing and reporting system (acars)," in *20th DASC. 20th Digital Avionics Systems Conference (Cat. No. 01CH37219)*, vol. 2. IEEE, 2001, pp. 7A2–1.

[47] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, 2013.

Marking, IOT Traceability and Data Acquisition System for shopfloor of Gas Boiler Factory

José Paulo Santos
, and Henrique Barros
Department of Mechanical Engineering,
University of Aveiro Aveiro, Portugal
e-mail: jps@ua.pt
Pedro Nunes
School of Design, Management and Production Technologies Northern Aveiro
University of Aveiro Oliveira de Azeméis, Portugal
e-mail: pnunes@ua.pt

***Abstract*—Traceability and digitalisation are important in the industry because they affect the final quality of the products produced. This article seeks to find solutions that enable recording the operations carried out at each workstation during the production of a product (traceability). Typically, 2D, 3D, Radio Frequency IDentification (RFID) and vision industrial sensors are connected to industrial Programmable Logic Controllers (PLCs). These PLCs also require data communication boards to store this data in databases. The question is: can traceability be achieved using a low-cost solution for integrating industrial sensors into corporate databases? Technologies based on concepts such as the Industrial Internet of Things (IIoT) enable companies to track components in their assembly lines and acquire crucial production environment-related data. Combined with the development of data analysis algorithms, these technologies enable continuous process improvement and failure prediction. This document presents a study of various traceability technologies, data acquisition, and monitoring systems. Additionally, it details the development and implementation of a traceability solution applied to the production of gas boilers. The study incorporates IIoT technologies to record production-related data. The system's objectives align with the company's requirements, providing improvements to its current traceability system. Furthermore, it aims to establish a historical record for all produced gas boilers, provide tools for real-time production tracking and shop floor environment monitoring, and facilitate access to all available information. The system has a flexible structure that allows for adaptation to future improvements and future integration with commercial Enterprise Resouce Planning (ERPs) by bypassing expensive conventional automation sensors and PLCs from Siemens, Rockwell Automation and others. To address this problem this study proposes an "Iot Traceability Station" (IoTTS), as a first step. Other question is: How fast can the product be traced with the proposed IoTTS.**

Keywords-Shop floor Data Acquisition; Industry 4.0; IoT; Traceability; MQTT.

I. Introduction

Traceability is an area of high importance in the industrial environment. As defined in Cambridge dictionary "the ability to discover information about where and how a product was made". Currently, traceability in a production line, data acquisition directly from the factory floor, and component marking are factors of significant impact on efficient resource management for a company. Obtaining information about factory components and processes is essential for creating a reliable and comprehensive traceability system. To expand capabilities and complexity, these types of systems use various technologies that create a collection, processing, and storage of information in a digital and as automated a manner as possible. Control of environmental conditions in the factory environment is equally important for ensuring the quality of both stored components and those produced in the factory. Specifically, gathering information related to these conditions, along with data collected by traceability technologies, contributes to an overall increase in product quality, optimization of factory processes, and prevention of defects and/or failures. Consequently, the use of manual traceability systems represents a higher risk of failures, lower reliability, and a much slower data collection and processing speed when compared to automated systems that utilize marking/traceability technologies such as barcodes, radio frequency identification (RFID), Indoor Global Positioning System (IGPS) of Gas Boiler. The control and traceability of each of these stages and the components that pass through them are essential for achieving results that meet customer requirements. In this application area, there are various factors to consider during production and manufacturing, and the prevention of errors and the optimization of production quality can lead to significant cost savings. In this case, traceability, data processing, and control of environmental conditions are factors to consider for improving the quality and reliability of the final product.

A. Gas Boiler

This paper proposes the introduction of a new monitoring system for a gas boiler manufacturing facility. To support this initiative, it is essential to analyze the machines produced in the factory, along with their individual components, in order to gain a deeper understanding of the manufacturing processes and identify the key stages that require monitoring.

A gas boiler is a stationary device designed to transfer energy from gas to water [1]. As illustrated in Figure 1, a gas boiler consists of numerous components, such as: the gas

valve (which regulates or interrupts the flow of gas to the burner); the burner (which mixes gas and air); the combustion chamber (where heat is generated to warm the water); the heat exchanger; the flame sensor (which shuts off the gas supply if no flame is detected); the igniter (which provides the spark to ignite the gas-air mixture); the control board; various safety devices; and several other components [1].

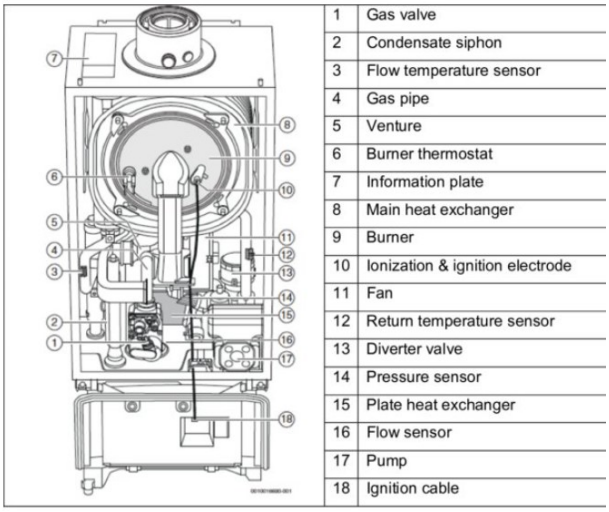


Figure 1. Gas boiler main components.

To ensure proper assembly, the correct components must be assembled in the correct sequence for each specific model. This is accomplished through assembly lines composed of multiple manual or automated stations, where each workstation is responsible for assembling a specific component or performing a specific operation. This structured approach is essential in the gas boiler assembly line to maintain efficiency, consistency, and product quality.

B. Traceability Technologies

The gas boiler (product) and component code, can be registered on a label with a 1D or 2D barcode [2][3] or on an RFID tag [4][5].

The concept of traceability in the industrial context represents the ability to track the entire journey of a product or specific components. In other words, it is the capacity to obtain information about their production processes and create a history of the product and its lifecycle. The need for traceability and the application of information collection systems arises from the producers' and customers' need to know the origin, the process, and the destination of a product. To achieve this, and organize all, the collected information about a particular component, product, or industrial process, identification codes, are created. This allows information to be associated with objects or processes. Identifying each component or product enables its traceability throughout the production process, making it more efficient. In an industrial environment, traceability requires auxiliary technologies to create identification codes for components and products. Several types of marking, and data collection technologies, are crucial at this stage, including barcodes, RFID tags, and others, which make information collection and processing more automated and efficient. There are closed solutions from various automation companies, such as Siemens, Rockwell Automation, and others, which, with their programmable controllers and specific programs, are able to collect data from sensors and store it in databases. The problem is the cost and customer loyalty to these companies. It is important to study low-cost solutions that make use of the latest technologies to propose new solutions, in this case for the collection of traceability data. Using the traceability technologies (sensors) in conjunction with Internet of Things (IoT) monitoring methods, it is possible to create intelligent production processes, increase product quality, reduce costs, improve information flow, and ensure better factory management [6] [7] [8] [9]. Processing the data acquired, within IoT devices, is not always easy, given their processing and memory limitations. In [10], new algorithms are presented that can be used in IoT devices for both training and using models. Another example is presented in [11], where the quality of gas boiler flames can be analyzed based on their color, using the Backpropagation Algorithm (BPA) and Ant Colony Optimization (ACO) to process the acquired data. IoT devices, together with traceability technologies, communication technologies, and data management algorithms, can be used in many fields. In [12], an overview of these technologies applied to food traceability is presented. In [13] is presented an overview of Digital Twins and enabling technologies, associated with IoT/Industrial IoT (IIoT) and machine learning, namely for predictive maintenance and fault detection.

In section II is presented the proposed solution to integrate shop floor industrial sensor to enterprise database, via Message Queuing Telemetry Transport (MQTT) broker. In section III is presented the proposed IoT traceability station, one for each shopfloor production station. In section IV, conclusions are presented.

II. Proposed Solution Architecture

In the development of a solution that considers the problems addressed by the project and its objectives, there was a need to reflect on the current methods of data collection and recording in the Gas boiler factory. The completion of record sheets with parameters that are important for production and essential for the final quality of the transformer is done manually by operators on the production line, and these sheets are subsequently physically stored in the factory. Following this, the sheets are scanned and saved in the project folder available on the company's server. The proposed traceability and monitoring system solution aims to enable data collection and facilitate access to it by digitising the process and storing the data in real time. The proposed traceability system involves installing an IoT Traceability Station (IoTTS) at each workstation. This station will be responsible for recognizing the implemented marking system, receiving data from the operator, processing, and transmitting the data recorded by the operator during production. In addition to the traceability station, this allows for

the almost automatic verification of the overall manufacturing conditions for each component and the final product.

III. Proposed IoT Traceability Station

The IoTTS is one of the system's key components. As shown in Figure 2, this block of the proposed solution will be responsible for acquiring and transmitting data to subsequent levels of the solution. The production stations: assembly and transport, are represented at a low level. It is proposed that a IoTTS is used for each station. The QRCode and RFID presented in the figure collect data, these data are shown in a local LCD interface (Nextion NX4827T043), and is also sent to an MQTT broker.

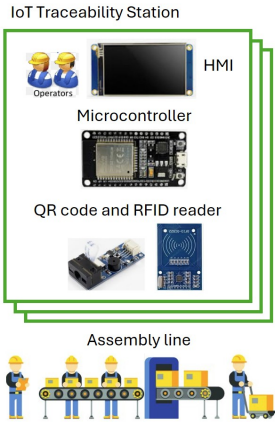


Figure 2. Iot Traceability Station.

Figure 3. IoT Traceability Station – Implementation.

Figure 3 shows the practical implementation of the IoTTS. Given that this project aims to implement traceability and component marking technologies, such as 1D and 2D barcodes or RFID tags, the Traceability Station will need to be equipped with hardware capable of reading these marking technologies to enable the reading of references and data association. To achieve this, the Iot Traceability Station has a barcode scanner (type H1/1690S) or an RFID tag reader (RFID RC522), allowing the operator to handle materials easily without disrupting normal production processes. Finally, this unit requires hardware capable of processing the received data and transmitting it via Wi-Fi to the subsequent levels of the system. This role will be fulfilled by an Iot microcontroller (ESP32-WiFi), a low-cost and compact technology that will make the Iot Traceability Station a small unit that can be easily transported by the operator and ready for use in any area of the factory floor. It is also proposed to use MQTT as an intermediary between the different IoTS and the production database (Figure 4).

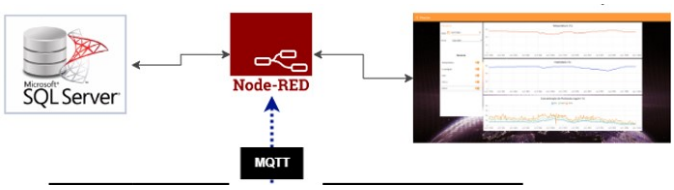


Figure 4. Back-end schematic.

It is proposed that the Quality of Service (QoS) of the MQTT be at least equal to 1. So, the exchange of messages will be done in a confirmed manner. Although the exchange of information takes time, for low rates, i.e. one part per second, it is enough.

IV. Conclusions

The developed system is structured into three distinct modules: the IoT traceability station, the server, and the user interfaces. In conjunction with these modules, communication protocols were established between all layers of the system to ensure that it functions as intended. The association of information from both stations is carried out at this point in the system, making it possible to build information related to each component for each product. In conclusion, the marking, traceability, and data acquisition system from the Gas boiler factory floor has been implemented and met the proposed objectives. The development of the system considered the budget and tried to minimize the total solution cost, thus creating an efficient, low-cost system that applies IoT technologies and concepts to Gas boiler production. The implementation of the developed system allows for storing the historical data related to the product and production.

Future work: The proposed solution has the potential of leveraging the historical traceability data collected through predictive AI / ML models, which could significantly enhance the value and impact of the proposed system.

References

[1] G. J. Bennet, "The secret life of boilers: Dynamic performance of residential gas boiler heating systems - a modeling and empirical study," Online: https://www.researchgate.net/publication/331148896_The_secret_life_of_boilers_Dynamic_performance_of_residential_gas_boiler_heating_systems_-_a_modelling_and_empirical_study/figures?lo=1 (Accessed: 2025-04-14), Ph.D. dissertation, PhD Thesis, 2019.

[2] GS1, *GS1 barcodes*, https://www.gs1.org/standards/barcodes, Accessed: 2025-04.

[3] GS1, *EPCglobal*, https://www.gs1.org/epcglobal, Accessed: 2025-04.

[4] S. Ahuja and P. Potti, "An introduction to rfid technology," *Communications and Network*, vol. 2, no. 3, pp. 183–186, 2010. DOI: 10.4236/cn.2010.23026.

[5] FID4u, *How to select a correct tag – frequency*, https://rfid4u.com/rfid-frequency/, Accessed: 2025-04.

[6] B. N. Pasi, S. K. Mahajan, and S. B. Rane, "Redesigning of smart manufacturing system based on iot: Perspective of disruptive innovations of industry 4.0 paradigm," *International Journal of Mechanical and Production Engineering Research and Development*, vol. 10, no. 3, pp. 727–746, Jun. 2020. DOI: 10.24247/ijmperdjun202067.

[7] E. P. Hinchy, N. P. O'Dowd, and C. T. McCarthy, "Using open-source microcontrollers to enable digital twin communication for smart manufacturing," in *Procedia Manufacturing*, Elsevier B.V., 2019, pp. 1213–1219. DOI: 10.1016/j.promfg.2020.01.212.

[8] P. Viana, "Proposta de um sistema automático de rastreabilidade 4.0," Accessed: 2025-04, http://hdl.handle.net/10773/31415, M.S. thesis, University of Aveiro, 2021.

[9] G. Salgueiro, "Proposal for an automatic traceability system - renault 4.0," Accessed: 2025-04, http://hdl.handle.net/10773/32150, M.S. thesis, University of Aveiro, 2021.

[10] B. Sudharsan, J. G. Breslin, and M. I. Ali, "Ml-mcu: A framework to train ml classifiers on mcu-based iot edge devices," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15 007–15 017, Aug. 2022. DOI: 10.1109/JIOT.2021.3098166.

[11] K. Sujatha, N. P. G. Bhavani, T. K. Reddy, and K. S. R. Kumar, "Internet of things for flame monitoring power station boilers," in *2017 Trends in Industrial Measurement and Automation (TIMA)*, Chennai, India, 2017, pp. 1–7. DOI: 10.1109/TIMA.2017.8064783.

[12] R. Mehannaoui, K. N. Mouss, and K. Aksa, "Iot-based food traceability system: Architecture, technologies, applications, and future trends," *Food Control*, vol. 145, p. 109 409, 2023, ISSN: 0956-7135. DOI: 10.1016/j.foodcont.2022.109409.

[13] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108 952–108 971, 2020. DOI: 10.1109/ACCESS.2020.2998358.

Dual-Link Data Resilient Edge-to-cloud Communication Framework for Agricultural Robots

Iman Esfandiyar
Łukasiewicz Research Network
Poznan Institute of Technology
Poznan, Poland
e-mail:iman.esfandiyar@pit.lukasiewicz.gov.pl

Kamil Młodzikowski
Łukasiewicz Research Network
Poznan Institute of Technology
Poznan, Poland
e-mail:kamil.mlodzikowski@pit.lukasiewicz.gov.pl

***Abstract*—Reliable and high-throughput communication between field robots and cloud services remain a key challenge in precision agriculture, where remote rural areas often lack consistent high-bandwidth connectivity. In this work, we introduce a new dual-link edge-to-cloud data transfer framework that combines long-range Low-Power Wide Area Networking (LPWAN) for essential control and monitoring with IEEE 802.11 Wi-Fi that carries bulk data over a Zenoh protocol. In addition, a data router dynamically switches the robot between 'Transfer Mode', in which sensor streams and imagery data are being forwarded via Wi-Fi, and 'Storage Mode', in which data are locally recorded in Robotic Operating System (ROS) 2 bags to prevent loss when connectivity degrades. To preemptively detect Wi-Fi link failures and issue routing instructions to the data router, an onboard anomaly detection node monitors heartbeat timing using a machine learning-based algorithm, namely the XGBoost model. Field trials demonstrate that (1) Wi-Fi transfers maintain sub-100 ms latency within 240 m of the gateway, (2) Long Rang (LoRa) communication persists reliably beyond 350 m with ≈0.1 s latency, (3) the router achieves an average of 0.8 s overlap when entering Storage Mode, and (4) the anomaly detector successfully flags link degradation ahead of an outage. Our framework scales to multi-robot deployments via ROS 2 namespaces and Zenoh multicast, laying the groundwork for resilient swarm operations in rural environments.**

Keywords-Autonomous Agricultural Robot; Anomaly Detection; IoT-cloud continuum; LoRa; Zenoh.

I. Introduction

Precision farming and autonomous machinery are two concepts that are becoming increasingly prevalent in modern agriculture, to simplify key aspects of agricultural work by transferring physically demanding tasks to machines and maximizing crop yields, therefore conserving resources [1]. Tasks such as weed and pest control or precise plant fertilization are among those performed by autonomous machines in agriculture, such as unmanned autonomous robots. For the detection of environmental and/or soil parameters, the robots are equipped with Internet of Things (IoT) sensors that can detect objects on site, generating a substantial amount of data. The analysis, utilization and storage of this data requires the availability of extensive computing resources, which can be provided through cloud computing [2]. However, a challenge arises in the transfer of data from the robot to the cloud, as an internet connection in the fields is often unreliable or unavailable [1]. Given the expansive and sparsely populated areas typically utilized for agricultural purposes, there is a clear necessity for a communication solution capable of operating over considerable distances while simultaneously transmitting substantial quantities of data. The sole use of LPWAN technologies are not a viable option due to the high data volumes involved. While LPWAN enables data to be send over the necessary distances, their data rates and payload sizes are inadequate for transmitting more than a few kilobytes per day [3]. Even in the licensed domain of LPWAN solutions, the throughput would be insufficient. Conversely, application layer protocols operating over Wi-Fi do not achieve the required distance, yet can accommodate the necessary data volume [4]. To deliver the necessary data while maintaining a constant connection to the edge/cloud, we propose the integration of both solutions in an agricultural use case that incorporates an autonomous robot into the edge/cloud continuum.

In this paper, we propose a novel data transfer method that employs unlicensed spectrum physical layer LoRa to transmit control messages as well as minimal vital messages to an agricultural robot, thereby providing information regarding the robot status and its location at a self-provided gateway and enabling an emergency shutdown of the system if necessary. Additionally, the recently, from the eclipse foundation and Zettascale developed Zenoh protocol is utilized for data exchange between the three participants of the data exchange, namely the robot, the gateway and the cloud.

Zenoh is a publisher/subscriber/query protocol designed to operate in the microcontroller to cloud continuum, supporting peer-to-peer, routed and brokered communication via WiFi [5].

To detect packet loss during data transmission in an agricultural setting, where the distance between the robot and the gateway is rather high, to minimize the distance traveled by the robot, we employ an anomaly detection mechanism in the robot to assess whether data transmission works properly or if it is better to start recording backup data. The performance of the proposed system is evaluated through field experiments, which demonstrates the efficacy of the data exchange between the robot and the gateway.

The rest of the paper is organized as follows. Section II presents the related work. Section **??** shows the system architecture. Section VI describes the experiment methodology. Section VII discusses the experiment results. Finally, Section VIII concludes the paper.

II. Related Work

The authors of [6] used open-source software to build a LoRa network connecting several sensor nodes to a gateway node to be used in an agricultural scenario. Communication from the gateway to the server is done using Message Queuing Telemetry Transport (MQTT) over Long Term Evolution (LTE). Our system differentiates from their work by utilising Zenoh over Wi-Fi for communication between the sensor node, gateway and server, while having the sensor node connected to an autonomously moving robot. In [7], a salable hybrid network for monitoring an agricultural environment is proposed. This work relies on LoRa to transmit all the gathered sensor data and aims to cover a size of land that makes it necessary to include LoRa relay nodes to reach the gateway from where it uploads the data to the cloud using Wi-Fi. In contrast to this work, our proposed system relies on Wi-Fi for data transmission, utilizing LoRa only for minimal communication to the robot to detect its position and to send emergency commands. Using LoRa as a control link has been done by the authors of [8] as well. In their case, the control link is established to an Unmanned Aerial Vehicle (UAV) to increase its operational range. Experimental results were obtained from simulations only. In comparison to this work, the use of LoRa is limited to the transmission of minimal control messages, rather than the encapsulation of other protocol messages within the LoRa payload.

In their study, the authors of [9] examine the potential of Zenoh in heterogeneous networks. They demonstrate that Zenoh can act as a middleware for peers in different networks, enabling communication using a pub/sub approach in real-time. We utilize Zenoh for intercommunication between devices operating on disparate systems, including ROS and Linux. Zenoh has been used as the backbone of a cloud-to-edge communication Framework, introduced in [10]. The proposed framework aims to create a domain for distributed computing for IoT scenarios, leveraging decentralized pub/sub communication using Zenoh, lightweight virtualization and orchestration of the system and its components. It is our objective to leverage the capabilities of Zenoh to extend to the IoT nodes. Our intention is not to limit our scope to the communication between the edge and cloud computing systems. The authors in [11] compared the performance of three Wi-Fi standards, IEEE 802.11ax, 802.11ac and 802.11, in outdoor IoT scenarios. Transmission throughput was evaluated in the range of 2 to 125 m. Our approach is similar, but we utilized Zenoh over WiFi and analysed packet loss and delay while increasing and decreasing transmission distances. In [12] the authors have proposed an algorithm that predicts the quality of WiFi and Bluetooth Low Energy (BLE) communication with accuracies of 94 % and 92 %. They are using Received Signal Strength (RSS) as the assessment metric for the quality of the connection. The basis of their prediction is a support vector regression model using a radical base function. Our system differs from this by using a linear regression model in order to find outlier transmission behaviour to find an ideal spot for starting/stopping the transmission of packets. The anomaly detection in WiFi signals is being done by [13] as well. Their research focuses on the development of a Radio Frequency (RF) fingerprinting system for devices used in a WiFi dataset, in order not only to detect abnormal transmitter but also to learn from their behaviour and reject them in the future. Our approach utilizes the detection of anomalies in the WiFi connection to identify any issues with the transmission of WiFi signals to a gateway. This is necessary since WiFi can be disturbed at any time before the robot crosses the distance threshold. By detecting anomalies in data transfer we ensure as little data is lost as possible.

III. Agricultural Robot

The agricultural robotic platform, AgroRob, is designed to autonomously navigate fields for precision farming tasks such as crop spraying and weeding. Equipped with advanced sensors, communication modules, and a modular software architecture, it ensures reliable localization, efficient operation, and seamless data exchange with the cloud-based systems. This section details the autonomous functionalities, hardware setup, software architecture, and communication protocols employed by the robot.

1) Robot Autonomous Functionality: The agricultural platform (AgroRob) autonomously navigates fields for precise crop spraying and weeding. It achieves accurate localization by fusing data from dual Global Navigation Satellite Systems (GNSS) modules, an Inertial Measurement Unit (IMU), and wheel odometry. This enables it to follow crop lines and share its position with a cloud-based system. A Deep Neural Network (DNN) model processes camera images to detect crops and weeds, for precise spraying. Computer vision minimizes chemical use, reducing fertilizer and herbicide consumption while improving efficiency and sustainability.

2) Robot Hardware: The robot features an onboard computer managing control and communication. It includes localization sensors, cameras, a Wi-Fi router, and a LoRa transmitter for cloud data transfer. Communication occurs via a Controller Area Network (CAN) to USB adapter, handling status updates and control commands. Figure 1 illustrates the hardware setup.

3) Robot Software: The robot's software is developed using ROS 2 [14], utilises peer-to-peer communication via the Data Distribution Service (DDS). Modules, such as mission handling, localization, and navigation, communicate via UDP or TCP, based on Quality of Service (QoS) settings. Data is transmitted through a publish-subscribe model for broadcast communication or services for direct interactions. Certain topics enable cloud communication for control and monitoring, as shown in Figure 2.

4) Messages: LoRa communication involves sending string data. Messages to the gateway contain three comma-separated values, totalling up to $29bytes$:

- **ID**: Unique packet identifier.
- **Coordinates**: Latitude and longitude.
- **Time**: UTC timestamp.

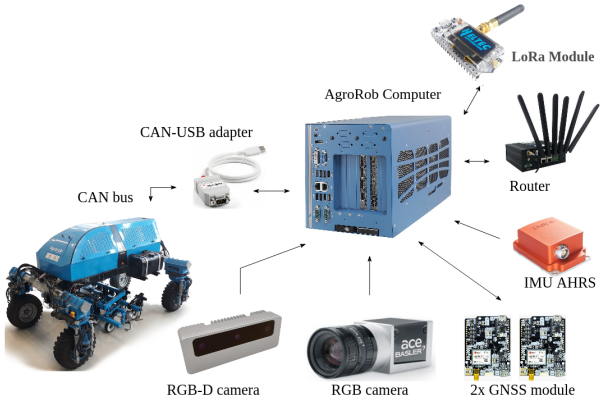


Figure 1. Hardware configuration of the agricultural robotic platform.

The gateway sends two boolean control commands under $0.5Hz$:

- **Data Control Command**: Chooses Wi-Fi transmission or local logging.
- **Emergency Stop Command**: Immediately halts the robot.

Wi-Fi communication transmits operational data, including sensor readings, mission status, and field analysis, essential for robot performance and agricultural insights.

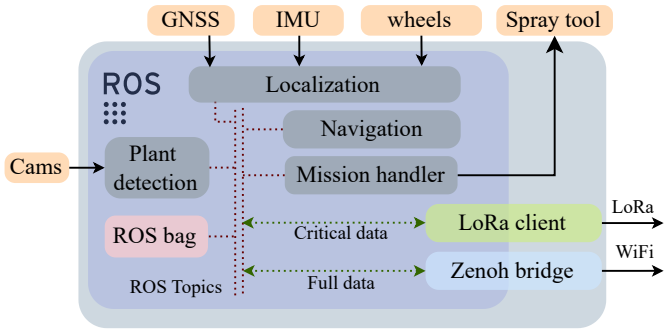


Figure 2. Data flow architecture of the AgroRob platform.

IV. Data Transfer and Storage

As shown in Figure 3, our proposed data transfer method assumes that both the robot and the gateway can communicate using LoRa and Wi-Fi, with both systems having independent GNSS localization available via a u-blox ZED-F9P GNSS module onboard. The robot is equipped with an industrial Wi-Fi router, the NR600 from NavigateWorx, along with a Heltec WiFi LoRa 32 V3 module, while the gateway features a Nighthawk® AXE3000 Wi-Fi USB adapter and a Heltec WiFi LoRa 32 V3 module. In addition, the gateway is also equipped with internet connectivity through a 5G/LTE modem. Both the robot and the gateway are performing localization using GNSS. Robot geolocation is sent through LoRa to the gateway. Based on this information and its own position, the gateway

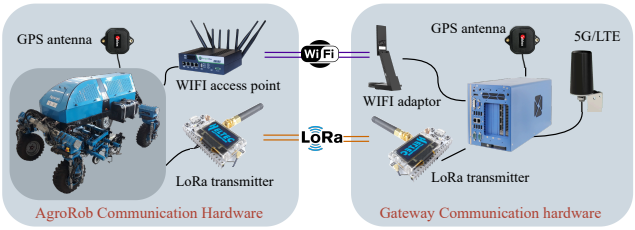


Figure 3. The communication hardware configuration of the AgroRob LoRa-based network.

calculates the distance to the robot. This data together with heartbeat delay calculated based on UTM time is then used by *Data Router* software to switch between two states:

- *Transfer Mode*: While the robot is in an efficient range and strength of Wi-Fi connection with the gateway, it operates in *Transfer Mode*. Selected data (represented by ROS2 topics) is being sent over Wi-Fi to the gateway using a Zenoh bridge.
- *Storage Mode*: Conversely, when there is a risk of losing the Wi-Fi connection between the robot and the gateway, the robot is switched to *Storage Mode*. In this mode, the Zenoh bridge is turned off to minimise the risk of data interception. The data that normally in Transfer Mode would be sent to the gateway is instead being recorded using ROS2 bags and stored locally for future synchronization. The proposed communication flow is presented in Figure 4.

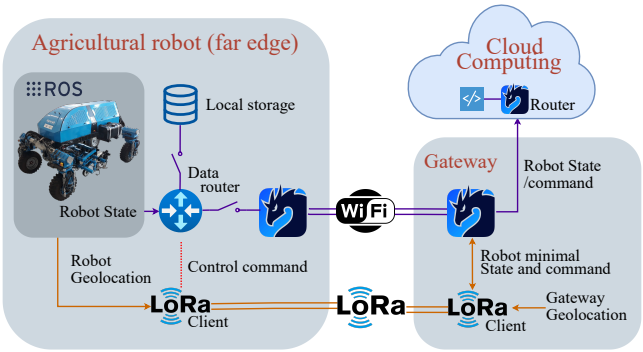


Figure 4. The communication architecture of the AgroRob system.

A. Data router

Every time the gateway receives a geolocation of the robot (latitude ϕ and longitude λ) through LoRa, it calculates the distance between itself and the robot using the following equations:

$$c = \frac{1}{\sqrt{\cos^2(\phi) + (1-f)^2 \cdot \sin^2(\phi)}} \quad (1)$$

$$s = (1-f)^2 \cdot c \quad (2)$$

$$x = (R \cdot c + h) \cdot \cos(\phi) \cdot \cos(\lambda)$$
$$y = (R \cdot c + h) \cdot \cos(\phi) \cdot \sin(\lambda)$$
$$z = (R \cdot s + h) \cdot \sin(\phi)$$

Given two points: gateway $= (x_G, y_G, z_G)$ and robot $= (x_R, y_R, z_R)$, the Euclidean distance d_{GR} is:

$$d_{GR} = \sqrt{(x_G - x_R)^2 + (y_G - y_R)^2 + (z_G - z_R)^2} \quad (3)$$

Where:

$R = 6356752.3142$ (Earth radius)
$f = 1/298.257223563$ (Earth flattening factor)
ϕ is the latitude
λ is the longitude

The calculated distance, together with the value of delay calculated based on the timestamp of messages received from the gateway is continuously fed to the anomaly detection software. The software analyzes this data in real-time to detect any abnormalities in communication behaviour. Upon identifying an anomaly, it issues commands to the data router on the robot. The data router then switches between Storage Mode and Transfer Mode as needed, ensuring an overlap between data recording and transmission to prevent any potential data loss.

In cases of *Storage Mode* data loss is mitigated through local storage on the edge device. However, since the operational data of the agricultural robot primarily consists of numerical values and image data that are processed locally, the volume of stored information remains relatively low and does not necessitate large-scale storage solutions. It should be noted, however, that the local storage of data is inherently constrained by the physical storage capacity of the edge device. Despite this limitation, retaining operational data is essential for the robot's continued functionality—for example, to maintain a record of the location and status of individual crop instances, which is critical for planning and executing future operations on the same field plots.

V. Anomaly Detection

Our anomaly detection system employs a machine learning approach to identify abnormal behaviour in Wi-Fi data transmission. The system monitors robot's heartbeat timing data and the distance between the robot and the gateway, to detect potential failures or malfunctions. It implements a two-stage process: first, a model training phase using XGBModel with KMeansScorer to learn normal operational patterns from historical data; second, a detection phase, where the AnomalyDetectionNode continuously analyzes incoming data against these learned patterns in real time.

The detection mechanism combines IQRDetector and ThresholdDetector methodologies to identify statistical outliers, publishing alerts when anomalies exceed a configurable percentage threshold. Operating independently on ROS2, the system samples data at regular intervals (configurable, set to 2 seconds in the current implementation) and maintains a sliding window of observations to balance detection sensitivity with computational efficiency.

For reproducibility, the `XGBModel` was trained on 3285 heartbeat intervals. The model uses `lags`=64. Anomaly scores are produced by a `KMeansScorer` with $k = 20$ clusters and a 32-sample window (`component_wise`=False).

By continuously analyzing heartbeat timing and flagging outliers in real-time, the anomaly detector enables the robot to switch preemptively between Transfer and Storage modes, beginning local data logging before Wi-Fi breaks down and reenabling Zenoh the instant link quality recovers, thus eliminating data gaps and negative overlaps. Moreover, when sustained anomalies indicate worsening channel conditions, the system can dynamically throttle non-critical streams (e.g., reduce image resolution) to preserve essential telemetry, while simultaneously relaying "link degrading" alerts back to the operator over LoRa. If anomaly rates cross a critical threshold, the detector can even trigger an immediate emergency-stop command, ensuring both data integrity and operational safety without human intervention.

Our implementation incorporates adaptive sensitivity adjustments based on environmental conditions and operational context. During periods of known network congestion or when the robot traverses areas with documented Wi-Fi interference, the system automatically adjusts detection thresholds to reduce false positives while maintaining vigilance for genuine anomalies.

This approach allows for early warning of developing issues before they cause critical failures, making it possible to act accordingly to prevent data loss as much as possible. The modular design of the system also enables easy integration of additional detection algorithms as they become available, ensuring future extensibility.

VI. Experiments Methodology

This section describes the methodology used to evaluate our approach's performance and accuracy. The experiments test the hypothesis under various conditions to ensure comprehensive and real-world-representative results.

A. Experiment Setup

In our experiments, we mimic real-world applications. The gateway is stationary while the robot moves toward and away from it as shown in Figure 5.

To ensure accurate time synchronization for one-way communication measurements, messages are timestamped using GNSS-based UTC time [15], as both the robot and the gateway are equipped with GNSS receivers. The gateway also functions as an Real-Time Kinematic (RTK) base station, providing localization corrections to the robot for improved accuracy. GPS signals serve as a common time reference, enabling timestamp comparisons to calculate one-way communication delays, especially when switching between LoRa and Wi-Fi.

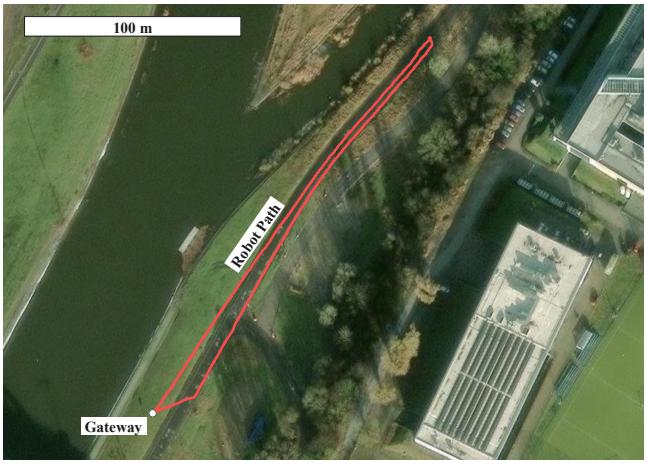


Figure 5. A satellite view map illustrating the robot's path during the test experiment. The gateway computer was positioned at a fixed location, while the robot began its movement near the gateway, traveled away, and eventually returned to its initial position. The red line on the map represents the path followed by the robot.

This method avoids complexities in round-trip measurements, which can obscure path delays in asymmetric networks.

Two series of connectivity and data transfer experiments were conducted:

1. The robot moves away from the gateway while transmitting data via both LoRa and Wi-Fi (using the Zenoh bridge). As the distance increases, Wi-Fi eventually goes out of range. During this process, data is logged, including timestamps of messages generated by the robot and received at the gateway. This information is used to analyze transfer characteristics and to generate training data for the anomaly detection model.

2. The same procedure is repeated with the anomaly detection and data routing system enabled; the result is illustrated in Figure 8.

B. Experiment Metrics

Key performance metrics include:

- *Communication Latency*:
  Wi-Fi: The time taken for data transfer over Wi-Fi within range. It is computed as:

$$\Delta_t = t_{\text{curr}} - t_{\text{stamp}} \tag{4}$$

$$\tau = t_{UTC_G} - t_{UTC_R} + \Delta_t \tag{5}$$

  Where:

  t_{curr} is the current ROS2 time,
  t_{stamp} is the UTC message timestamp,
  t_{UTC_G} is UTC time on the gateway,
  t_{UTC_R} is UTC time on the robot,
  τ is the delay.

  LoRa: Measured similarly, with UTC time added to LoRa messages.
- *Packet Loss*:
  LoRa: Reliability of position data sent from the robot. Packet loss is calculated by tracking message ID gaps.
- *Network Coverage*:
  Wi-Fi: Maximum reliable connection distance.
  LoRa: Maximum distance for reliable command reception.
  Range-based Switching: Effectiveness of transitioning between Wi-Fi and LoRa.
- *Data Overlap*:
  As described in Section IV-A, switching between *Transfer Mode* and *Storage Mode* must ensure data overlap. The target overlap is $1s$, though factors like Zenoh bridge stand-up time may influence it.
  Zenoh to Bag: Time between the first message stored in *rosbag2* on the robot and the last received at the gateway. A positive value indicates overlap, while a negative value means data loss.
  Bag to Zenoh: Time between the first message received at the gateway and the first stored in *rosbag2*. A positive value means overlap; a negative value indicates loss.

These evaluation metrics ensure a balanced assessment of the method's performance. Each configuration underwent multiple runs to ensure consistency and account for variance. The final results are reported as averages with standard deviations, where applicable.

VII. Experiments Results

A series of field test experiments have taken place involving the robot moving away from the gateway while measuring the defined metrics of Wi-Fi and LoRa at the gateway.

A. WiFi and LoRa delay

Figure 6 illustrates the delay experienced by both Zenoh and LoRa communication over time and distance from the gateway. In this experiment, the distance between the robot and the gateway is gradually increased. As the distance between the two devices increases, the average delay of the Zenoh messages also increases until approximately 240 meters, at which point connectivity to the gateway is lost. The distance is then extended to 350 meters, which has no impact on the delay of the LoRa messages.

In order to regulate the transfer of data via Wi-Fi and to facilitate local logging, a threshold of 50 meters was implemented for Wi-Fi transmissions in the course of the following experiments. The results of this can be observed in Figure 7a. In this experiment, the distance between the robot and the gateway initially increases and subsequently decreases. Upon reaching the threshold of 50 meters, the Wi-Fi transmissions are terminated, while the LoRa control messages continue to be exchanged. Figure 7b illustrates the number of Wi-Fi packets received and LoRa packets lost. The impact of the threshold can be observed here, as Wi-Fi packets are only transmitted when the distance is less than 50 m and the delay therefore remains below 0.1s. However, at a distance of 60 m, loss of LoRa packets occurs. The packet loss has no influence

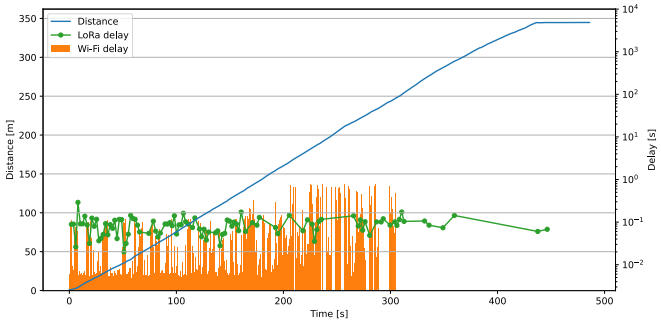


Figure 6. WiFi and LoRa packet delays as the robot moves away from the gateway. As the robot recedes from the gateway, packet transmission delays increase; the Wi-Fi link fails beyond approximately 300 m, whereas the LoRa channel continues to deliver low-bandwidth data with an almost constant latency.

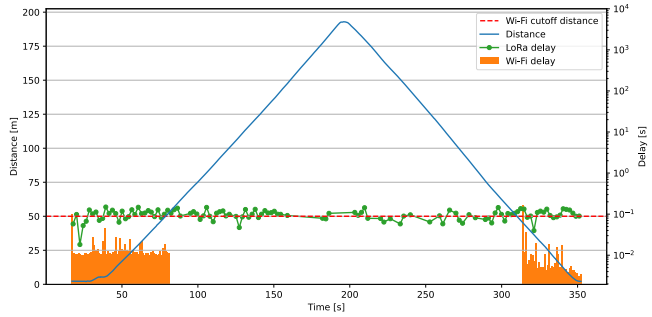
on the delay of the subsequent LoRa packets as this value fluctuates around 0.1 s for LoRa packets.

In order to regulate the transfer of data via Wi-Fi and to facilitate local logging, a threshold of 50 meters was implemented for Wi-Fi transmissions in the course of the following experiments. The results of this can be observed in Figure 7a. In this experiment, the distance between the robot and the gateway initially increases and subsequently decreases. Upon reaching the threshold of 50 meters, the Wi-Fi transmissions are terminated, while the LoRa control messages continue to be exchanged. Figure 7b illustrates the number of Wi-Fi packets received and LoRa packets lost. The impact of the threshold can be observed here, as Wi-Fi packets are only transmitted when the distance is less than 50 m and the delay therefore remains below 0.1s. However, at a distance of 60 m, loss of LoRa packets occurs. The packet loss has no influence on the delay of the subsequent LoRa packets as this value fluctuates around 0.1 s for LoRa packets.

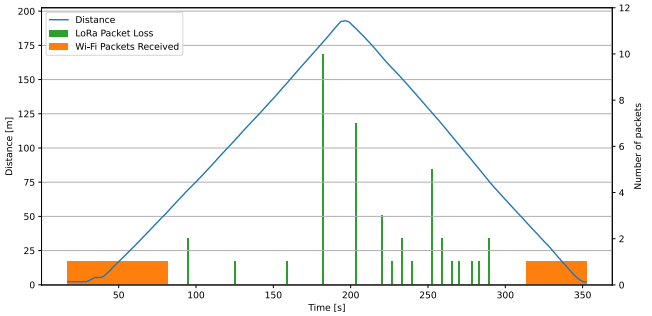
Time overlap between data sent over Wi-Fi and stored in *rosbag2* was measured in multiple experiments. The results are presented in Table I. The data shows that the average time of data overlap for switching from *Transfer Mode* to *Storage Mode* is 0.8 seconds. This means that for an average of 0.8 seconds data is stored both locally at the robot and sent over Wi-Fi (using Zenoh) to the gateway. Therefore, the process of starting bag recording takes an average of 0.2 seconds (as the desired overlap was set to 1 second).

In the second case, where the system switches from *Storage Mode* to *Transfer Mode*, the average overlap is -1.0667 seconds. The negative value indicates that there was a gap between the data stored locally on the robot and the data sent using the Zenoh bridge. The result is illustrated in Figure 8.

Such a result indicates that a much higher overlap is needed when switching from *Storage Mode* to *Transfer Mode*. The most probable cause of this behaviour is the stand-up time of the Zenoh bridge, as the process is stopped each time the system switches to *Storage Mode*.



(a) WiFi and LoRa packet delays



(b) WiFi Received packets and LoRa packet lost

Figure 7. (a) WiFi and LoRa packet delays, and (b) WiFi received packets and LoRa packet loss as the robot moves away from and gets close to the gateway, switching between Transfer and Storage Modes at a 50-meter distance threshold.

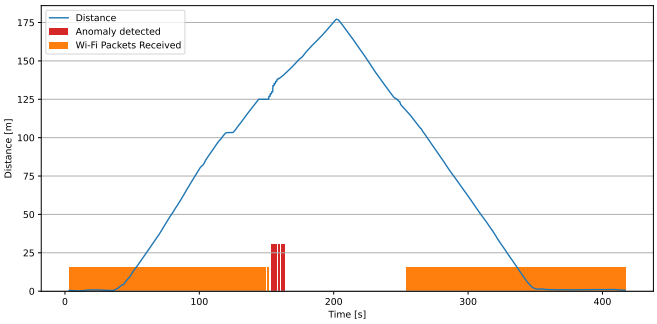


Figure 8. Anomaly detection system recognizes issues with Wi-Fi data transfer, particularly as the distance between the robot and the gateway increases and signal quality begins to degrade.

TABLE I. AVERAGE DATA OVERLAP TIME (IN SECONDS) FOR TRANSFER TO STORAGE AND STORAGE TO TRANSFER MODE SWITCHES, WITH STANDARD DEVIATION AND DIFFERENCE FROM DESIRED 1 SECOND.

	Transfer→Storage [s]	Storage→Transfer [s]
Avg.	0.8000	-1.0667
Std.	5.19×10^{-9}	1.0263
Diff.	0.2000	2.0667

B. Anomaly detection model performance

The performance of the anomaly detection model was evaluated using standard classification metrics: precision, recall, and F1-score. These metrics were calculated by comparing

the predicted labels (`pred_labels`) against the ground truth labels (`gt_labels`). The calculations were performed using the `precision_score`, `recall_score`, and `f1_score` functions, with the `zero_division` parameter set to 0 to handle any potential division by zero issues gracefully. The results of these evaluations are summarized in Table II, providing a view of the model's ability to correctly identify anomalies in Wi-Fi communication while minimizing false positives and false negatives.

TABLE II. PERFORMANCE METRICS OF THE ANOMALY DETECTION MODEL: PRECISION, RECALL, AND F1-SCORE.

	Precision	Recall	F1-score
Score	0.951	0.966	0.958

VIII. CONCLUSION AND FUTURE WORK

This study presents a novel data transfer method that integrates LoRa communication with Wi-Fi to enhance the operational capabilities of autonomous agricultural robots. Utilizing LoRa for essential control messages and minimal status updates facilitates reliable communication in rural areas, where connectivity is frequently limited. The results indicate that employing LoRa to support Wi-Fi communication can significantly improve the functionality of robots operating in remote regions.

In this work, we demonstrated the viability of our framework using a single robotic platform while inherently retaining the capability to support multiple robots and instances. Our architecture leverages the Robot Operating System's namespace and topic remapping features, allowing each robot to publish and subscribe to uniquely prefixed topics (e.g., `/robot_<ID>/cmd_vel`), thereby isolating and managing concurrent Wi-Fi message streams. A single instance of the Zenoh bridge at the gateway is sufficient to ingest and process these parallel communications. Once received, messages are archived in the cloud along with their originating edge-device identifiers. Conversely, command messages can be targeted to individual robots by publishing to the appropriate namespaced topic.

Moreover, our framework accommodates LoRa communications: multicast downlink enables the simultaneous delivery of identical packets to a group of robots via a single gateway module. In principle, one gateway can orchestrate the bidirectional data flow for an entire robotic swarm, seamlessly linking edge devices with the cloud.

While the framework already supports multi-robot and multi-communication mechanisms, empirical validation within a true swarm setting remains to be conducted. Future work will focus on: (1) deploying and stress-testing the system with a heterogeneous fleet of robots; (2) evaluating network performance and latency in high-density LoRa multicast scenarios; (3) extending the cloud-storage schema to incorporate advanced metadata and secure access controls; and (4) optimizing the system's behaviour during communication mode switching, specifically addressing the stand-up time of the Zenoh bridge. In the current implementation, the Zenoh bridge process is terminated when switching from Transfer Mode to Storage Mode and restarted when switching back. This reinitialization introduces additional latency due to the Zenoh bridge's stand-up time, affecting the continuity of data transfer. To mitigate this, we propose developing an improved switching mechanism that avoids re-executing the Zenoh process.

This work contributes to the development of use-case scenarios for the validation of the IoT Cloud Operating System (ICOS), a meta operating system under development within the European Union's Horizon program. A notable limitation of the proposed framework is that, when data is stored locally in the absence of Wi-Fi, the logged data must be transferred to the cloud manually. It is anticipated that ICOS will ultimately manage the data transmission functionalities associated with this use case, encompassing data transfer and storage between edge devices and the cloud.

ACKNOWLEDGMENT

This project has received funding from the European Union's HORIZON research and innovation program under grant agreement No 101070177.

REFERENCES

[1] O. Kopishynska, Y. Utkin, O. Galych, M. Marenych, and I. Sliusar, "Main aspects of the creation of managing information system at the implementation of precision farming," in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, pp. 404–410.

[2] S. S. Baghel *et al.*, "Ai, iot and cloud computing based smart agriculture," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 2022, pp. 1658–1661.

[3] M. Iqbal, A. Y. M. Abdullah, and F. Shabnam, "An application based comparative study of lpwan technologies for iot environment," in *2020 IEEE Region 10 Symposium (TENSYMP)*, 2020, pp. 1857–1860.

[4] B. Jackson, A. S. A. Nisha, S. Varalakshmi, N. Darwin, and M. Varun, "Enhancing wifi range and throughput with beam steering antennas," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2023, pp. 1749–1754.

[5] A. Corsaro *et al.*, "Zenoh: Unifying communication, storage and computation from the cloud to the microcontroller," in *2023 26th Euromicro Conference on Digital System Design (DSD)*, 2023, pp. 422–428.

[6] X. Wang *et al.*, "Sparc-lora: A scalable, power-efficient, affordable, reliable, and cloud service-enabled lora networking system for agriculture applications," in *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2024, pp. 151–156.

[7] S. Ding *et al.*, "A scalable hybrid network for agriculture environment monitoring," in *2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN)*, 2021, pp. 566–570.

[8] Z. B. Arslanbenzer, B. Bayram, T. T. Sarı, and G. Seçinti, "Utilizing lora for control link in software-defined aerial networks: Analysis and implementation," in *2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2023, pp. 164–169.

[9] C.-S. Shih, H.-J. Lin, Y. Yuan, Y.-H. Kuo, and W.-Y. Liang, "Scalable and bounded-time decisions on edge device network using eclipse zenoh," in *2022 IEEE 28th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, 2022, pp. 170–179.

[10] J. J. L. Escobar, F. Gil-Castiñeira, and R. P. D. Redondo, "Decentralized serverless iot dataflow architecture for the cloud-to-edge continuum," in *2023 26th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, 2023, pp. 42–49.

[11] I. ElKassabi and A. Abdrabou, "An experimental comparative performance study of different wifi standards for smart cities outdoor environments," in *2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2022, pp. 0450–0455.

[12] B. Sudharsan, J. G. Breslin, and M. I. Ali, "Adaptive strategy to improve the quality of communication for iot edge devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–6.

[13] T. Zhao, S. Sarkar, Y. Tian, and D. Cabric, "Anomaly transmitter recognition and tracking," in *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2024, pp. 357–364.

[14] S. Macenski, T. Foote, B. Gerkey, C. Lalancette, and W. Woodall, "Robot operating system 2: Design, architecture, and uses in the wild," *Science Robotics*, vol. 7, no. 66, eabm6074, 2022.

[15] L. D. Vito, S. Rapuano, and L. Tomaciello, "One-way delay measurement: State of the art," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 12, pp. 2742–2750, 2008.