Janusz POCHMARA, Aleksandra ŚWIETLICKA, Krzysztof KOLANOWSKI

DOI: 10.15199/48.2025.04.16

# Industrial cybersecurity and machine learning

*Cyberbezpieczeństwo przemysłowe i uczenie maszynowe*

***Abstract.***
*Currently, we are witnessing the rapid development of industrial technologies, which bring numerous benefits but also introduce new threats. Many technological industries are focusing on Industry 4.0, where digitization and process automation are key, while emerging cyberthreats are becoming an increasingly significant issue. As the industry advances, cyberthreats evolve as well, requiring constant adaptation of defense strategies. However, by leveraging machine learning, we can better predict, detect, and neutralize these threats, safeguarding critical industrial assets from the growing number of cyberattacks. Therefore, the aim of this paper is to provide a comprehensive overview of the role of machine learning in enhancing cybersecurity in the industrial sector, considering both the benefits this technology offers and the challenges that must be overcome to effectively protect industrial systems from modern cyberthreats.*

***Streszczenie.***
*Współcześnie mamy do czynienia z dynamicznym rozwojem technologii przemysłowych, które przynoszą liczne korzyści, ale również nowe zagrożenia. Wiele branż technologicznych koncentruje się na Przemyśle 4.0, gdzie cyfryzacja i automatyzacja procesów odgrywają kluczową rolę, a pojawiające się cyberzagrożenia stają się coraz poważniejszym problemem. Wraz z rozwojem przemysłu ewoluują również zagrożenia cybernetyczne, co wymaga ciągłego dostosowywania strategii obronnych. Jednak dzięki zastosowaniu uczenia maszynowego możemy lepiej przewidywać, wykrywać i neutralizować zagrożenia, chroniąc kluczowe zasoby przemysłowe przed rosnącą liczbą cyberataków. Celem niniejszej pracy jest kompleksowe przedstawienie roli uczenia maszynowego w poprawie cyberbezpieczeństwa w przemyśle, z uwzględnieniem zarówno korzyści płynących z tej technologii, jak i wyzwań, które należy pokonać, aby skutecznie chronić systemy przemysłowe przed współczesnymi zagrożeniami cybernetycznymi.*

**Keywords:** Industrial Technologies, Industry 4.0, Machine Learning, Cybersecurity, Cyberattacks
**Słowa kluczowe:** technologie przemysłowe, Przemysł 4.0, uczenie maszynowe, cyberbezpieczeństwo, ataki cybernetyczne

## Introduction

Many technological industries are focusing on Industry 4.0, where digitization and process automation are key, and emerging cyberthreats are becoming an increasingly significant challenge. As the industry evolves, so do cyberthreats, necessitating constant adaptation of defense strategies. However, by leveraging machine learning (ML), we can better predict, detect, and neutralize these threats, protecting critical industrial resources from the growing number of cyberattacks. This has driven the search for new solutions utilizing artificial intelligence. For example, ML models can analyze data from sensors and programmable logic controllers (PLCs), identifying unusual patterns that may indicate potential attacks or system failures. ML is revolutionizing industrial cybersecurity by providing robust methods for anomaly detection, predictive maintenance, and real-time threat detection [1].

For instance, ML models analyze sensor data from Industrial Control Systems (ICS), such as SCADA, DCS, and PLCs, to identify irregular patterns signaling potential cyberattacks or system malfunctions [2]. Additionally, predictive maintenance powered by ML helps anticipate and prevent equipment failures, reducing downtime and repair costs [3].

Special attention should be given to the real-time operation of industrial systems, as it introduces additional challenges in detecting anomalies.

The growing reliance on networked solutions in industry increases the risk of cyberattacks. ML's capability to detect advanced persistent threats (APTs) in industrial networks is critical, as these models can identify subtle indicators of long-term, targeted attacks [4]. Federated learning further enhances security by enabling ML models to be trained across multiple sites without sharing raw data, thus preserving privacy and security [5]. Real-time threat detection is strengthened by ML models that continuously analyze data streams, flagging suspicious activities [6].

However, captured data can be compromised by unauthorized access, which may prevent ML models from functioning properly.

Therefore, ML systems must be protected against adversarial attacks that manipulate input data to deceive the models, posing significant risks to cyber-physical systems [7]. Integrating Security Orchestration, Automation, and Response (SOAR) tools with ML can greatly improve the efficiency of incident response [8]. Network traffic analysis using ML algorithms aids in identifying potential security breaches in industrial systems, combining ML with traditional security measures to ensure comprehensive defense [9].

Particular focus should be placed on devices, especially those in the Industrial Internet of Things (IIoT), which are rapidly advancing.

Securing IIoT devices with ML is both challenging and essential, requiring continuous adaptation to evolving threats [10]. ML models also enhance malware detection by identifying new and previously unknown malware variants [11]. Behavioral analysis using ML detects insider threats by spotting deviations from established user activity norms [12].

By considering user behavior in industrial systems, ML models allow for the observation and analysis of patterns, including user errors. Additionally, ML improves the security of remote access to industrial systems by continuously monitoring and authenticating user activities [13]. Enhancing SCADA security with ML involves real-time detection and response to cyberthreats, protecting critical industrial processes [14]. Phishing attacks targeting industrial systems are detected and blocked by ML algorithms, safeguarding sensitive information [15]. Finally, ML helps verify the integrity of industrial system data, ensuring it remains untampered and uncorrupted [16].

## Machine Learning (ML) in industry

Today, tools such as Artificial Intelligence (AI) can help detect patterns and identify potential adversaries whose behavior may be imperceptible to traditional methods. Recognizing cybersecurity as a balance between security and usability is key to understanding and implementing effective protection strategies. Detecting security incidents as they happen—or even before they fully develop—can significantly reduce potential damage. Therefore, developing and implementing advanced threat detection systems has become an essential element of effective protection in today's complex digital landscape.

Machine learning (ML) is a subfield of artificial intelli-

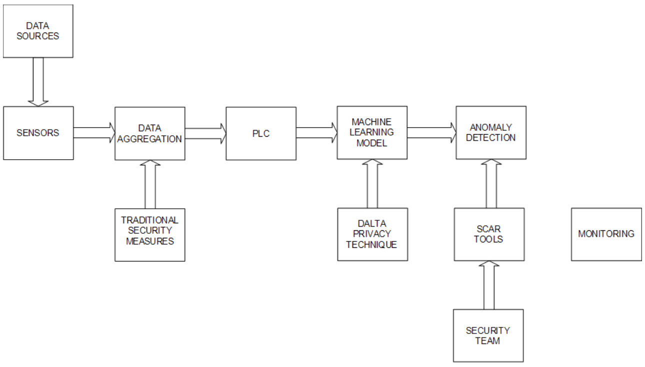

Fig. 1. Detecting anomalies in industry architecture.

gence that focuses on the development of algorithms and statistical models enabling computers to perform specific tasks without explicit instructions. Instead, ML relies on patterns and inference. Below are some basic concepts of machine learning, along with an introduction to common algorithms and evaluation techniques.

Machine learning can be categorized into several types:

- Supervised Learning
- Unsupervised Learning
- Semi-Supervised Learning
- Reinforcement Learning
- Self-Supervised Learning
- Multi-Instance Learning
- Transfer Learning

In supervised learning, the goal is often to minimize the loss function. For example, the loss function for regression is the mean squared error (MSE), given by the equation:

$$L(y, \hat{y}) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \tag{1}$$

where $y_i$ is the actual output, $\hat{y}_i$ is the predicted output, and $N$ is the number of samples.

Several common algorithms are used in machine learning. Some of the widely used ones include:

- Linear Regression
- Logistic Regression
- Support Vector Machines (SVM)

For instance, the formula for a linear regression model is given by:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + \epsilon \tag{2}$$

where $\beta$ represents the coefficients, and $\epsilon$ is the error term.

Model evaluation is a critical part of machine learning. Common metrics include: Accuracy is the proportion of true results (both true positives and true negatives) among the total number of cases examined. A confusion matrix provides a detailed breakdown of the model's performance, showing the number of true positives, true negatives, false positives, and false negatives. Optimization techniques are used to improve the performance of machine learning models by minimizing loss functions and adjusting model parameters.

In the field of cybersecurity, the pursuit of perfection is crucial. All potential access points, both physical and virtual, must be tightly secured. However, for an adversary, finding just one vulnerability or unsecured entry point is enough to achieve their goals. This asymmetry highlights the fact that while security is critically important, it cannot be the sole pillar of a defense strategy. There is a need not only to prevent attacks but also to prioritize detecting them.

The architecture diagram of a cybersecurity system using machine learning in industry shows the main components and their interactions. Here is its description:

- **Data Sources**: The initial point of the system where raw data is collected from various industrial processes.
- **Sensors**: Devices that gather real-time data from different aspects of industrial operations, such as temperature, pressure, or machine status.
- **PLCs (Programmable Logic Controllers)**: Essential components in industrial automation that process sensor data and control industrial equipment.
- **Data Aggregation**: The stage where data from various sources, including sensors and PLCs, is combined and formatted for further analysis.
- **Machine Learning Model**: The core analytical tool that processes the aggregated data to detect anomalies and predict potential security threats.
- **Anomaly Detection**: A dedicated module within the system that identifies unusual or suspicious patterns in the data.
- **SOAR Tools**: Tools that automate responses to detected threats, improving operational efficiency.
- **Traditional Security Measures**: Includes firewalls, IDS, and other classic protection techniques.
- **Data Privacy Techniques**: Protecting data privacy when training ML models, such as federated learning and differential privacy.
- **Security Team**: Specialists who monitor the system, respond to threats, and update protection strategies.

Today, industry cannot work without PLC controllers, which are a main elements of process automation systems. With technological improvement, need to secure these devices from increasingly sophisticated cyberthreats is growing. Machine learning appears to be a tool that can significantly enhance the security of PLC-based systems. Additionally, ML properties can be utilized for predictive maintenance of production processes, allowing for the prediction and prevention of equipment failures, thus minimizing downtime and repair costs.

### Machine modeling in industry

Increasing attention is being paid to the use of artificial intelligence (AI) elements for industrial security purposes. As mentioned earlier, this focus is becoming increasingly important as industrial systems grow more complex and are exposed to various cyberthreats. Machine learning (ML) is particularly noteworthy in this context, as it can significantly enhance the security of these systems by automatically detecting anomalies and threats in real time.

ML models can analyze data from sensors and programmable logic controllers (PLCs), identifying unusual patterns that may indicate potential attacks or failures. Today, the industry cannot operate without PLC controllers, which are key elements of process automation systems. As technology advances, the need to secure these devices from increasingly sophisticated cyberthreats is also growing. Machine learning emerges as a valuable tool for enhancing the security of PLC-based systems. Additionally, the capabilities of ML can be utilized for predictive maintenance of production processes, allowing for the anticipation and prevention of equipment failures, thereby minimizing downtime and repair costs.

1. **Building a machine learning model**
   Before the model can be used, it must be adapted to the function it is intended to perform in the process. To achieve this, it must go through specific stages of creation [17]. Creating a model in machine learning involves collecting an appropriate amount of data, which serves as the foundation for its development. The collected data is used to define problems and determine the requirements of the machine learning application. Data is an important element; therefore, the more data available, the better the ability to predict or identify potential sources. The quality of the data significantly affects the model's capabilities, ensuring that predictions and decision-making are reliable.
2. **Preprocessing data**
   Preprocessing and preparing data is a crucial step that involves transforming raw data into a format suitable for training and testing our models. This phase aims to clean the data by removing null and erroneous values, as well as normalizing and preprocessing it to achieve greater accuracy and performance in our machine learning models.
3. **Choosing a learning model**
   Selecting the appropriate machine learning model can be challenging, given the large number of algorithms available today. Therefore, it is necessary to carefully analyze their applications. Digital simulations are a valuable tool for this purpose.
   First, it is important to understand what problem the model will address in order to classify it appropriately. Different types of problems require different algorithms to create an effective predictive model.
   The best approach is often to experiment with multiple models, evaluate their metrics, and iteratively assess how well each algorithm generalizes to unseen data [17].
4. **Training the model**
   The training phase consists of preparing the model to develop expected responses based on progressive predictions. By using input data during training, the model begins to predict appropriate output data, which should correspond to actual values. In the context of cybersecurity, the model should be capable of distinguishing between anomalies and expected values.
5. **Evaluating performance**
   The model is evaluated by comparing the predicted values with the actual values obtained. This approach enables the estimation of error values, allowing us to determine how the model deviates from the desired response. Various metrics are used to evaluate model performance, which can be categorized into two forms [17]:
   (a) **Regression tasks**: Mean Absolute Error, Mean Squared Error, Root Mean Squared Error, R-squared Value (R²);
   (b) **Classification tasks**: Accuracy, Precision, Recall, F1-score, Confusion Matrix.
6. **Matching and optimization**
   To enhance the model's performance, the next step is to optimize it further. Optimization involves fine-tuning hyperparameters, selecting the best algorithm, and improving features through feature engineering techniques. Hyperparameters are settings defined before the training process begins, and they influence the behavior of the machine learning model. Examples include learning rate, regularization, and other model-specific parameters. Properly tuning these aspects allows us to maximize the model's performance.
7. **Making predictions**
   This process ensures that the model, when working on data it has not previously encountered, makes accurate predictions. Once deployment is complete, the model is ready to predict new data, which involves feeding unseen data into the deployed model to enable real-time decision-making [17].
8. **Algorithms**
   In this paper, the description of the linear model based on regression is limited. Of course, this is only the beginning of the research, but the intention is to demonstrate how well simple solutions work in practical applications. In the context of linear models used in classification, the main models are:
   (a) **Logistic Regression**: This is the most popular linear classification model. It models the relationship between input variables and the probability of belonging to a specific class using the sigmoid function. Despite the name "regression," it is used for classification tasks.
   (b) **Linear Discriminant Analysis (LDA)**: LDA is a model that seeks a linear combination of features to maximally separate the classes. It is particularly effective for problems where the data follow a normal distribution.
   (c) **Linear Support Vector Machine (Linear SVM)**: This is a variant of SVM that uses a linear kernel for classification. The model aims to find a linear decision boundary that maximizes the margin between different classes.
   (d) **Perceptron**: This is the simplest neural network model that performs linear classification. It is designed for binary classification problems, where the output is determined by a linear combination of features.
9. **Detailed steps**
   - **Initialization**: Assume all weights are initially set to 0 or small random values.
   - **Iteration over data**: The model iterates through the entire dataset to minimize the error.
   - **Weight update**: Weights are updated only when the perceptron makes an error.
   - **Convergence**: The training process continues until the perceptron correctly classifies all data or reaches the maximum number of iterations.
   - **Repeat for a specified number of iterations or until convergence**:
     - For each training sample $(x_i, y_i)$, calculate the weighted sum:

       $$z = w_1 \cdot x_{i1} + w_2 \cdot x_{i2} + \ldots + w_n \cdot x_{in} + b \tag{3}$$

     - Apply the activation function (usually a step function):

       $$y_{\text{pred}} = \begin{cases} 0 \text{ if } z < 0 \\ 1 \text{ if } z \geqslant 0 \end{cases} \tag{4}$$

     - If $y_{\text{pred}}$ is different from the true label $y_i$, update the weights and bias:

       $$\Delta w_j = \eta \cdot (y_i - y_{\text{pred}}) \tag{5}$$

       $$w_j \leftarrow w_j + \Delta w_j \tag{6}$$

$$b \leftarrow b + \eta \cdot (y_i - y_{\text{pred}}) \tag{7}$$

where $\eta$ is the learning rate.

- **End of the algorithm**: After completing the iterations or achieving convergence, the perceptron is ready to be used on new data.

A simple demonstration of how it works uses a Perceptron-based machine learning algorithm. The perceptron was trained on the example of the AND logic gate. The decision boundary of the perceptron at initialization, when the weights are set using the Xavier method, is random due to the random nature of the weights. After 10 iterations of training, it produced the following results:

(a) **Weights**: $[0.2358, 0.2387]$,

(b) **Bias (offset value)**: $-0.4074$,

(c) The operation of the perceptron on the training set leads to the following predictions:

- For input $[0, 0]$, the perceptron predicts 0.
- For input $[0, 1]$, the perceptron predicts 0.
- For input $[1, 0]$, the perceptron predicts 0.
- For input $[1, 1]$, the perceptron predicts 1.

Figure 2 demonstrates the detected logic anomalies $[1, 0]$, while Figure 3 presents the architecture of the used perceptron (2 inputs, 1 output, and bias). It is clear that it performs well with classification problems, but more complex issues require more advanced algorithms.

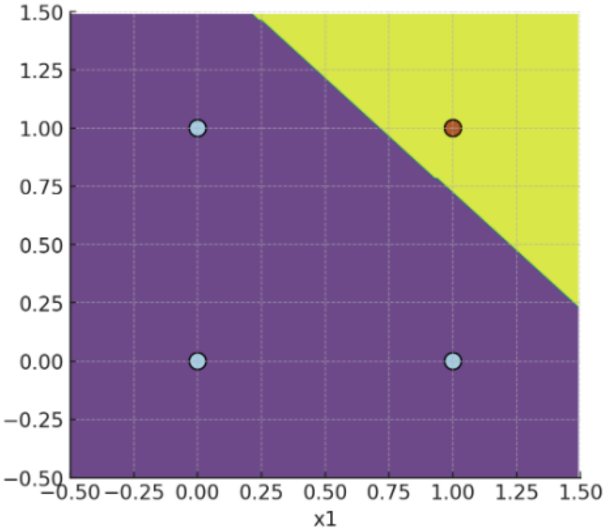

Fig. 2. Decision Boundary of perceptron for AND logic function.

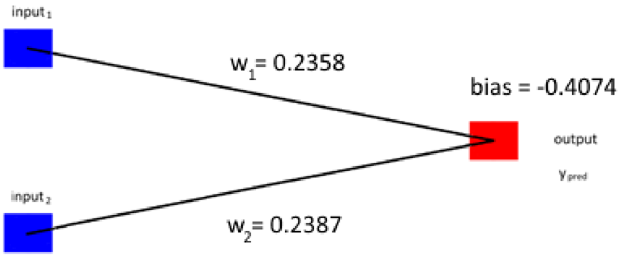

Fig. 3. Architecture of perceptron used for simulation of the AND logic gate.

The decision boundary after training shows that the perceptron has successfully learned to classify the points for the AND function. The AND function can be applied to detect anomalous situations that may indicate a cyberattack or system breach. For example:

```
    IF (Access level = Administrator AND
Control parameter changes outside of working
hours) THEN Report suspicious activity.
```

Such rules help identify potential threats when specific conditions are met (e.g., an administrator changing settings at an unusual time), which could indicate unauthorized activity within the system.

## Conclusions

At the same time, machine learning (ML) systems must be secured against attacks that can manipulate input data, potentially distorting the models. Cybersecurity in ML also involves protecting data privacy through techniques that enable model training without revealing operational data. An integrated approach to cybersecurity, combining traditional methods with modern ML techniques, is essential for safeguarding industrial infrastructure. Furthermore, automating security processes with additional tools can enhance the efficiency of threat response.

As ML technology continues to evolve, it is crucial to research and update protection strategies continually to keep pace with the changing threat landscape. Educating and training security teams on ML-specific threats is also vital for effectively protecting industrial systems.

In our article, we point out that PLCs are vulnerable and it is now common for them to lack adequate security. The only protection used so far is complete isolation from the outside world, which does not fully fit into the definitions of Industry 4.0 and 5.0.

To effectively use technologies such as perceptron or regression in the context of hazard classification, it is essential to use real data that reflects complex operational conditions. This is the only way to develop reliable and useful models that can effectively identify and respond to real threats. Therefore, it was decided to focus on potential tools rather than solutions that are still in development.

An algorithm has been demonstrated that illustrates how ML can be applied to make decisions in classification problems, making it particularly well-suited for digital data classification. The next step will be to implement ML in real systems, allowing us to confront the genuine challenges of time and data management.

## Acknowledgment

This work is financed from the research Grant No. 0211/SBAD/0123.

***Authors:***
*Ph.D. Janusz Pochmara, janusz.pochmara@put.poznan.pl, Ph.D. D.Sc. Aleksandra Świetlicka, aleksandra.swietlicka@put.poznan.pl, Ph.D. Krzysztof Kolanowski, krzysztof.kolanowski@put.poznan.pl, Institute of Automatic Control and Robotics, Poznań University of Technology, 60-965 Poznań, POLAND*
.

# REFERENCES

[1] J. Pochmara and A. Świetlicka, “Cybersecurity of industrial systems—a 2023 report,” Electronics, vol. 13, no. 7, 2024, doi: https://doi.org/10.3390/electronics13071191.

[2] M. Nankya, R. Chataut, and R. Akl, “Securing industrial control systems: Components, cyber threats, and machine learningdriven defense strategies,” Sensors, vol. 23, no. 21, 2023, doi: https://doi.org/10.3390/s23218840.

[3] B. Kumbhar, K. Kene, A. Raut, and P. Pisal, “Suspicious activity detection using machine learning,” International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 5, pp. 3745–3748, 2023, doi: https://doi.org/10.22214/ijraset.2023.52486.

[4] P. Shah, “Machine learning-based real-time threat detection for banks,” 2024, accessed: 2024-08-26. [Online]. Available: https://www.impetus.com/resources/blog/machinelearning-based-real-time-threat-detection-for-banks/

[5] L. A. Johnson Kinyua, “Ai/ml in security orchestration, automation and response: Future research directions,” Intelligent Automation & Soft Computing, vol. 28, no. 2, pp. 527–545, 2021, doi: https://doi.org/10.32604/iasc.2021.016240.

[6] A. M. Y. Koay, R. K. L. Ko, H. Hettema, and K. Radke, “Machine learning in industrial control system (ics) security: current landscape, opportunities and challenges,” Journal of Intelligent Information Systems, vol. 60, no. 2, pp. 377–405, Apr 2023, doi: https://doi.org/10.1007/s10844-022-00753-1.

[7] Kaspersky Company, “Ai and machine learning in cybersecurity – how they will shape the future,” 2024, accessed: 2024-08-26. [Online]. Available: https://www.kaspersky.com/resourcecenter/definitions/ai-cybersecurity

[8] R. King, “The role of ai & ml in industry 4.0,” 2024-04-18, accessed: 2024-08-26. [Online]. Available: https://www.rowse.co.uk/blog/post/the-role-of-ai-ml-inindustry-4-0

[9] C. S. D. Souza, “Adversarial attacks on ai/ml models: Everything you need to know,” 2023-07-30, accessed: 2024-08-26. [Online]. Available: https://www.linkedin.com/pulse/adversarialattacks-aiml-models-everything-you-need-know-d-souza/

[10] J. Harper, “Machine learning for real-time data analysis: Training models in production,” 2023-10-24, accessed: 2024-08-26. [Online]. Available: https://thenewstack.io/machine-learningfor-real-time-data-analysis-training-models-in-production/

[11] M. Ramaiah and M. Y. Rahamathulla, “Securing the industrial iot: A novel network intrusion detection models,” in 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), 2024, pp. 1–6, doi: https://doi.org/10.1109/AIIoT58432.2024.10574728.

[12] B. Al-Muntaser, M. A. Mohamed, A. Y. Tuama, and I. A. Rana, “Cybersecurity advances in scada systems,”International Journal of Advanced Computer Science and Applications, vol. 14, no. 8, 2023, doi: https://doi.org/10.14569/IJACSA.2023.0140835.

[13] Perception Point, “Phishing detection: Identifying phishing emails and websites,” 2024, accessed: 2024-08-26. [Online]. Available: https://perception-point.io/guides/phishing/phishingdetection-identifying-phishing-emails-and-websites/

[14] B. J. Aboze, “Why data integrity is crucial for effective ml monitoring,” https://deepchecks.com/why-data-integrity-iscrucial-for-effective-ml-monitoring/, 2023, accessed: 2024-08-26. [Online]. Available: https://deepchecks.com/why-dataintegrity-is-crucial-for-effective-ml-monitoring/

[15] R. S. Siva Kumar, M. Nyström, J. Lambert, A. Marshall, M. Goertzel,A. Comissoneru, M. Swann, and S. Xia, “Adversarial machine learning-industry perspectives,” in 2020 IEEE Security and Privacy Workshops (SPW), 2020, pp. 69–75, doi: https://doi.org/10.1109/SPW50608.2020.00028.

[16] European Commission, “Ethics guidelines for trustworthy AI,” https://digital-trategy.ec.europa.eu/en/library/ethicsguidelines-trustworthy-ai, 2019-04-08, accessed: 2024-08-26. [Online]. Available: https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthyai

[17] GeeksforGeeks, “Steps to build a machine learning model,” https://www.geeksforgeeks.org/steps-to-build-amachine-learning-model/, 2024-02-29, accessed: 2024-08-26. [Online]. Available: https://www.geeksforgeeks.org/steps-tobuild-a-machine-learning-model/