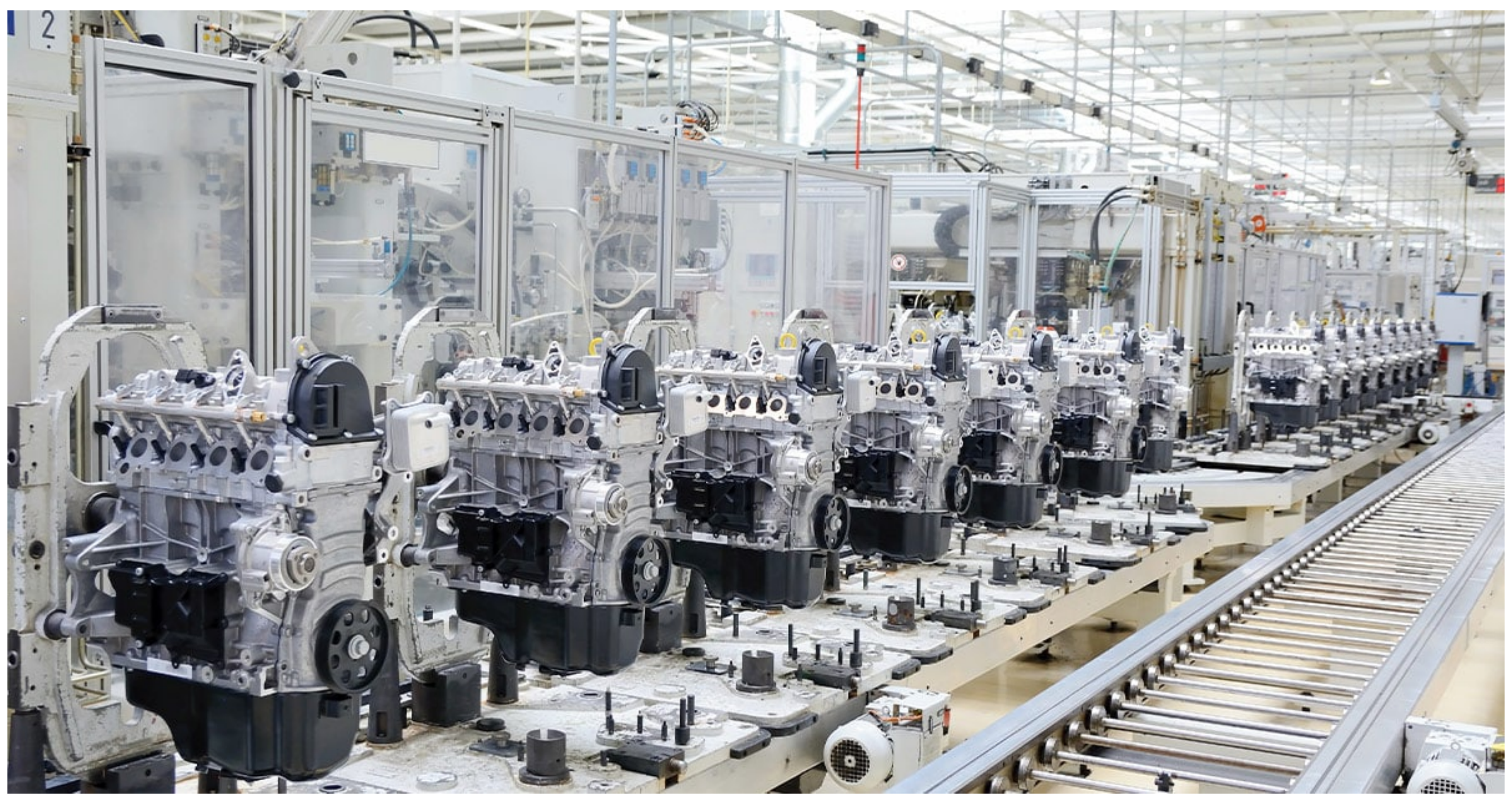
THREAT DETECTION IN IIOT NETWORKS THROUGH DEEP PACKET INSPECTION AND MACHINE LEARNING MECHANISMS

Jan Guziuk, Hubert Masłowski, Waldemar Graniszewski, Krzysztof Sosnowski
Faculty of Eletronics, Warsaw University of Technologies
jan.guziuk.stud@pw.edu.pl, hubert.maslowski.stud@pw.edu.pl,
waldemar.graniszewski@ee.pw.edu.pl, krzysztof.sosnowski@pw.edu.pl

Introduction

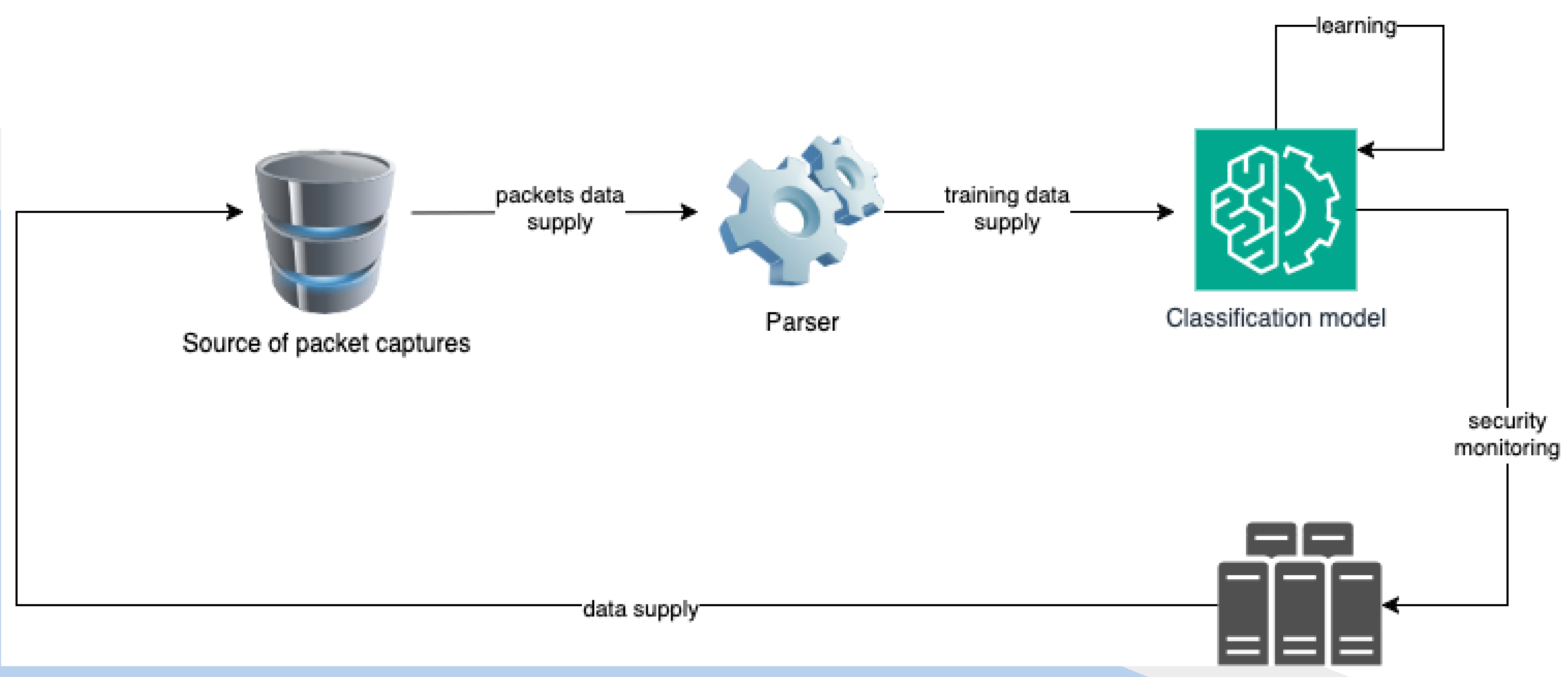
The proliferation of Industrial Internet of Things (IIoT) net- works has precipitated unprecedented cybersecurity challenges across critical infrastructure domains. Emerging communication paradigms in power grids, manufacturing, and healthcare systems expose intricate vulnerabilities to sophisticated cyber threats, including precision-targeted attacks such as protocol manipulation, data exfiltration, and distributed denial of service methodologies. Deep Packet Inspection (DPI) has emerged as a pivotal analytical approach, enabling granular extraction of protocol-specific behavioral signatures that transcend traditional network surveillance methodologies. This research instantiates a threat detection pipeline structured to analyze IIoT communication protocols through machine learning mechanisms. By developing protocol-aware parsing architectures and implementing classification algorithms, the study explores the computational boundaries of anomaly detection in industrial networked environments.



Methodology

Solution architecture

The pipeline begins with protocol parsing, where each packet's structure is dissected to extract meaningful fields such as headers, flags, and payload data. These extracted features are then fed into classification algorithms trained on labeled datasets of normal and malicious packets. The ML models employ Random Forest to detect anomalies based on learned patterns. This approach enables real-time detection of threats such as unauthorized access, data manipulation, or suspicious data spikes, which allows industrial architecture owners to effectively handle security incidents.



Datasets

For Modbus analysis, we utilized the ToN IoT dataset, developed by UNSW Canberra Cyber, which includes telemetry from IIoT protocols such as Modbus, collected in a realistic Industry 4.0 testbed.
For MQTT analysis, we employed the MQTTset dataset, which captures detailed MQTT traffic from a simulated smart environment. The dataset includes both normal and attack traffic, such as DoS, MQTT Publish floods, SlowITe attacks, and malformed packets.

Results

Classification performance

Modbus

Random Forest not only achieved the highest accuracy but also provided the most balanced performance in terms of precision and recall.

Model	Accuracy	Precision	Recall	F1	AUC
Random Forest	0.9933	0.9825	0.9876	0.9851	0.9913
Naive Bayes	0.8036	0.5638	0.5449	0.5542	0.7116
Neural Network	0.9854	0.9525	0.9840	0.9680	0.9849

MQTT

The Random Forest model provided the most balanced performance across accuracy, precision, recall, and F1 score. Naive Bayes, while offering the fastest training time, exhibited comparatively weaker results.

Model	Accuracy	Precision	Recall	F1
Random Forest	0.9633	0.9600	0.9600	0.9624
Naive Bayes	0.8542	0.8900	0.8500	0.8294
Neural Network (0.52)	0.9960	1.0000	0.7083	0.8292

Neural network ptimization with SMOTE

SMOTE-based augmentation significantly increased false positives, rendering the model impractical for real-world deployment.

Non-SMOTE neural network

	Predicted Benign	Predicted Malicious
Actual Benign	357,449	0
Actual Malicious	1,455	3,533

SMOTE neural network

	Predicted Benign	Predicted Malicious
Actual Benign	224,800	132,649
Actual Malicious	53	4,935

Conclusion

This study demonstrated that integrating deep packet inspection with machine learning enables effective binary classification of IIoT network traffic. By extracting protocol-specific features from MQTT and Modbus traffic, we evaluated and compared the performance of multiple classifiers under realistic conditions of class imbalance.

Random Forest proved to be the most reliable model, achieving balanced precision and recall across both protocols without requiring extensive oversampling, in contrast to the neural network model, underscoring the importance of aligning model complexity with data characteristics.

These results highlight the value of protocol-aware feature engineering and stress the limitations of using a one-size-fits-all approach in security-critical environments. For practitioners deploying intrusion detection systems in IIoT networks, model interpretability, data imbalance handling, and sensitivity to thresholds must be prioritized alongside accuracy.

References

[1] Modbus Organization. ”Modbus Application Protocol Specification v1.1b3.” Accessed February 2, 2025. `https://modbus.org/`.

[2] Harrington, David, Presuhn, Randy, and Wijnen, Bert. ”An Architecture for Describing SNMP Management Frameworks.” RFC 3411, 2002.

[3] Vaccari, I.; Chiola, G.; Aiello, M.; Mongelli, M.; Cambiaso, E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT. Sensors 2020, 20, 6578.

[4] Moustafa, Nour, and Jill Slay. ”UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set).”Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

[5] Jeatrakul, P., Wong, K.W., Fung, C.C. (2010). Classification of Imbalanced Data by Combining the Complementary Neural Network and SMOTE Algorithm. In: Wong, K.W., Mendis, B.S.U., Bouzerdoum, A. graphic graphic graphic

[6] ATS — Machine Data Collection in Manufacturing `https://www.advancedtech.com/blog/machine-data/`