Graduate School MADIS-631, University of Lille, ENSAIT & GEMTEX

Ph.D. VAE THESIS

To obtain the grade of:

Doctor from the University of Lille

Specializing in

Computer Science and Automatic Control

(Sub-specialty: Artificial Intelligence)

By

Kim Duc Tran

Contributions to Monitoring, Anomaly Detection, and Classification Using Artificial Intelligence and Statistical Methods: Applications in Smart Manufacturing and Healthcare

The thesis was defended on 21 - 11 - 2025 before the jury composed of:

Ludovic MACAIRE	Prof.	University of Lille	(President)
Abdessamad KOBI	Prof.	University of Angers	(Reviewer)
Salah BOURENNANE	Prof.	Ecole Centrale de Marseille	(Reviewer)
Anthony FLEURY	Prof.	IMT Nord Europe	(Examiner)
Christine THOMAS-AGNAN	Prof.	Toulouse School of Economics	(Examiner)
Maroua NOUIRI	MCF	University of Nantes	(Examiner)
Ludovic KOEHL	Prof.	University of Lille	(VAE Thesis Director)

Ecole doctorale MADIS-631, Université de Lille, ENSAIT & GEMTEX

Doctorat par la VAE

pour obtenir le grade de:

Docteur de l'Université de Lille

dans la spécialité

Informatique et Automatique (sous-spécialité : Intelligence Artificielle)

par

Kim Duc Tran

Contributions à la surveillance, à la détection des anomalies et à la classification à l'aide de l'intelligence artificielle et de méthodes statistiques: Applications dans la fabrication intelligente et les soins de santé intelligents.

Thèse soutenue le 21 - 11 - 2025 devant le jury composé de :

Ludovic MACAIRE	Prof.	Université de Lille	(Président)
Abdessamad KOBI	Prof.	Université d'Angers	(Rapporteur)
Salah BOURENNANE	Prof.	Ecole Centrale de Marseille	(Rapporteur)
Anthony FLEURY	Prof.	IMT Nord Europe	(Examinateur)
Christine THOMAS-AGNAN	Prof.	Toulouse School of Economics	(Examinateur)
Maroua NOUIRI	MCF	Université de Nantes	(Examinateur)
Ludovic KOEHL	Prof.	Université de Lille	(Directeur de thèse VAE)

Declaration of Authorship

I, **Kim Duc TRAN**, declare that this thesis titled, "Contributions to Monitoring, Anomaly Detection, and Classification Using Artificial Intelligence and Statistical Methods: Applications in Smart Manufacturing and Healthcare" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at the University of Lille.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have quoted from the work of others, the source is always given. Except for such quotations, this thesis is entirely my work.
- Where the thesis is based on work I did jointly with others, I have clarified exactly what others did and what I contributed myself.

Signed:

Date:

"The more I know, the more I realize I know nothing."

Socrates

Résumé

(*French*)

La convergence des technologies avancées – intelligence artificielle (IA), Internet des objets (IoT), cloud computing et analyse en périphérie a accéléré la transformation de l'industrie manufacturière vers le paradigme numérique de l'Industrie 4.0. Au-delà de l'automatisation, la vision émergente de l'Industrie 5.0 met l'accent sur la durabilité, la conception centrée sur l'humain et la résilience des systèmes. Cette thèse contribue à cette évolution en développant des cadres robustes et explicables pour la surveillance, la détection des anomalies et la classification, adaptés aux deux domaines de la fabrication intelligente et de la santé.

S'appuyant sur plus de dix ans d'expérience pratique en IA et alignée sur les objectifs stratégiques de la Chaire internationale en science des données et intelligence artificielle explicable (DS & XAI), cette recherche s'articule autour de trois piliers interconnectés. Premièrement, elle introduit des cadres adaptatifs et respectueux de la confidentialité pour la détection et la classification des anomalies, destinés aux applications de santé intelligentes, utilisant des techniques d'apprentissage fédéré et d'IA explicable. Ces modèles permettent une analyse décentralisée et en temps réel des données de santé sensibles, favorisant ainsi une prestation de soins prédictive et personnalisée.

Dans un second temps, ces travaux favorisent l'intégration de l'IA dans les pratiques industrielles durables en améliorant la détection et le pronostic des anomalies dans la fabrication intelligente. En combinant l'apprentissage fédéré, la blockchain et les algorithmes d'apprentissage automatique, les systèmes proposés privilégient la sécurité, l'équité et la transparence – principes fondamentaux de l'Industrie 5.0 – tout en optimisant l'efficacité des processus et la résilience opérationnelle.

Troisièmement, la thèse exploite le calcul statistique et les statistiques industrielles – notamment les cartes de contrôle et l'analyse de fiabilité pour améliorer la surveillance des processus, le contrôle qualité et la prise de décision dans les environnements industriels. Ces méthodologies contribuent à l'objectif plus large de relier la recherche théorique en IA à des mises en œuvre pratiques et efficaces.

Ces recherches sont étroitement liées au projet REVALOTEX (2023-2026) et bénéficient de collaborations internationales entre l'Université Dong A (Vietnam) et l'ENSAIT–Université de Lille (France), sous l'égide de la Chaire internationale 'International Research Institute for Artificial Intelligence and Data Science' hébergée à l'Université de Dong A au Vietnam. Elles renforcent la mission de la Chaire: promouvoir une IA fiable, transparente, éthique et centrée sur l'humain, tout en contribuant à la formation des futurs leaders en systèmes d'IA durables. En formalisant ce travail par la Validation des Acquis de l'Expérience (VAE) et la recherche doctorale, cette thèse établit une base pour diriger une innovation transdisciplinaire et pertinente à l'échelle mondiale à l'ère de l'Industrie 5.0.
Mots clés: Sécurité, protection des données, soins de santé, détection d'anomalies, intelligence artificielle explicable, intelligence artificielle, systèmes embarqués, attaques par empoisonnement, empoisonnement de données, empoisonnement de modèles, attaques byzantines.

Abstract

The convergence of advanced technologies- artificial intelligence (AI), the Internet of Things (IoT), cloud computing, and edge analytics innovations catalyzed the transformation of manufacturing into the digital paradigm of Industry 4.0. Moving beyond automation, the emergent Industry 5.0 vision emphasizes sustainability, human-centered design, and resilient systems. This thesis contributes to this evolving landscape by developing robust and explainable frameworks for monitoring, anomaly detection, and classification, tailored to the dual domains of smart manufacturing and healthcare.

Grounded in over a decade of practical experience in AI and aligned with the strategic objectives of the International Chair in Data Science and Explainable Artificial Intelligence (DS & XAI), the research unfolds across three interconnected pillars. First, it introduces adaptive, privacy-preserving anomaly detection and classification frameworks for smart healthcare applications using federated learning and explainable AI techniques. These models enable real-time, decentralized analysis of sensitive health data, supporting predictive and personalized healthcare delivery.

Second, the work advances AI integration into sustainable industrial practices by enhancing anomaly detection and prognostics in smart manufacturing. By combining federated learning, blockchain, and machine learning algorithms, the proposed systems prioritize security, fairness, and transparency—core principles of Industry 5.0—while also optimizing process efficiency and operational resilience.

Third, the thesis leverages statistical computing and industrial statistics, including control charts and reliability analysis, to improve process monitoring, quality control, and decision-making in industrial environments. These

methodologies contribute to the broader goal of bridging theoretical AI research with practical, impactful implementations.

This research is closely connected to the REVALOTEX (2023–2026) project and benefits from international collaborations between Dong A University (Vietnam) and ENSAIT–University of Lille (France), under the auspices of the International Chair's International Research Institute for Artificial Intelligence and Data Science, hosted in Dong A University, Vietnam. It reinforces the Chair's mission of fostering Trustworthy, Transparent, Ethical, and Human-Centered AI while contributing to the training of future leaders in sustainable AI systems. By formalizing this work through the Validation of Acquired Experience (VAE) and doctoral research, this thesis establishes a foundation for leading transdisciplinary and globally relevant innovation in the Industry 5.0 era.

Keywords: Federated Learning, Healthcare, privacy, security, explainable AI, anomaly detection, poisoning attacks, data poisoning, model poisoning, Byzantine attacks.

Acknowledgements

I would like to express my deepest gratitude to the Evaluation Committee for their rigorous, fair, and constructive assessment throughout the VAE process. This doctoral degree—obtained through the Validation des Acquis de l'Expérience (VAE) at the Université de Lille—recognizes more than a decade of scientific contributions in Artificial Intelligence, Applied Statistics, Smart Manufacturing, and Smart Healthcare. I am profoundly thankful to my family, whose support made this journey possible: my wife Thi Diem Doan, who cared for our children during my time in France; my father Kim Mot Tran, whose lifelong philosophy shaped my scientific mindset; my mother Thi Lan Phan, whose resilience has always inspired me; and my brother Kim Phuc Tran, who guided and encouraged me from childhood. My sincere appreciation goes to Dong A University, especially Rector Nguyen Thi Anh Dao and President Luong Minh Sam, for entrusting me with the development of the AI & Data Science Research Institute, and for supporting the supervision of young researchers such as Hoang Nguyen Le, Long Hai Le, and Tran Viet Hieu, as well as the expansion of the International Chair in DS & XAI. I also extend my heartfelt thanks to ENSAIT – GEMTEX – Université de Lille, my academic home in France, and to the distinguished professors whose mentorship shaped my scientific trajectory: Ludovic Koehl, Cédric Heuchenne, Xianyi Zeng, Bruno Agard, Hongmei He, Sébastien Thomassey, Damien Soulat, Giovanni Celano, Pascal Bruniaux, Khanh Nguyen, and Guillaume Tartare. Finally, I am grateful to my colleagues and friends whose collaboration and encouragement have been essential throughout this long journey. This recognition marks both the culmination of a mature scientific path and the beginning of a renewed commitment to advancing human-centered AI and France–Vietnamese scientific cooperation.

Dissemination

The work presented in this thesis has been disseminated in the following journal publications, presented in descending chronological order:

Peer-reviewed Journals (Indexed in the Web of Science)

- T. Banfalvi, D.H. Nguyen, K.D. Tran*, G. Tartare, P. Bruniaux, K.P. Tran. (2025). "Mesh Deep Support Vector Data Description: Unsupervised Anomaly Detection in 3D Human Leg Morphologies for Adaptive Compression Stocking Design," Intelligent Systems with Applications, Elsevier, Under Review

- T.T.V. Nguyen, C. Heuchenne , K.D. Tran, G. Tartare, K.P. Tran. (2024). "SVDD Control Charts Based on Mewma Technique for Monitoring Compositional Data," Computers & Industrial Engineering, Elsevier, https://doi.org/10.1016/j.cie.2025.110865

- A. Raza, S. Li, K.P. Tran, L. KOEHL, K.D. Tran* (2024). "Using Anomaly Detection to Detect Poisoning Attacks in Federated Learning Applications" *Knowledge-Based Systems*. Elsevier. Under Review.

- A. Raza, K.P. Tran, L. KOEHL, X. Zeng, K. Benzaidi, S. Li, S. Hotham, K.D. Tran*(2024). "Lightweight Transformer in Federated Setting for Human Activity Recognition in Home Care" *Pattern Recognition*. Elsevier. Under Review.

- H.D. Nguyen, A.A. Nadi, K.D. Tran*, P. Castagliola, G. Celano, K.P. Tran (2023). "The Shewhart-type RZ control chart for monitoring the ratio of autocorrelated variables" *International Journal of Production Research*. Taylor & Francis, pp. 6746-6771. http://dx.doi.org/10.1080/00207543.2022.2137594

- A.A. Nadi, B.S. Gildeh, J. Kazempoor, K.D. Tran, K.P. Tran (2023). "Cost-effective optimization strategies and sampling plan for Weibull quantiles under type-II censoring" *Applied Mathematical Modelling*. Elsevier, pp. 16–31. http://dx.doi.org/10.1016/j.apm.2022.11.004

- K.D. Tran, A.A. Nadi, T.H. Nguyen, K.P. Tran (2021). "One-sided Shewhart control charts for monitoring the ratio of two normal variables in short production runs" *Journal of Manufacturing Processes*. Elsevier, vol. 69, pp. 273–289. http://dx.doi.org/10.1016/j.jmapro.2021.07.031

- H.D. Nguyen, K.P. Tran, K.D. Tran(2021). "The effect of measurement errors on the performance of the Exponentially Weighted Moving Average control charts for the Ratio of Two Normally Distributed Variables" *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2020.11.042

- Q.T. Nguyen, V. Giner-Bosch, K.D. Tran, C. Heuchenne, K.P. Tran (2021). "One-sided variable sampling interval EWMA control charts for monitoring the multivariate coefficient of variation in the presence of measurement errors" *The International Journal of Advanced Manufacturing Technology*. Springer London, vol. 115, pp. 1821-1851. https://link.springer.com/article/10.1007/s00170-021-07138-8

- K.D. Tran, H.D. Nguyen, T.H. Nguyen, K.P. Tran (2021). "Design of a variable sampling interval exponentially weighted moving average median control chart in the presence of measurement errors" *Quality and Reliability Engineering International*, vol. 37, pp. 374-390. http://dx.doi.org/10.1002/qre.2726

Chapters in Books

- T. Nguyen, Q.T. Nguyen, K.D. Tran*, L. KOEHL, K.P. Tran, (2024), "Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data," in *Book: Responsible Artificial Intelligence and Data Science* https://link.springer.com/book/9783032140548

- L.H. Nguyen, Q.T. Nguyen, K.D. Tran*, H.D. Nguyen, S. Thomassey, X.Zeng, K.P. Tran, (2024), "Deep CNN for Remaining Useful Life Prediction: An XAI Approach Using SHAP for Model Interpretation," in *Book: Responsible Artificial Intelligence and Data Science* https://link.springer.com/book/9783032140548

- D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran, (2024), "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study," in *Responsible Artificial Intelligence and Data Science* .

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024), "Explainable Transformer-based Approach for ECG Anomaly Detection," in *Book: Responsible Artificial Intelligence and Data Science* https://link.springer.com/book/9783032140548

- T. Banfalvi, D.H. Nguyen, K.D. Tran, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024), "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings," in *Book: Responsible Artificial Intelligence and Data Science* https://link.springer.com/book/9783032140548

- T. Banfalvi, K.D. Tran, G. Tartare, P. Bruniaux, K.P. Tran (2024), "Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression

Stockings: A survey and perspective," in *Book: Responsible Artificial Intelligence and Data Science*
https://link.springer.com/book/9783032140548

- D.H. Nguyen, D.P.T. Nguyen, Q.C. Ta, S. Thomassey, and K.D. Tran*(2025). "Natural Language Processing applications in Smart Manufacturing: A Survey and Perspective" Book: Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0, Springer Nature Switzerland AG. Submitted.

- T.H. Nguyen, J.M. Masereel, D.H. Nguyen, K.D. Tran*, and K.P. Tran (2025). "Explainable anomaly detection with Artificial Intelligence and Statistical Methods for Predictive Maintenance in Smart Manufacturing systems: A Survey and Perspective" Book: Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0, Springer Nature Switzerland AG. Submitted.

- D.H. Nguyen, D.P.T. Nguyen, Q.C. Ta, S, K.D. Tran*, and K.P. Tran (2025). "Human-Centered Explainable Anomaly Detection in Smart Manufacturing: Bridging AI and Human Decision-Making in Industry 5.0" Book: Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0, Springer Nature Switzerland AG. Submitted.

- V.H. Tran, D.H. Nguyen, K.D. Tran*, S. Thomassey, and K.P. Tran (2025). "Anomaly and Novelty Detection in Non-Stationary Time Series: Deep, Hybrid, and Federated Perspectives" Book: Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0, Springer Nature Switzerland AG. Submitted.

- T.Q.D. Pham, K.D. Tran*, K.T.P. Nguyen, X.V. Tran,L. KOEHL, and K.P. Tran (2024). "A new framework for prognostics in decentralized industries: Enhancing fairness, security, and transparency through Blockchain and Federated Learning" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- T.H. Nguyen, A. Saghir, K.D. Tran*,D.H. Nguyen,N.A. Luong, K.P. Tran (2024). "Safety and Reliability of Artificial Intelligence systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_9

- T. Nguyen, D.H. Nguyen, Q.T. Nguyen, K.D. Tran*, K.P. Tran (2024). "Human-Centered Edge AI and Wearable Technology for Workplace Health and Safety in Industry 5.0" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_8

- H.C Vu,K.D. Tran*, V.H Tran, K.P. Tran (2024). "Predictive Maintenance Optimization based on Genetic Algorithms for Future Industrial Systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_3

- D.H Nguyen, T.H. Nguyen,K.D. Tran*, K.P. Tran (2024). "Physics-informed Machine Learning for Industrial Reliability and Safety Engineering: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_2

- L.H Nguyen, K.D. Tran*, X. Zeng, K.P. Tran (2024). "Human-Centered Edge Artificial Intelligence for Smart Factory Applications in Industry 5.0: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_5

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System" Book: *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

- A. Saghir, H. Beniwal, K.D. Tran, A. Raza, L. KOEHL, X. Zeng, K.P. Tran (2023). "Explainable Transformer-Based Anomaly Detection for Internet of Things Security" Book: *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 83-109. http://dx.doi.org/10.1007/978-3-031-53028-9_6

- T. Nguyen, K.D. Tran*, A. Raza, Q.T. Nguyen, H.M. Bui, K.P. Tran (2023). "Wearable Technology for Smart Manufacturing in Industry 5.0" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 225-254. http://dx.doi.org/10.1007/978-3-031-30510-8_11

- T.P. Bac, D.T. Ha, K.D. Tran*, K.P. Tran (2023). "Explainable Artificial Intelligence for Cybersecurity in Smart Manufacturing" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 199-223. http://dx.doi.org/10.1007/978-3-031-30510-8_10

- D.T. Ha, T.P. Bac,K.D. Tran*, K.P. Tran (2023). "Efficient and Trustworthy Federated Learning-Based Explainable Anomaly Detection: Challenges, Methods, and Future Directions" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 145-166. http://dx.doi.org/10.1007/978-3-031-30510-8_8

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, D.D.K. Nguyen, K.P. Tran (2022). "Enabling smart supply chain management with artificial intelligence" Book: *Machine Learning and Probabilistic Graphical Models for Decision Support Systems*. CRC Press, pp. 294-310. http://dx.doi.org/10.1201/9781003189886-12

- P.H. Tran, A.A. Nadi, T.H. Nguyen, K.D. Tran, K.P. Tran (2022). "Application of machine learning in statistical process control charts: A survey and perspective" Book: *Control Charts and Machine Learning for Anomaly Detection in Manufacturing*. Springer Cham, pp. 7–42. https://link.springer.com/chapter/10.1007/978-3-030-83819-5_2

- T.T.V. Nguyen, T.H. Nguyen,K.D. Tran, C. Heuchenne, K.P. Tran (2023). "Monitoring the Ratio of Two Normal Variables and Compositional Data: A Literature Review and Perspective." In *Advances of Computational Techniques for Smart Manufacturing in the Industry 5.0: Methods and Applications*, CRC Press. Accepted. https://hal.science/hal-04331557/

Presenting at the Conferences and Refereed Proceedings

- T. Nguyen, Q.T. Nguyen, K.D. Tran*, L. KOEHL, K.P. Tran, (2024), "Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- L.H. Nguyen, Q.T. Nguyen, K.D. Tran*, H.D. Nguyen, S. Thomassey, X.Zeng, K.P. Tran, (2024), "Deep CNN for Remaining Useful Life Prediction: An XAI Approach Using SHAP for Model Interpretation," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran, (2024), "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* .

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024), "Explainable Transformer-based Approach for ECG Anomaly Detection," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* .

- T. Banfalvi, D.H. Nguyen, K.D. Tran, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024), "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T. Banfalvi, K.D. Tran, G. Tartare, P. Bruniaux, K.P. Tran (2024), "Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings: A survey and perspective," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System" proceeding of the *International Conference on Safety* *and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

- A. Saghir, H. Beniwal,K.D. Tran, A. Raza, L. KOEHL, X. Zeng, K.P. Tran (2023). "Explainable Transformer-Based Anomaly Detection for Internet of Things Security" proceeding of the *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 83-109. http://dx.doi.org/10.1007/978-3-031-53028-9_6

- T. Nguyen, K.D. Tran*, A. Raza, Q.T. Nguyen, H.M. Bui, K.P. Tran (2023). "Wearable Technology for Smart Manufacturing in Industry 5.0: Applications, Challenges, and Case Studies" proceeding of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283956_Wearable_Technology_for_Smart_Manufacturing_in_Industry_50_Applications_Challenges_and_Case_Studies

- T.H. Nguyen, H.D. Nguyen,K.D. Tran*, D.D.K. Nguyen, P.H. Tran, K.P. Tran (2023). "Smart Supply Chain Management with Artificial Intelligence: a survey and perspective" proceeding of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283704_Smart_Supply_Chain_Management_with_Artificial_Intelligence_a_survey_and_perspective

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, T.H. Truong, K.H. Phung, L.H. Nguyen, T.T.N. Le, K.P. Tran (2019). "One-Sided Synthetic-RZ control charts: a new method for anomaly detection" proceeding of the *6th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, pp. 262-267. http://dx.doi.org/10.1109/NICS48868.2019.9023851

Invited Talks

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2023) "Wearable Technology for Workplace Safety in Smart Manufacturing" *International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare*, December 21, 2023, Da Nang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023

- K.D. Tran*, T. Nguyen, A. Raza, Q.T. Nguyen, H.M. Bui, and K.P. Tran (2023) "From Blackbox to Explainable Artificial Intelligence for Healthcare 5.0" *International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare*, December 21, 2023, Da Nang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023

- K.D. Tran*, T. Nguyen, A. Raza, Q.T. Nguyen, H.M. Bui, and K.P. Tran (2022) "A novel Transformer-based Anomaly Detection approach for ECG Monitoring Healthcare System: a perspective" *International workshop "E-textiles Internet of Things and Artificial Intelligence with applications in Healthcare"*, December 21, 2022, Ho Chi Minh, Vietnam. https://www.gemtex.fr/2023/06/06/premiere-rencontre-prometteuse/

List of Abbreviations

AE	**Autoencoder**
BC	**Blockchain**
CAM	**Class Activation Maps**
CHF	**Chronic Heart Failure**
CNN	**Convolutional Neural Networks**
DL	**Deep Learning**
DP-SGD	**Differentially Private Stochastic Gradient Descent**
ECG	**Electrocardiograph**
FL	**Federated Learning**
HAR	**Human Activity Recognition**
IID	**Independently and Identically Distributed**
KL	**Kullback-Leibler**
LSTM	**Long Short-Term Memory**
MAE	**Mean Absolute Error**
MIA	**Membership Inference Attacks**
MIT-BIH	**Massachusetts Institute of Technology and Beth Israel Hospital**
ML	**Machine Learning**
MSE	**Mean Squared Error**
OC-SVM	**One-Class Support Vector Machine**
ReLU	**Rectified Linear Unit**
SC	**Smart Contract**
SGD	**Stochastic Gradient Descent**
SHAP	**Shapley Additive Explanations**

SOTA	**State of the Art**
SVDD	**Support Vector Data Description**
VAE	**Variational Autoencoder**
XAI	**Explainable Artificial Intelligence**

Chapter 1

Introduction

1.1 Activity Report

1.1.1 Individual notice

Name: TRAN KIM DUC

Date and place of birth: 01 January 1988 à Hoi An, Vietnam

Current situation: AI Research Engineer at GEMTEX, ENSAIT

Permanent Researcher, Permanent Lecturer (Two-year sabbatical from June 25, 2024)

Professional address: 33 Xo Viet Nghe Tinh, 50000 DA NANG

Research Unit: International Research Institute for Artificial Intelligence and Data Science (IAD)

Establishment : Dong A University

Discipline : Computer science, Automation

Phone: +84914792268

Email: ductk@donga.edu.vn

Web page: https://sites.google.com/view/kimductran

1.1.2 Education Background

- **Master of Business Administration (BAC +6)**.
  - University: Duy Tan University, Da Nang, Vietnam. The university is ranked 495th worldwide in the QS World University Rankings 2025
  - Year: August 2019 - January 2022
- **Bachelor of Business Administration (BAC+4)**
  - University: Duy Tan University, Da Nang, Vietnam. The university is ranked 495th worldwide in the QS World University Rankings 2025
  - Year: September 2013 - December 2015
- **Engineer (BAC + 5) Civil Engineering Hydroelectricity Irrigation**
  - University: University of Science and Technology - The University of Da Nang, Vietnam
  - Year: September 2006 - December 2011

1.1.3 Research and work experiences

- 11/2025- present: Postdoctoral Researcher in GEMTEX, specializing in Data Sciences for the SYMPHONIES Project
- 07/2024-11/2025: Research Engineer in GEMTEX, specializing in Data Sciences for the REVALOTEX Project (01-07-2024). REVALOTEX runs from April'2023 to September 2026
- 2024- present: Permanent Lecturer at the Department of Fundamentals – Dong A University, Da Nang, Vietnam

- 2022- present: Permanent Vice Director at International Research Institute for Artificial Intelligence and Data Science (IAD), Dong A University, Da Nang, Vietnam
- 2018-present: Local Chair at International Chair in Data Science and Explainable Artificial Intelligence, Dong A University, Da Nang, Vietnam
- 2018-present: Permanent Researcher of Artificial Intelligence and Data Science at the International Research Institute for Artificial Intelligence and Data Science (IAD), Dong A University, Da Nang, Vietnam
- 2010 –2018: Co-founder and R&D Director at Kien Phuc Co., Ltd., Automation, Electrical & Mechanical - Technical Supplying technical solutions and executing and upgrading automatic production systems

1.2 Summary of educational activities and student supervision

1.2.1 Teaching Responsibilities

- 2022-2025: Machine Learning with Python (in English), in the international semester at Dong A University

1.2.2 Qualifications and Certificates

- 08/2022: Certificate of Pedagogical Professional Training for University and College Lecturers

1.2.3 Awards

- 2024: Award for Scientific Excellence given by Da Nang City, Vietnam

- 2005: Award for Third prize in Quang Nam Province excellent student contest
- 2004: Award for Third prize in Quang Nam Province excellent student contest

1.2.4 Expertise

- 2018-: Expert and Evaluator for the Research and Innovation program at XAI &DS chair of Dong A University, Vietnam
- 2018-: Expert and Evaluator for the scholarship program of excellent lecturers-researchers at XAI &DS chair of Dong A University, Vietnam

1.2.5 Supervised Master (Engineer) students and co-authored research publications within doctoral theses

- Supervised Master (Engineer) students in the International semester at Dong A University, Vietnam

  1. Bondoni Jeanne, ENSAIT - University of Lille- France
  2. Pendolino Emma Chiara, ENSAIT - University of Lille- France
  3. Viale Lukas TiTouan, ENSAIT - University of Lille- France
  4. DOMINICI TIRANTI Thelma, ENSAIT - University of Lille- France
  5. TRONEL Emma, Elisabeth, ENSAIT - University of Lille- France
  6. CHANTELOT BARCHEMIN Victoire, ENSAIT - University of Lille- France
  7. CHEA Apsara, Tess, ENSAIT - University of Lille- France
  8. DUFFAUT Eugénie, Marie, ENSAIT - University of Lille- France
  9. Elisa CASALS, ENSAIT – University of Lille – France
  10. Lilla SORREL, ENSAIT – University of Lille – France
  11. Alix EMPISSE, ENSAIT – University of Lille – France

12. Clémentine CHANTRY, ENSAIT – University of Lille – France
13. Emma LESCIEUX, ENSAIT – University of Lille – France
14. Jeanne, Anny, Annie FONTIER, ENSAIT – University of Lille – France
15. Louise OGIEZ, ENSAIT – University of Lille – France
16. Capucine, Sylvie COSTES, ENSAIT – University of Lille – France
17. Daphné MANIOULOUX, ENSAIT – University of Lille – France
18. Louis DEBRET, ENSAIT – University of Lille – France
19. Ludmilla BAUVIN, ENSAIT – University of Lille – France
20. Olivia GONZALEZ, ENSAIT – University of Lille – France
21. Binôme JOANA, ENSAIT – University of Lille – France
22. Kim Anh LEMEILLE, ENSAIT – University of Lille – France

- Contribute to doctoral theses through co-authorship of research publications

2022-: Ms.Thi Thuy Van NGUYEN

- Thesis Directors: Kim Phuc TRAN Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France. and Cédric HEUCHENNE, University of liège Belgium.

- Co-supervisor: Guillaume TARTARE (ENSAIT/GEMTEX)

Title: Anomaly Detection in Multivariate IoT Time Series Data with Statistical and Machine Learning Techniques

Publications have resulted from the research conducted in this Ph.D. thesis, in which I was a co-author:

- T.T.V. Nguyen, C. Heuchenne , K.D. Tran, G. Tartare, K.P. Tran. (2024). "Svdd Control Charts Based on Mewma Technique for

Monitoring Compositional Data," Computers & Industrial Engineering, Elsevier,https://doi.org/10.1016/j.cie.2025.110865

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024), "Explainable Transformer-based Approach for ECG Anomaly Detection," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.
- T.T.V. Nguyen, C. Heuchenne , K.D. Tran, G. Tartare, K.P. Tran. (2024). "Svdd Control Charts Based on Mewma Technique for Monitoring Compositional Data," Computers & Industrial Engineering, Elsevier, Revise, http://dx.doi.org/10.2139/ssrn.4828113
- T.T.V. Nguyen, T.H. Nguyen, K.D. Tran, C. Heuchenne, K.P. Tran. (2023). "Monitoring the Ratio of Two Normal Variables and Compositional Data: A Literature Review and Perspective," In Advances of Computational Techniques for Smart Manufacturing in the Industry 5.0: Methods and Applications, CRC Press, accepted, https://hal.science/hal-04331557/ https://doi.org/10.1016/j.ifacol.2022.09.608
- T.T.V. Nguyen, C.Heuchenne, K.D. Tran, , K.P.Tran.(2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System," Book: International Conference on Safety and Security in IoT, Springer Nature Switzerland Publishing, pp 111-129 http://dx.doi.org/10.1007/978-3-031-53028-9_7

2024-: Mr. Le Hoang NGUYEN

- Thesis Director: Kim Phuc TRAN (ENSAIT/GEMTEX,)
- Co-Director: Sébastien THOMASSEY (ENSAIT/GEMTEX)

– Financement: Dong A University International Research Institute for Artificial Intelligence and Data Science a scholarship program for excellent lecturersresearchers at XAI &DS chair

Title: Embedded Artificial Intelligence for Smart Factory Applications in Industry 5.0

Publications have resulted from the research conducted in this Ph.D. thesis, in which I was a co-author:

– L.H Nguyen, K.D. Tran*, X. Zeng, K.P. Tran (2024). "Human-Centered Edge Artificial Intelligence for Smart Factory Applications in Industry 5.0: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, accepted (book chapter).

– L.H. Nguyen, Q.T. Nguyen, K.D. Tran, X. Zeng, K.P. Tran (2024), "Explainable for Remaining Useful Life Prediction", in "International Conference on Responsible Artificial Intelligence and Data Science," DaNang, Vietnam (presentation).

2020-2023: Mr. Ali RAZA (PhD thesis in co-supervision with the University of Kent)

– The thesis was defended on 28/08/2023 (Thesis started on 01/10/2020).

– Thesis Directors: Ludovic KOEHL (ENSAIT/GEMTEX), Shujun Li (University of Kent, UK).

– Co-supervisor: Kim-Phuc TRAN (ENSAIT/GEMTEX).

- Funding: I-SITE ULNE

Title: Secure and Privacy-preserving Federated Learning with Explainable Artificial Intelligence for Smart Healthcare System

Publications have resulted from the research conducted in this Ph.D. thesis, in which I was a co-author::

- A. Raza, S. Li, K.P. Tran, L. Koehl, K.D. Tran* (2024). "Using Anomaly Detection to Detect Poisoning Attacks in Federated Learning Applications" *Knowledge-Based Systems*. Elsevier. Revise.

- A. Raza, K.P. Tran, L. Koehl, X. Zeng, K. Benzaidi, S. Li, S. Hotham, K.D. Tran*(2024). "Lightweight Transformer in Federated Setting for Human Activity Recognition in Home Care" *Pattern Recognition*. Elsevier. Submitted.

2023-: Ms.Timea BANFALVI

- Thesis Directors: Pascal BRUNIAUX (ENSAIT/GEMTEX) & Kim Phuc TRAN (ENSAIT/GEMTEX)
- Co-supervisor: Guillaume TARTARE (ENSAIT/GEMTEX)
- Funding: Project Symphonies - National PSPC Program

Title: Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings

Publications have resulted from the research conducted in this Ph.D. thesis, in which I was a co-author:

- T. Banfalvi, D.H. Nguyen, K.D. Tran, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024), "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* (Accepted).
- T. Banfalvi, K.D. Tran, G. Tartare, P. Bruniaux, K.P. Tran (2024), "Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings: A survey and perspective," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* (Accepted).

2024-: Ms.Minh Anh LUONG

- Thesis Director: Kim Phuc TRAN (ENSAIT/GEMTEX)
- Co-Director: Sébastien THOMASSEY (ENSAIT/GEMTEX)
- Financement: Dong A University International Research Institute for Artificial Intelligence and Data Science a scholarship program for excellent lecturersresearchers at XAI &DS chair

  Title: Intelligent Decision Support Systems for Supply Chain Management: Store Replenishment in Fashion Retailing

  Publication has resulted from the research conducted in this Ph.D. thesis, in which I was a co-author:

– D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran, (2024), "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* (Accepted).

2024-: Mr.Viet Hieu TRAN

– Thesis Director: Kim Phuc TRAN (ENSAIT/GEMTEX)

– Co-Director: Sébastien THOMASSEY (ENSAIT/GEMTEX)

– Financement: Dong A University International Research Institute for Artificial Intelligence and Data Science a scholarship program for excellent lecturersresearchers at XAI &DS chair
Title: Explainable Anomaly Detection in Smart Manufacturing through Deep Reinforcement Learning and Lightweight Federated Learning
Publication has resulted from the research conducted in this Ph.D. thesis, in which I was a co-author:

– H.C Vu,K.D. Tran*, V.H Tran, K.P. Tran (2024). "Predictive Maintenance Optimization based on Genetic Algorithms for Future Industrial Systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_3

- External examiner for master's project defense
1.2023: Pendolino Emma Chiara, Bondoni Jeanne , Viale Lukas TiTouan "How ChatGPT can be used for fashion",2023

1.3 Diffusion and influence

1.3.1 Member of Selection Committees (COS) for lecturer functions

- 1. Member of Selection Committees for the Electrical and Electronic Engineering faculty lecturer position - Dong A University in 2024 (selected candidate,**Du Dat Lam, MSc.**)
- 2. Member of Selection Committees for the Electrical and Electronic Engineering faculty lecturer position - Dong A University in 2023 (selected candidate,**Viet Vu Do, MSc.**)
- 3. Member of Selection Committees for the Electrical and Electronic Engineering faculty lecturer position - Dong A University in 2023 (selected candidate,**Hoang Gia Ngo, Ph.D.**)

1.3.2 Participation in networks, learned societies, scientific programming communities

- Prof. Philippe CASTAGLIOLA, Université de Nantes and LS2N UMR CNRS 6004, France.
- Prof. Bruno AGARDA, Ecole Polytechnique de Montreal, Canada.
- Prof. Fadel MEGAHED, Miami University (OH), USA.
- Prof. Giovanni CELANO, Università di Catania, Catania, Italy.
- Prof. Wei Lin TEOH, School of Mathematical and Computer Sciences, Heriot-Watt University, Malaysia.
- Prof. Athanasios RAKITZIS, University of Aegean, Karlovasi, Samos, Greece.

- Prof. Cédric Heuchenne, HEC Management School, University of Liège, Liège 4000, Belgium.
- Prof. Xianyi ZENG, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.
- Prof. Ludovic KOEHL, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.
- Prof. Kim Phuc TRAN, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.
- Dr. Huu Du NGUYEN, Hanoi University of Science and Technology, Vietnam.
- Dr. Ali RAZA, Research scientist at Honda Research Institute Europe, Germany.
- Prof. Pascal BRUNIAUX, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.
- Prof. Xianyi ZENG, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.
- Prof. Hongmei HE, University of Salford, United Kingdom.
- Prof. Abdessamad KOBI, University of Anger, France.
- Prof. Arne JOHANNSSEN, University of Hamburg, Germany.
- Prof. Ramla SADDEM, EiSINE School of Industrial and Digital Sciences Engineering, University of Reims Champagne-Ardenne (URCA) in France.
- Prof. Guillaume TARTARE, Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France.

- Prof. Khanh NGUYEN, Tarbes (ENIT), INP Toulouse, France.
- Prof. Rehmat Ullah KHAN, School of Technologies, Cardiff Metropolitan University, UK.
- Prof. Robab AFSHARI, University of Zanjan, Iran.
- Prof. Asma AMDOUNI, Tunis University, Tunisia.
- Prof. Zhenglei HE, South China University of Technology, China.

1.3.3 Invited Seminar

- T. T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran, (2023), "Wearable Technology for Workplace Safety in Smart Manufacturing", International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare, December 21, 2023, Danang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023
- K.D. Tran, T. Nguyen, A. Raza, Q.T. Nguyen, H.M. Bui and, K.P. Tran (2023), "From Blackbox to Explainable Artificial Intelligence for Healthcare 5.0", International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare, December 21, 2023, Danang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023
- K.D. Tran, T. Nguyen, A.Raza, Q.T. Nguyen, H.M. Bui and, K.P. Tran (2022), "A novel Transformer-based Anomaly Detection approach for ECG Monitoring Healthcare System: a perspective", International workshop "E-textiles, Internet of Things, and Artificial Intelligence with applications in Healthcare", December 21, 2022, Ho Chi Minh, Vietnam. https://www.gemtex.fr/2023/06/06/premiere-rencontre-prometteuse/

1.3.4 Speaker at international conferences

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran.(2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System," proceeding of the International Conference on Safety and Security in IoT, Springer Nature Switzerland Publishing, pp 111-129,
http://dx.doi.org/10.1007/978-3-031-53028-9_7

- A. Saghir, H. Beniwal, K.D. Tran, A. Raza, L. KOEHL, X. Zeng, K.P. Tran.(2023). "Explainable Transformer-Based Anomaly Detection for Internet of Things Security," proceedings of the International Conference on Safety and Security in IoT, Springer Nature Switzerland Publishing, pp83-109,
http://dx.doi.org/10.1007/978-3-031-53028-9_6

- T. Nguyen, K.D.Tran, A.Raza, Q.T. Nguyen, H.M.Bui, K.P.Tran.(2023). "Wearable Technology for Smart Manufacturing in Industry 5.0 Applications, Challenges, and Case Studies " proceeding of the Conference: ISSAT International Conference on Data Science in Business, Finance and Industry (DSBFI 2023)At: Danang, Vietnam,
https://www.researchgate.net/publication/368283956_Wearable_Technology_for_Sma

- T.H.Nguyen, H.D.Nguyen, K.D.Tran, D.D.K.Nguyen, P.H.Tran, K.P.Tran.(2023). "Smart Supply Chain Management with Artificial Intelligence: a survey and Perspective" proceeding of the Conference: ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)At: Danang, Vietnam,
https://www.researchgate.net/publication/368283704_Smart_Supply_Chain_Manage

- T.H. Nguyen, H.D.Nguyen, K.D.Tran, T.H.Truong, K.H.Phung, L.H.Nguyen, T.T.N. Le, K.P.Tran.(2019). "One-Sided Synthetic-RZ control charts: a new method for anomaly detection ", Proceedings of the 6th NAFOSTED Conference on Information and Computer Science (NICS).IEEE, pp. 262-267.
  http://dx.doi.org/10.1109/NICS48868.2019.9023851

1.3.5 Peer-reviewed articles

Journal	**2023**	**2024**	**2025**	**Total**
Chemometrics and Intelligent Laboratory Systems	0	1	0	1
Engineering Applications of Artificial Intelligence	9	17	11	37
European Journal of Operational Research	0	1	0	1
Information Processing and Management	0	1	0	1
Information Sciences	1	0	0	1
IEEE Transactions on Intelligent Transportation Systems	5	13	6	24
International Journal of Production Research	0	1	0	1
Journal of Mathematics in Industry	0	0	1	1
Measurement	0	1	0	1
Next Sustainability	0	0	1	1
Quality Technology & Quantitative Management	0	1	0	1
Reliability Engineering & Systems Safety	0	0	1	1
Results in Engineering	0	3	2	5
Sustainable Futures	0	1	0	1
Total				**77**

Conference	2019	2023	2024	2025	Total
EAI RAIDS			14		14
EAI SaSeIoT		5	5		10
International Society of Science and Applied Technologies (ISSAT)- The Data Science in Business, Finance and Industry (DSBFI)	4	5		5	14
Total					38

1.4 Scientific responsibilities

1.4.1 Member of the scientific committee of international/national conferences

- Local Chair of the International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare, December 21, 2023, Da Nang, Vietnam (https://iad.donga.edu.vn/International-Workshop-2023)
- Technical program of the EAI SaSeIoT 2023 - 7th EAI International Conference on Safety and Security in the Internet of Things, October 24-26, 2023, Bratislava, Slovakia (https://securityiot.eai-conferences.org/2023/technical-program-committee/)
- Local Arrangement Chair of the Explainable Artificial Intelligence for Industry 5.0, September 5-6, 2023, Da Nang, Vietnam (https://iad.donga.edu.vn/International-Conference-2023)
- Member of the Organizing Committee of the ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023) (https://www.issatconferences.org/dsbfi2023.html)
- Member of the Organizing Committee of the EAI SaSeIoT 2023 - 7th EAI International Conference on Safety and Security in the Internet of

Things, October 24-26, 2023, Bratislava, Slovakia (https://securityiot.eai-conferences.org/2023/full-program/)

- Sponsorship Chair of the EAI Smart Life Summit 2024: The AI Era, October 22-24, 2024, Da Nang, Vietnam (https://smartlife.eai-summits.org/2024/summit_organizing_committees/)
- Member of the Organizing Committee of the ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2025) (https://www.issatconferences.org/dsbfi2025.html)
- Technical program of the International Congress on Advanced Technologies ICAT'2025, November 19-21, 2025, Marrakech, Morocco (https://www.icat2025.net/#committee)
- Sponsorship Chair of the 2nd EAI International Conference on Responsible Artificial Intelligence and Data Science, 10 - 12 March 2026, Da Nang, Vietnam (https://raids.eai-conferences.org/2026/organizing-committee/)

1.4.2 Academic responsabilities

- 2018-: Local chair of the International Chair in Data Science and Explainable Artificial Intelligence at Dong A University & International Research Institute for Artificial Intelligence and Data Science (IAD), Vietnam, https://iad.donga.edu.vn/International-Chair-in-DS-and-XAI
- 2018-: Coordinator for projects of the International semester at Dong A University, Vietnam
- 2020-: Judge for the final round of the student scientific research competition, Dong A University, Da Nang, Vietnam
- 2021-: Deputy Head for the Engineering program in AI for the Faculty of Electrical and Electronics Engineering, Dong A University, Vietnam

- 2022-: Deputy Head for the program of improving advanced mathematics, probability, statistics, applied mathematics, Python programming, and algorithms, Dong A University, Vietnam

1.5 Expertise activities

- **Below is the list of selected ongoing projects that I am a Principal Investigator (PI) or co-PI**

  1. XAIDS_IChair(2018-2028): International Chair in Data Science and Explainable Artificial Intelligence, funding for the development of the International Research Institute for Artificial Intelligence and Data Science (IAD) at Dong A University, Vietnam (co-PI, TOTAL COST: 300 K EUR).

  2. IAD-4(2022-2024): " A new framework for prognostics in decentralized industries: Enhancing fairness, security, and transparency through Blockchain and Federated Learning," funded by International Research Institute for Artificial Intelligence and Data Science (IAD) at Dong A University, Vietnam (PI, TOTAL COST: 5 K EUR).

  3. IAD-3(2023-2024): "Predictive Maintenance Optimization based on Genetic Algorithms for Future Industrial Systems," funded by the International Research Institute for Artificial Intelligence and Data Science (IAD) at Dong A University, Vietnam (PI, TOTAL COST: 5 K EUR).

- **Below is the ongoing project that I am a member of**

  1. REVALOTEX (2023-2026): "Focuses on transforming the textile industry according to circular economy principles, emphasizing creating multiple values and extending the lifespan of textile products."

  PI: Ludovic KOEHL

  Members: Pr. Maud HERBERT, Dr. Isabelle ROBERT, Dr. Romain

BENKIRANE, Noémie PICHON, and Kim Duc TRAN.

Pr. Ludovic KOEHL coordinates this project from the GEMTEX laboratory (Univ. Lille, ENSAIT, ULR 2461 - GEMTEX - Génie et Matériaux Textiles, F-59000 Lille, France). (TOTAL COST: €342,384.42).

1.6 List of scientific production

Review of Scientific Production		
	Accept	Submit
Chapters in scientific volumes	19	5
Articles in Peer-reviewed Journals (Indexed in the Web of Science)	7	3
Peer-reviewed communications with proceedings at an international conference	5	6
Oral communications with peer review without proceedings at an international or national conference	9	

(*JCR refers to the Journal Citation Reports)

*Source (last accessed on 24/11/2025): https://mjl.clarivate.com/home

Note regarding the list of publications:

The co-authors of the publications are:

Co-authored in the research projects of PhD students (L.H. Nguyen, T.T.V. Nguyen, A. Raza, T. Banfalvi, M.A. Luong, L.H. Le, V.H. Tran, N.A. Luong).

Permanent members of the International Chair in Data Science and Explainable Artificial Intelligence - Da Nang, Vietnam (Prof K.P Tran, Prof. X. Zeng, Prof. L. Köehl, and Dr. G. Tartare) or from external laboratories (Prof. P. Castagliola, Prof. C. Heuchenne, Prof. G. Celano, . . .).

Young researchers or engineers from Vietnamese universities where I have conducted research: (T.H. Do, T.H. Nguyen, P.H. Tran, T.Q.D. Pham, P.B. Ta . . .).

My name is underlined.

*: corresponding author

Peer-reviewed Journals (Indexed in the Web of Science)

- T. Banfalvi, D.H. Nguyen, K.D. Tran*, G. Tartare, P. Bruniaux, K.P. Tran (2025). "Mesh Deep Support Vector Data Description: Unsupervised Anomaly Detection in 3D Human Leg Morphologies for Adaptive Compression Stocking Design," *Intelligent Systems with Applications*. Elsevier. Under Review.

- T.T.V. Nguyen, C. Heuchenne , K.D. Tran, G. Tartare, K.P. Tran. (2024). "SVDD Control Charts Based on Mewma Technique for Monitoring Compositional Data," Computers & Industrial Engineering, Elsevier,https://doi.org/10.1016/j.cie.2025.110865

- A. Raza, S. Li, K.P. Tran, L. KOEHL, K.D. Tran* (2024). "Using Anomaly Detection to Detect Poisoning Attacks in Federated Learning Applications" *Knowledge-Based Systems*. Elsevier. Under Review.

- A. Raza, K.P. Tran, L. Köehl, X. Zeng, K. Benzaidi, S. Li, S. Hotham, K.D. Tran*(2024). "Lightweight Transformer in Federated Setting for Human Activity Recognition in Home Care" *Pattern Recognition*. Elsevier. Under Review http://dx.doi.org/10.2139/ssrn.5021631

- H.D. Nguyen, A.A. Nadi, K.D. Tran*, P. Castagliola, G. Celano, K.P. Tran (2023). "The Shewhart-type RZ control chart for monitoring the ratio of autocorrelated variables" *International Journal of Production Research*. Taylor & Francis, pp. 6746-6771. http://dx.doi.org/10.1080/00207543.2022.2137594

- A.A. Nadi, B.S. Gildeh, J. Kazempoor, K.D. Tran, K.P. Tran (2023). "Cost-effective optimization strategies and sampling plan for Weibull quantiles under type-II censoring" *Applied Mathematical Modelling*. Elsevier, pp. 16–31. http://dx.doi.org/10.1016/j.apm.2022.11.004

- K.D. Tran, A.A. Nadi, T.H. Nguyen, K.P. Tran (2021). "One-sided Shewhart control charts for monitoring the ratio of two normal variables in short production runs" *Journal of Manufacturing Processes*. Elsevier, vol. 69, pp. 273–289. http://dx.doi.org/10.1016/j.jmapro.2021.07.031

- H.D. Nguyen, K.P. Tran, K.D. Tran(2021). "The effect of measurement errors on the performance of the Exponentially Weighted Moving Average control charts for the Ratio of Two Normally Distributed Variables" *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2020.11.042

- Q.T. Nguyen, V. Giner-Bosch, K.D. Tran, C. Heuchenne, K.P. Tran (2021). "One-sided variable sampling interval EWMA control charts for monitoring the multivariate coefficient of variation in the presence of measurement errors" *The International Journal of Advanced Manufacturing Technology*. Springer London, vol. 115, pp. 1821-1851. https://link.springer.com/article/10.1007/s00170-021-07138-8

- K.D. Tran, H.D. Nguyen, T.H. Nguyen, K.P. Tran (2021). "Design of a variable sampling interval exponentially weighted moving average median control chart in the presence of measurement errors" *Quality and Reliability Engineering International*, vol. 37, pp. 374-390. http://dx.doi.org/10.1002/qre.2726

Chapters in Books

- T. Nguyen, Q.T. Nguyen, K.D. Tran*, L. Koehl, K.P. Tran (2025)."Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data." Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- L.H. Nguyen, Q.T. Nguyen, K.D. Tran*, H.D. Nguyen, S. Thomassey, X. Zeng, K.P. Tran (2025). "Deep CNN for Remaining Useful Life Prediction: An XAI Approach Using SHAP for Model Interpretation" Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran (2024). "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study" Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024). "Explainable Transformer-based Approach for ECG Anomaly Detection" Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- T. Banfalvi, D.H. Nguyen, K.D. Tran*, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024). "Deep Convolutional K-Means of 3D Morphologies of Human Legs for the Implementation of Adaptive Leg Morphotypes and Medical Compression Stockings" Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- T. Banfalvi, K.D. Tran*, G. Tartare, P. Bruniaux, K.P. Tran (2024). "Unsupervised Classification of 3D Morphologies of Human Legs for the

Implementation of Adaptive Leg Morphotypes and Medical Compression Stockings: A Survey and Perspective" Book: *Responsible Artificial Intelligence and Data Science*, Springer Nature Switzerland AG. https://link.springer.com/book/9783032140548.

- D.H. Nguyen, D.P.T. Nguyen, Q.C. Ta, S. Thomassey, K.D. Tran* (2025). "Natural Language Processing Applications in Smart Manufacturing: A Survey and Perspective" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- T.H. Nguyen, J.M. Masereel, D.H. Nguyen, K.D. Tran*, K.P. Tran (2025). "Explainable Anomaly Detection with AI and Statistical Methods for Predictive Maintenance in Smart Manufacturing Systems: A Survey and Perspective" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- D.H. Nguyen, D.P.T. Nguyen, Q.C. Ta, S. Thomassey, K.D. Tran*, K.P. Tran (2025). "Human-Centered Explainable Anomaly Detection in Smart Manufacturing: Bridging AI and Human Decision-Making" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- V.H. Tran, D.H. Nguyen, K.D. Tran*, S. Thomassey, K.P. Tran (2025). "Anomaly and Novelty Detection in Non-Stationary Time Series: Deep, Hybrid, and Federated Perspectives" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- T.Q.D. Pham, K.D. Tran*, K.T.P. Nguyen, X.V. Tran,L. KOEHL, and K.P. Tran (2024). "A new framework for prognostics in decentralized industries: Enhancing fairness, security, and transparency through Blockchain and Federated Learning" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- T.H. Nguyen, A. Saghir, K.D. Tran*,D.H. Nguyen,N.A. Luong, K.P. Tran (2024). "Safety and Reliability of Artificial Intelligence systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_9

- T. Nguyen, D.H. Nguyen, Q.T. Nguyen, K.D. Tran*, K.P. Tran (2024). "Human-Centered Edge AI and Wearable Technology for Workplace Health and Safety in Industry 5.0" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_8

- H.C Vu,K.D. Tran*, V.H Tran, K.P. Tran (2024). "Predictive Maintenance Optimization based on Genetic Algorithms for Future Industrial Systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_3

- D.H Nguyen, T.H. Nguyen,K.D. Tran*, K.P. Tran (2024). "Physics-informed Machine Learning for Industrial Reliability and Safety Engineering: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_2

- L.H Nguyen, K.D. Tran*, X. Zeng, K.P. Tran (2024). "Human-Centered Edge Artificial Intelligence for Smart Factory Applications in Industry 5.0: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_5

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System" Book: *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

- A. Saghir, H. Beniwal, K.D. Tran, A. Raza, L. KOEHL, X. Zeng, K.P. Tran (2023). "Explainable Transformer-Based Anomaly Detection for Internet of Things Security" Book: *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 83-109. http://dx.doi.org/10.1007/978-3-031-53028-9_6

- T. Nguyen, K.D. Tran*, A. Raza, Q.T. Nguyen, H.M. Bui, K.P. Tran (2023). "Wearable Technology for Smart Manufacturing in Industry 5.0" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 225-254. http://dx.doi.org/10.1007/978-3-031-30510-8_11

- T.P. Bac, D.T. Ha, K.D. Tran*, K.P. Tran (2023). "Explainable Artificial Intelligence for Cybersecurity in Smart Manufacturing" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 199-223. http://dx.doi.org/10.1007/978-3-031-30510-8_10

- D.T. Ha, T.P. Bac,K.D. Tran*, K.P. Tran (2023). "Efficient and Trustworthy Federated Learning-Based Explainable Anomaly Detection: Challenges, Methods, and Future Directions" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 145-166. http://dx.doi.org/10.1007/978-3-031-30510-8_8

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, D.D.K. Nguyen, K.P. Tran (2022). "Enabling smart supply chain management with artificial intelligence" Book: *Machine Learning and Probabilistic Graphical Models for Decision Support Systems*. CRC Press, pp. 294-310. http://dx.doi.org/10.1201/9781003189886-12

- P.H. Tran, A.A. Nadi, T.H. Nguyen, K.D. Tran, K.P. Tran (2022). "Application of machine learning in statistical process control charts: A survey and perspective" Book: *Control Charts and Machine Learning for Anomaly Detection in Manufacturing*. Springer Cham, pp. 7–42. https://link.springer.com/chapter/10.1007/978-3-030-83819-5_2

- T.T.V. Nguyen, T.H. Nguyen,K.D. Tran, C. Heuchenne, K.P. Tran (2023). "Monitoring the Ratio of Two Normal Variables and Compositional Data: A Literature Review and Perspective." In *Advances of Computational Techniques for Smart Manufacturing in the Industry 5.0: Methods and Applications*, CRC Press. Accepted. https://hal.science/hal-04331557/

Presenting at the Conferences and Refereed Proceedings

- T. Nguyen, Q.T. Nguyen, K.D. Tran*, L. KOEHL, K.P. Tran, (2024), "Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- L.H. Nguyen, Q.T. Nguyen, K.D. Tran*, H.D. Nguyen, S. Thomassey, X.Zeng, K.P. Tran, (2024), "Deep CNN for Remaining Useful Life Prediction: An XAI Approach Using SHAP for Model Interpretation," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran, (2024), "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* .

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024), "Explainable Transformer-based Approach for ECG Anomaly Detection," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* .

- T. Banfalvi, D.H. Nguyen, K.D. Tran, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024), "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T. Banfalvi, K.D. Tran, G. Tartare, P. Bruniaux, K.P. Tran (2024), "Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings: A survey and perspective," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System", Proceedings of the *International Conference on Safety* *and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

- A. Saghir, H. Beniwal,K.D. Tran, A. Raza, L. KOEHL, X. Zeng, K.P. Tran (2023). "Explainable Transformer-Based Anomaly Detection for Internet of Things Security", Proceedings of the *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 83-109. http://dx.doi.org/10.1007/978-3-031-53028-9_6

- T. Nguyen, K.D. Tran*, A. Raza, Q.T. Nguyen, H.M. Bui, K.P. Tran (2023). "Wearable Technology for Smart Manufacturing in Industry 5.0: Applications, Challenges, and Case Studies" proceeding of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283956_Wearable_Technology_for_Smart_Manufacturing_in_Industry_50_Applications_Challenges_and_Case_Studies

- T.H. Nguyen, H.D. Nguyen,K.D. Tran*, D.D.K. Nguyen, P.H. Tran, K.P. Tran (2023). "Smart Supply Chain Management with Artificial Intelligence: a survey and perspective" proceeding of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283704_Smart_Supply_Chain_Management_with_Artificial_Intelligence_a_survey_and_perspective

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, T.H. Truong, K.H. Phung, L.H. Nguyen, T.T.N. Le, K.P. Tran (2019). "One-Sided Synthetic-RZ control charts: a new method for anomaly detection", Proceedings of the *6th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, pp. 262-267. http://dx.doi.org/10.1109/NICS48868.2019.9023851

Invited Talks

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2023) "Wearable Technology for Workplace Safety in Smart Manufacturing" *International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare*, December 21, 2023, Da Nang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023
- K.D. Tran*, T. Nguyen, A. Raza, Q.T. Nguyen, H.M. Bui, and K.P. Tran (2023) "From Blackbox to Explainable Artificial Intelligence for Healthcare 5.0" *International Workshop on Responsible Artificial Intelligence and Applications in Integrated Circuit Industry, Manufacturing, and Healthcare*, December 21, 2023, Da Nang, Vietnam. https://iad.donga.edu.vn/International-Conference-2023
- K.D. Tran*, T. Nguyen, A. Raza, Q.T. Nguyen, H.M. Bui, and K.P. Tran (2022) "A novel Transformer-based Anomaly Detection approach for ECG Monitoring Healthcare System: a perspective" *International workshop "E-textiles Internet of Things and Artificial Intelligence with applications in Healthcare"*, December 21, 2022, Ho Chi Minh, Vietnam. https://www.gemtex.fr/2023/06/06/premiere-rencontre-prometteuse/

1.7 Research subject

My research focuses on developing an integrated framework combining advanced statistical computing with modern machine learning techniques to enhance monitoring, anomaly detection, and classification in smart manufacturing and smart healthcare. The aim is to address the limitations of traditional methods and overcome the challenges of scalability, real-time processing, privacy, and interpretability that currently hinder the effectiveness of anomaly detection systems. We explore new approaches in smart manufacturing that leverage machine learning to process high-dimensional, nonlinear data for real-time fault detection and predictive maintenance. In healthcare, we investigate the application of federated learning to protect privacy while enabling effective anomaly detection across distributed data sources alongside the development of explainable AI techniques to ensure transparency and trust in clinical decision-making. By bridging the gap between statistical models and machine learning, this research will create a unified framework that optimizes performance in monitoring systems, improves early fault detection, and enables timely interventions in both complex industrial and healthcare environments.

Chapter 2

Background and Literature Review

In this chapter, we provide background and a literature review. In particular, we provide preliminary reviews of current work to identify its limitations.

2.1 Introduction

Monitoring, detecting anomalies, and classifying data in critical domains, such as smart manufacturing and healthcare, are essential for ensuring system reliability, efficiency, and accurate decision-making. Artificial Intelligence and Statistical Methods for Monitoring, Anomaly Detection, Classification, and their Applications in Smart Manufacturing and Healthcare, as well as Industrial AI for Health and Wellbeing and Smart Healthcare, play a crucial role in these areas. Statistical Computing and Industrial Statistics provide fundamental methodologies for these tasks, enhancing process monitoring, anomaly detection, and classification through rigorous data analysis and control techniques. Monitoring involves continuously observing processes to identify deviations from expected behavior, while anomaly detection plays a crucial role in recognizing unexpected patterns that may indicate potential failures or risks. Classification further enhances these processes by organizing data into meaningful categories, enabling predictive analytics and optimized interventions. Integrating machine learning (ML), a branch of Artificial Intelligence (AI), and statistical techniques has significantly improved the effectiveness of these tasks, enhancing both accuracy and efficiency in complex, data-driven environments. In smart manufacturing, ML algorithms facilitate predictive maintenance by analyzing sensor data to forecast equipment failures, thereby reducing downtime and maintenance costs [36, 88]. Traditional maintenance approaches, such as reactive and scheduled maintenance, often lead to inefficiencies, whereas predictive maintenance powered by ML leverages real-time data to anticipate malfunctions before they occur, optimizing production processes and increasing operational longevity [110]. Additionally, defect detection has been transformed through AI-driven computer vision systems, particularly convolutional neural networks (CNNs), which enable real-time identification of product defects, ensuring high-quality manufacturing standards while minimizing waste. The combination of ML with statistical process control (SPC), such as Shewhart and EWMA control charts, provides a robust framework for detecting variations in production quality and maintaining process stability [141, 237].

ML has demonstrated exceptional capabilities in disease diagnosis and patient monitoring in healthcare, revolutionizing medical decision-making. Deep learning models, especially CNNs, have surpassed traditional diagnostic methods in analyzing medical images, enabling precise detection of conditions such as cancer, pneumonia, and diabetic retinopathy [176, 265]. Beyond imaging, ML-based anomaly detection plays a critical role in real-time patient monitoring through wearable medical devices, identifying irregularities in physiological data such as heart rate, blood pressure, and glucose levels [251]. These AI-driven monitoring systems empower clinicians with timely insights, facilitating early intervention and personalized treatment plans. Integrating federated learning (FL) further enhances healthcare analytics by enabling collaborative model training across multiple institutions without compromising patient privacy, addressing key challenges in medical data security and regulatory compliance [138]. Despite the advancements brought by ML, the need for model interpretability remains a significant challenge, particularly in high-stakes domains such as manufacturing automation and clinical decision-making. Explainable AI (XAI) techniques, including SHAP values and LIME, provide transparency into ML-driven decisions, ensuring that stakeholders understand the reasoning behind predictive outcomes [77]. In smart manufacturing, XAI facilitates root-cause analysis in predictive maintenance and defect detection, enabling engineers to make informed corrective actions. Similarly, in healthcare, interpretable AI models enhance trust and reliability, ensuring that AI-generated diagnoses align with clinical knowledge and best practices. Statistical methodologies complement ML by providing robust frameworks for uncertainty quantification, hypothesis testing, and reliability analysis, further strengthening decision confidence in industrial and medical applications [141].

In vital sectors such as smart manufacturing and healthcare, the combination of statistical methods and machine learning (ML) has led to revolutionary breakthroughs in monitoring, anomaly detection, and classification. Organizations can maximize operational efficiency, ensure superior quality control, and enhance system resilience by leveraging AI-driven tools such as predictive maintenance, defect detection, disease diagnosis, and patient monitoring. Due to these advancements, intelligent, self-governing systems can be developed that quickly detect and resolve problems before they escalate, thereby improving overall system performance and minimizing operational disruptions. Explainable AI (XAI) and robust statistical approaches are becoming increasingly important as the need for transparency and confidence in AI technologies grows. By ensuring that AI systems remain dependable, interpretable, and used ethically, these tools will promote broader adoption and enhance their efficacy in the real world. AI is a key driving force behind technological advancements that benefit society by enhancing economic productivity and improving the quality of life. As it continues to develop in these domains, it promises to improve healthcare outcomes, in addition to optimizing industrial processes [88]. With an emphasis on their applications in monitoring, anomaly detection, and classification, this thesis examines the intersection between machine learning and statistical methods. It aims to help create intelligent systems that will shape the future of these crucial fields by enhancing operational effectiveness and system resilience, while also ensuring the ethical application and transparency of AI-driven technologies. A review of blockchain technology and its applications in predicting the Remaining Useful Life (RUL), an examination of industrial artificial intelligence, statistical computing, and industrial statistics in advanced SPM (Statistical Process Monitoring), and a discussion of monitoring, anomaly detection, and classification techniques and their uses in smart manufacturing and healthcare are all covered in the sections that follow.

2.2 Statistical Computing and Industrial Statistics in advanced SPM

Statistical Computing and Industrial Statistics are essential in advanced Statistical Process Monitoring (SPM), enabling real-time anomaly detection, process optimization, and predictive maintenance in smart manufacturing [212]. Statistical computing leverages optimization algorithms to analyze high-dimensional industrial data efficiently and enhance predictive capabilities. Industrial statistics, through Multivariate Statistical Process Control (MSPC), time-series analysis, and hypothesis testing, ensure robust process control and early fault detection. By combining these approaches with Bayesian inference and uncertainty quantification, advanced SPM enhances decision-making, reduces downtime, and improves manufacturing efficiency.

Additionally, several statistical distributions play a crucial role in the modeling process, such as the Normal distribution for Gaussian processes, the Weibull distribution for failure time analysis, the Gamma distribution for reliability modeling, and the Poisson distribution for detecting rare events. Control charts, including Shewhart charts, CUSUM (Cumulative Sum) charts, and EWMA (Exponentially Weighted Moving Average) charts, are widely used to monitor process stability, detect shifts, and minimize defects in manufacturing operations [170]. However, their applications to compositional data (CoDa), which represent strictly positive vectors of relative proportions of components (e.g., mineral compositions in a rock or product ingredients), have been relatively limited in the literature. As a special case, in many industrial manufacturing processes, the quality of products can depend on the relative amount between two quality characteristics X and Y. Often, this requires the online monitoring of the ratio X/Y as a quality characteristic itself using a control chart. It has been demonstrated in the SPC literature that the ratio of two normal variables is a major concern in several studies. The motivation for these studies stems from the fact that this ratio is a crucial characteristic for ensuring the quality of products in many processes. For example, in the food industry, keeping the relative weights of two main ingredients could be a requirement to ensure the quality of a food recipe. In the pharmaceutical industry, the safety and effectiveness of drugs could be guaranteed by stabilizing the proportion of two active ingredients. An overview of typical situations that require monitoring the ratio of two quantities has been discussed in [33]. Regarding the methods for monitoring the ratio of two normal variables, several control charts have been proposed, as detailed in [34], [33], and [210].

In a general case, although CoDa applications arise in various domains such as chemical research, econometric and survey data analyses, and the food industry ([6]), its special structure makes the traditional control charts, which are designed for continuous data, cannot adequately address it. To overcome this, the literature has seen the development of specialized control charts for monitoring CoDa. An early contribution by [23] proposed a chi-square control chart for monitoring CoDa based on the Dirichlet distribution. [75] conducted a study examining the relationship between response and predictor variables using a Dirichlet regression and evaluated the method's performance by plotting five different T^2 control charts. Building on this, [226, 225, 224] investigated T^2 control charts for monitoring CoDa with $p = 3$, for the individual observations case and an out-of-control signal interpretation in case $p > 3$, respectively. In [207], the authors introduced the MEWMA-CoDa control chart to monitor CoDa with arbitrary components, showing its effectiveness in identifying small to moderate shifts in processes, surpassing its competitor's performance (T^2-CoDa chart), and motivating further enhancements with variable sampling interval and variable sample size adaptive strategies ([154, 96, 95]). Proposed a CUSUM-CoDa chart that outperforms T^2-CoDa and is comparable to the MEWMA-CoDa chart. Influence of measurement errors on the performances of T^2-CoDa, MEWMA-CoDa, MCUSUM-CoDa, and VSI T^2-CoDa were also investigated by [255, 254, 92, 93], respectively. Addressing the challenge in industrial processes, [253] proposed an enhanced residuals T^2 control chart using a time series autoregressive moving average model for autocorrelated CoDa, while [94] developed a principal component analysis-based T^2-CoDa control chart for managing large and high-dimensional CoDa datasets. Recent advances have incorporated machine learning tools, with [252] and [91] utilizing artificial neural networks to detect abnormal patterns and analyze out-of-control signals in monitoring CoDa. Most of the control charts in these studies utilized the isometric log-ratio (ilr) transformation method to map CoDa into a vector in $\mathbb{R}^{p-1}$ space, thereby removing its constraints before applying traditional control charts.

In addition to CoDa control charts, related fields such as profile monitoring and functional data analysis provide tools for addressing challenges like nonlinearity, dimensionality, and autocorrelation. Recent advancements include spatiotemporal smooth sparse decomposition for real-time anomaly detection on high-dimensional data by focusing on dimensionality reduction and spatiotemporal correlations ([247]). Deep-stacked denoising autoencoders also enhance anomaly detection in complex profiles ([41]). Similarly, [250] employed artificial neural networks to effectively monitor logistic profiles, demonstrating machine learning's adaptability to complex data. While not directly applied to CoDa, these techniques offer valuable insights for advancing CoDa monitoring, particularly in managing high-dimensional datasets.

Besides CoDa's structural challenges, traditional control charts often require extensive preliminary experimental data (Phase I data), which poses a significant problem in low-volume or custom production, where collecting sufficient Phase I data is impractical. [220] introduced a defects-per-unit control chart that leverages defect prediction models, thereby overcoming the need for large preliminary experimental data and suggesting similar approaches that could be adapted for CoDa applications. Another major challenge comes from the traditional control charts' assumption that CoDa follows a multivariate normal distribution on the Simplex space, which is not always met in practice. To address this, SPC has explored distribution-free approaches, notably control charts based on one-classification algorithms. [198] proposed kernel distance-based charts, K-chart, using Support Vector Data Description (SVDD), originally proposed by [204] based on Support Vector

Machines. Kernel methods, powerful tools in computational intelligence, enhance accuracy by mapping data into a higher-dimensional space, reduce computational costs, and improve classification by learning data structures implicitly. Leveraging kernel methods and other one-classification algorithms, [109] developed a robust K-chart that can handle autocorrelation in data. [132] proposed an SVDD control chart using the Mahalanobis kernel and showed its outperformance compared with the one using the Gaussian kernel and T^2 control chart. Later, [201] examined the impact of the Phase I dataset size on the efficiency of Phase II monitoring of SVDD-based control charts. [5] combined SVDD and kernel density estimation (KDE) to address the challenges of network intrusion detection, demonstrating improved detection of process shifts and outliers within network traffic in both simulations and real-world datasets.

2.2.1 Ratio Distributions

Ratio distributions play a critical role in SPM, particularly in monitoring process ratios, quality control metrics, and industrial process stability. Many manufacturing and healthcare applications involve data that are naturally expressed as ratios, such as signal-to-noise ratios, defect rates, and chemical concentration ratios. Let $\mathbf{W} = (X, Y)^T$ be a bivariate normal random vector with the mean vector $\boldsymbol{\mu}_W$ and the variance-covariance matrix $\boldsymbol{\Sigma}_W$ where

$$\boldsymbol{\mu}_W = \begin{pmatrix} \mu_X \\ \mu_Y \end{pmatrix}, \ \boldsymbol{\Sigma}_W = \begin{pmatrix} \sigma_X^2 & \rho\sigma_X\sigma_Y \\ \rho\sigma_X\sigma_Y & \sigma_Y^2 \end{pmatrix}, \tag{2.1}$$

in which ρ is the correlation coefficient between X and Y. By definition, the coefficients of variation of the two random variables X and Y, and their standard-deviation ratio are $\gamma_X = \frac{\sigma_X}{\mu_X}$ $\gamma_Y = \frac{\sigma_Y}{\mu_Y}$, and $\omega = \frac{\sigma_X}{\sigma_Y}$ respectively.

The ratio of X to Y is defined as $Z = X/Y$. In the literature, the distribution of Z is a major concern in several studies. As discussed in [211], when the coefficient of variation of X and Y takes small values, for example, within the range $[0, 0.2]$, the distribution of Z can be well approximated by the following formula, which is proposed by [33]:

$$F_Z(z|\gamma_X, \gamma_Y, \omega, \rho) \simeq \Phi\left(\frac{A}{B}\right), \tag{2.2}$$

where $\Phi(.)$ is the $c.d.f$ (cumulative distribution function) of the standard normal distribution, and where A and B are functions of z, γ_X, γ_Y, ω and ρ in which

$$\begin{aligned} A &= \frac{z}{\gamma_Y} - \frac{\omega}{\gamma_X}, \\ B &= \sqrt{\omega^2 - 2\rho\omega z + z^2}. \end{aligned}$$

The authors ([33]) also showed that the $p.d.f$ (probability density function) of Z can be approximated by

$$f_Z(z|\gamma_X, \gamma_Y, \omega, \rho) \simeq \left(\frac{1}{B\gamma_Y} - \frac{(z - \rho\omega)A}{B^3}\right) \times \phi\left(\frac{A}{B}\right), \tag{2.3}$$

where $\phi(.)$ is the $p.d.f$ of the standard normal distribution.

Figure 2.1 illustrates the $p.d.f$ of Z for the case $\rho = 0.5$, $\omega = \gamma_X/\gamma_Y$ and some different values of γ_X and γ_Y. Ratio distributions are particularly important in multivariate SPM, where monitoring the relationships between process parameters provides more insights than analyzing individual variables independently. The Shewhart Ratio Control Chart and Exponentially Weighted Moving Average (EWMA) Ratio Control Chart have been developed based on these distributions to detect deviations from expected process behavior [141].

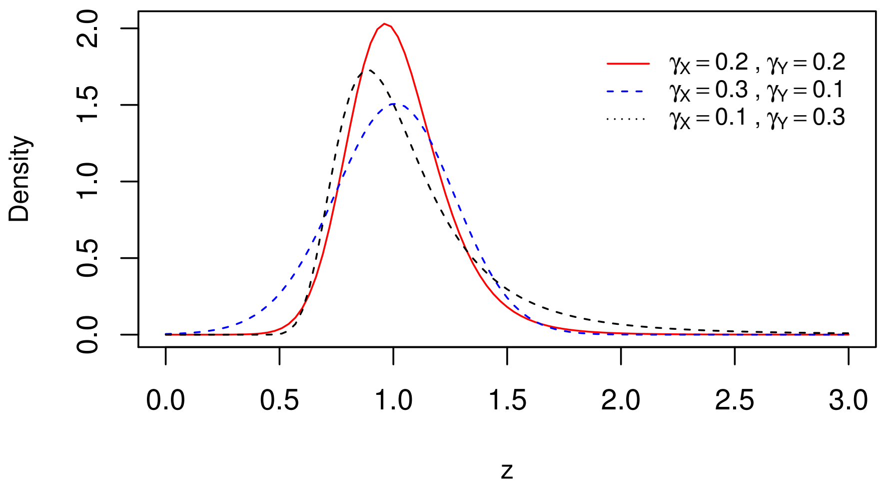


FIGURE 2.1: The probability density function of Z for the case $\rho = 0.5$, $\omega = \gamma_X/\gamma_Y$ and different values of γ_X, γ_Y.

2.2.2 Compositional Data (CoDa) Distributions

Compositional data (CoDa) distributions arise in situations where the monitored variables represent proportions of a whole, such as chemical compositions in material science, mixture proportions in food processing, and healthcare biomarker analysis. Traditional SPM techniques may fail to capture the inherent dependencies in such data, making specialized CoDa distributions essential for accurate monitoring.

Key distributions used in compositional data analysis for SPM include:

- The Dirichlet Distribution: One of the most commonly used models for multivariate compositional data, particularly when analyzing proportional relationships in quality control [7].

- The Logistic-Normal Distribution: Applied when compositional data exhibit skewness and dependency structures, making it more flexible than the Dirichlet model [7].

- The Multivariate T-Distribution for Compositional Data: Suitable for robust monitoring applications where outliers or heavy tails are present in process data [65].

CoDa distributions are particularly relevant in advanced process monitoring systems, where the relationships between process components must be jointly analyzed rather than treated as independent measurements. The application of Compositional Data Principal Component Analysis (CoDa-PCA) and Isometric Log-Ratio (ILR) Transformations has significantly improved the effectiveness of SPM techniques in dealing with compositional datasets [165].

The application of Ratio Distributions and Compositional Data Distributions in Statistical Process Monitoring (SPM) has enabled significant advancements in anomaly detection, quality control, and predictive analytics. These distributions provide essential tools for handling ratio-based and compositional data structures commonly encountered in manufacturing, healthcare, and industrial automation. The continued development of hybrid models that combine machine learning with statistical SPM techniques is expected to enhance the robustness, adaptability, and accuracy of monitoring systems in critical applications.

2.2.3 Isometric log-ratio transformation for multivariate CoDa

Consider a dataset $\mathbf{X}$ with N normal observations, denoted as $\mathbf{X}_i, i = 1, \ldots, N$, each observation is characterized by l CoDa vectors. Without loss of generality, we assume that the constant constraint on each CoDa vector $\mathbf{x} = (x_1, x_2, \ldots, x_p) \in \mathcal{S}^p$ is equal to 1, i.e., $\sum_{i=1}^{p} x_i = 1$. Additionally, we suppose that each of these l CoDa vectors may have a different number of parts, denoted as $p_1, p_2, \ldots, p_l$. Consequently, each $\mathbf{X}_i$ can be represented as follows:

$$\mathbf{X}_i = [\mathbf{x}_i^{(1)}, \dots, \mathbf{x}_i^{(l)}] = \left[x_{i1}^{(1)}, \dots, x_{ip_1}^{(1)}, \dots, x_{i1}^{(l)}, \dots, x_{ip_l}^{(l)}\right] \in \mathcal{S}_l^{p_1,\dots,p_l} \tag{2.4}$$

where $\mathcal{S}_l^{p_1,\dots,p_l}$ denote the multidimensional $(p_1, \dots, p_l)$- Simplex space with dimension l, i.e., $\mathcal{S}_l^{p_1,\dots,p_l} = \left\{[\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(l)}] : \ \mathbf{x}^{(j)} \in \mathcal{S}^{p_j}\right\}$, $\mathbf{X}_i$ has dimension $\sum_{j=1}^{l} p_j$. The whole dataset can be presented as follows:

$$\mathbf{X} = \begin{bmatrix} \mathbf{X}_1 \\ \vdots \\ \mathbf{X}_N \end{bmatrix} = \begin{bmatrix} x_{11}^{(1)}, x_{12}^{(1)}, \dots, x_{1p_1}^{(1)} & \dots & x_{11}^{(l)}, x_{12}^{(l)}, \dots, x_{1p_l}^{(l)} \\ \vdots & \ddots & \vdots \\ x_{N1}^{(1)}, x_{N2}^{(1)}, \dots, x_{Np_1}^{(1)} & \dots & x_{N1}^{(l)}, x_{N2}^{(l)}, \dots, x_{Np_l}^{(l)} \end{bmatrix}. \tag{2.5}$$

The procedure for transforming multivariate CoDa using ilr transformation method can be outlined as follows:

Algorithm 1: Ilr transformation method for transforming multivariate CoDa.

Input: A multivariate CoDa set of size N with l compositional features:

$$\mathbf{X} = \{\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_N; \ \ \mathbf{X}_i = [\mathbf{x}_i^{(1)}, \dots, \mathbf{x}_i^{(l)}] \in \mathcal{S}_l^{p_1,\dots,p_l}\}.$$

Output: Ilr transformed dataset:

$$\mathbf{X}^* = \{\mathbf{X}_1^*, \mathbf{X}_2^*, \dots, \mathbf{X}_N^*; \ \ \mathbf{X}_i^* \in \mathbb{R}^d, \text{ where } d = \sum_{j=1}^{l} (p_j - 1), i = 1, \dots, N\}.$$

Step 1: **Choose orthonormal bases:** For each CoDa feature $\mathbf{x}^{(j)}$, choose an orthonormal basis of $\mathcal{S}^{p_j}$ and form the contrast matrix $\mathbf{B}_j$ associated with this orthonormal basis.

Step 2: **Transforming data:** For each data point i^{th} and each CoDa feature j^{th}

– Compute the clr transformation using Equation

$$\mathrm{clr}(\mathbf{x}_i^{(j)}) = \left(\ln \frac{x_{i1}^{(j)}}{g_m(\mathbf{x}_i^{(j)})}, \ln \frac{x_{i2}^{(j)}}{g_m(\mathbf{x}_i^{(j)})}, \ldots, \ln \frac{x_{ip_j}^{(j)}}{g_m(\mathbf{x}_i^{(j)})}\right) \tag{2.6}$$

where $g_m(\mathbf{x}_i^{(j)}) = \left(\prod_{k=1}^{p_j} x_{ik}^{(j)}\right)^{\frac{1}{p_j}} = \exp\left(\frac{1}{p_j}\sum_{k=1}^{p_j}\log(x_{ik}^{(j)})\right)$ is the geometric mean of $\mathbf{x}_i^{(j)}$

– Compute the ilr coordinates of $\mathbf{x}_i^{(j)}$ by $\mathbf{x}_i^{*(j)} = \mathrm{clr}(\mathbf{x}_i^{(j)}) \cdot \mathbf{B}_j^{\mathsf{T}}$

– Concatenate all ilr coordinates of each feature to form the full ilr vector for each data point. The transformed dataset $\mathbf{X}^*$ is now free from the unit sum constraint and consists of N data points, each of the dimension $d = \sum_{j=1}^{l}(p_j - 1)$. The matrix representation of $\mathbf{X}^*$ can be presented as follows:

$$\mathbf{X}^* = \begin{bmatrix} \mathbf{X}_1^* \\ \vdots \\ \mathbf{X}_N^* \end{bmatrix} = \begin{bmatrix} \mathrm{clr}(\mathbf{x}_1^{(1)}) \cdot \mathbf{B}_1^{\mathsf{T}} & \mathrm{clr}(\mathbf{x}_1^{(2)}) \cdot \mathbf{B}_2^{\mathsf{T}} & \ldots & \mathrm{clr}(\mathbf{x}_1^{(l)}) \cdot \mathbf{B}_l^{\mathsf{T}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{clr}(\mathbf{x}_N^{(1)}) \cdot \mathbf{B}_1^{\mathsf{T}} & \mathrm{clr}(\mathbf{x}_N^{(2)}) \cdot \mathbf{B}_2^{\mathsf{T}} & \ldots & \mathrm{clr}(\mathbf{x}_N^{(l)}) \cdot \mathbf{B}_l^{\mathsf{T}} \end{bmatrix}. \tag{2.7}$$

2.3 Industrial Artificial Intelligence

Industrial Artificial Intelligence (Industrial AI) plays a pivotal role in revolutionizing the manufacturing and industrial sectors by optimizing processes, improving efficiency, and driving automation [113, 166]. This field leverages advanced AI methodologies, including machine learning and computer vision, to address complex industrial challenges and enhance real-time decision-making [264]. By integrating with the Industrial Internet of Things (IIoT) and utilizing state-of-the-art technologies such as edge computing, digital twins, and cybersecurity, Industrial AI enables the creation of smart manufacturing systems, predictive maintenance strategies, and overall operational improvements [202].

In the subsequent sections, we will examine how different machine learning algorithms contribute to these advancements, starting with an overview of fundamental algorithms and their industrial applications.

2.3.1 A review about Machine Learning Algorithms

Machine learning (ML) encompasses a range of algorithms designed to analyze data and make predictions. This section introduces essential ML algorithms and their theoretical foundations.

Linear Regression

Linear regression is a supervised learning algorithm used for predicting continuous values. It models the relationship between an input variable X and an output variable Y as:

$$Y = wX + b \tag{2.8}$$

where w is the coefficient and b is the bias term. The model minimizes the Mean Squared Error (MSE):

$$MSE = \frac{\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}{n} \tag{2.9}$$

cited from [140].

Logistic Regression

Logistic Regression is a simple yet powerful algorithm for binary classification tasks, using a logistic function to model the probability of an instance belonging to a particular class [173, 2]. By applying a linear equation to input features:

$$z = w_0 + w_1 x_1 + w_2 x_2 + \cdots + w_n x_n \tag{2.10}$$

and transforming the output with a sigmoid function:

$$\sigma(z) = \frac{1}{1 + e^{-z}} \tag{2.11}$$

Logistic Regression outputs values between 0 and 1, representing class probabilities. Due to its simplicity, efficiency, and interpretability, Logistic Regression is a popular choice for tasks with linearly separable data and provides a solid baseline for classification problems.

eXtreme Gradient Boosting (XGBoost)

XGBoost, or eXtreme Gradient Boosting, is an advanced machine learning algorithm known for its speed and high performance, particularly on structured data [76, 2]. It builds an ensemble of decision trees through boosting, where each tree corrects the errors of previous ones, ultimately creating a strong predictive model.

The objective function in XGBoost consists of a loss function and a regularization term:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} l(y_i, \hat{y}i) + \sum k\Omega(f_k) \tag{2.12}$$

Where is the loss function, and is the regularization term that helps prevent overfitting?

XGBoost incorporates regularization, making it resistant to overfitting, and optimizations such as parallel processing, tree pruning, and efficient handling of missing data. These features make XGBoost highly effective for classification and regression tasks, particularly in competitive data science scenarios that require accurate and efficient predictions.

Random Forest

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve prediction accuracy and robustness [222, 70, 2]. Training each tree on a different, randomly selected subset of data and features creates a diverse "forest" of models, thereby reducing overfitting and improving generalization.

The final prediction is made by:

Averaging predictions for regression:

$$\hat{y} = \frac{1}{M} \sum_{m=1}^{M} f_m(x) \tag{2.13}$$

Majority voting for classification:

$$\hat{y} = \text{mode} f_1(x), f_2(x), \ldots, f_M(x) \tag{2.14}$$

Random Forest is highly effective for both classification and regression tasks. It is popular due to its accuracy, resistance to overfitting, and ease of interpretation, as it provides insights into feature importance.

Light Gradient Boosting Machine (LightGBM)

Light Gradient Boosting Machine (LightGBM) is a highly efficient gradient boosting framework designed for speed and performance, particularly with large datasets. It builds an ensemble of decision trees [70, 2], like other boosting algorithms, but differs by using a leaf-wise growth strategy instead of level-wise, allowing it to capture more complex patterns and achieve higher accuracy.

The model follows a leaf-wise tree growth strategy:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} l(y_i, \hat{y}i) + \lambda \sum j = 1^T ||w_j||^2 \tag{2.15}$$

Where is the regularization term controlling complexity?

Decision Trees

A decision tree partitions data into subsets using feature-based splits. The split criterion is chosen based on measures like information gain:

$$IG = H(S) - \sum_{i=1}^{k} \frac{|S_i|}{|S|} H(S_i) \tag{2.16}$$

as described in [62].

Support Vector Machines (SVM)

SVM is a classification algorithm that finds an optimal hyperplane, maximizing the margin between classes. It solves the optimization problem:

$$\min_{w,b} \frac{1}{2} ||w||^2 \tag{2.17}$$

subject to:

$$y_i(w \cdot x_i + b) \geq 1, \quad \forall i \tag{2.18}$$

as formulated in [37].

K-Nearest Neighbors (KNN)

KNN is a non-parametric algorithm that classifies data points based on the majority class of their k nearest neighbors, computed using Euclidean distance:

$$d(x_i, x_j) = \sqrt{\sum_{k=1}^{n} (x_{ik} - x_{jk})^2} \tag{2.19}$$

[141].

K-Means Clustering

K-Means is an unsupervised learning algorithm that groups data into k clusters by minimizing intra-cluster variance:

$$J = \sum_{i=1}^{k} \sum_{x \in C_i} ||x - \mu_i||^2 \tag{2.20}$$

as discussed in [237].

Naive Bayes Classifier

Naive Bayes is a probabilistic classifier based on Bayes' theorem:

$$P(Y|X) = \frac{P(X|Y)P(Y)}{P(X)} \tag{2.21}$$

Assuming feature independence, it simplifies to:

$$P(Y|X) \propto P(Y) \prod_{i=1}^{n} P(X_i|Y) \tag{2.22}$$

as referenced in [185].

Support Vector Data Description (SVDD)

Support Vector Data Description (SVDD) is a one-class classification method that extends the concept of Support Vector Machines (SVM) to describe the boundary of a dataset. The goal of SVDD is to find a minimal enclosing hypersphere that captures most of the training data while minimizing the effect of potential outliers [205].

Mathematically, SVDD aims to determine a hypersphere characterized by center $\mathbf{c}$ and radius R that minimizes the objective function:

$$\min_{R,\mathbf{c},\xi_i} \quad R^2 + C \sum_{i=1}^{n} \xi_i \tag{2.23}$$

subject to the following constraints:

$$\|\mathbf{x}_i - \mathbf{c}\|^2 \leq R^2 + \xi_i, \quad \xi_i \geq 0, \quad i = 1, \ldots, n \tag{2.24}$$

where ξ_i are slack variables allowing for soft-margin tolerance, and C is a regularization parameter that controls the trade-off between the volume of the hypersphere and the penalty for outliers [205].

These fundamental ML algorithms form the basis for advanced machine-learning techniques explored in later sections.

KNN imputation

K-Nearest Neighbors (KNN) imputation is a technique for handling missing data by using the values of nearby, similar instances [258, 169]. For each missing value, it finds the "K" nearest neighbors based on feature similarity and then calculates an average or majority value from those neighbors to replace the missing entry. This approach enables more informed estimates than simply filling in with means or medians by leveraging relationships within the data.

Independent Component Analysis (ICA)

ICA is a computational technique used to separate a multivariate signal into additive, independent components [136]. It assumes that the observed data is a mixture of underlying sources and works to identify statistically independent signals, often used for tasks like noise reduction, feature extraction, and dimensionality reduction. ICA is particularly useful when the goal is to reveal hidden factors or patterns in data, and it has applications in areas such as image processing, EEG signal analysis, and finance.

Isolation Forest

Isolation Forest is an effective algorithm for detecting and removing outliers in datasets by isolating instances that differ significantly from the majority [245]. Unlike traditional methods that rely on distance or density, Isolation Forest works by randomly partitioning data points and constructing isolation trees. Outliers, being more isolated, tend to appear closer to the root of these trees, whereas normal points require more splits to be isolated. This makes Isolation Forest particularly suitable for high-dimensional datasets, as it efficiently identifies and eliminates outliers, improving the overall quality of the dataset for downstream tasks.

2.3.2 Deep Learning

Deep learning has emerged as one of the most powerful techniques in machine learning, achieving significant success in various domains, including image recognition, natural language processing, and speech recognition.

Convolutional Neural Networks

Convolutional Neural Networks (CNNs) are a class of deep neural networks specifically designed to process data with grid-like structures, such as images and videos. Unlike traditional neural networks, CNNs utilize convolutional layers to automatically learn features from data, thus reducing the reliance on manual feature extraction. The structure of CNNs typically consists of convolutional layers, pooling layers, and fully connected layers, enabling the network to learn features at various levels of abstraction [108]. CNNs have achieved remarkable success in various tasks such as image recognition and classification, particularly after Alex Krizhevsky and colleagues introduced the AlexNet architecture in 2012, which achieved impressive results in the ImageNet competition [108]. Moreover, CNNs have been widely applied in speech recognition, video analysis, and healthcare fields because they can effectively learn and extract features from complex data [159].

Long Short-Term Memory

Long Short-Term Memory (LSTM) is a type of recurrent neural network (RNN) designed to address the vanishing gradient problem commonly encountered in traditional RNNs. LSTM can retain information over long periods, enabling the model to learn long-term dependencies in sequential data. The structure of LSTM includes three main gates: the forget gate, the input gate, and the output gate, which control the flow of information into and out of the cell state, thereby regulating the storage and forgetting of information [83]. LSTM has been widely applied in various fields such as speech recognition, machine translation, time-series analysis, and human action recognition due to its capacity to capture and maintain long-term dependencies in data. For example, Graves et al. (2013) utilized LSTM to develop powerful language models for automatic speech recognition [74].

Generative Adversarial Networks

Generative Adversarial Networks (GANs) are a class of deep learning models introduced by Ian Goodfellow and colleagues in 2014. GANs consist of two neural networks: a generator and a discriminator, which operate in an adversarial manner. The generator creates fake data, while the discriminator attempts to distinguish between real and fake data. The training process is adversarial, where both networks improve their capabilities, resulting in the generation of increasingly realistic fake data [73]. Since their introduction, GANs have been widely applied across various fields, including image, video, and audio generation, as well as medical data synthesis. They have proven capable of generating high-quality fake data, opening up numerous potential applications in art, entertainment, and scientific research [230].

Deep Convolutional K-Means

Deep Convolutional K-Means (DCKM) is a novel clustering method proposed by Anurag et al.[71]. DCKM integrates the capabilities of convolutional neural networks (CNNs) with K-means clustering to create a robust framework for unsupervised learning suited for image data. Traditional CNN-based clustering approaches often rely on encoder-decoder architectures, which can lead to overfitting in data-limited situations due to the need for additional weights in the decoder network. DCKM addresses this limitation by introducing a Deep Convolutional Transform Learning (DCTL) that eliminates the decoder, thereby learning fewer parameters and reducing the potential for overfitting. The schematic diagram of DCKM is shown in Figure 2.2.

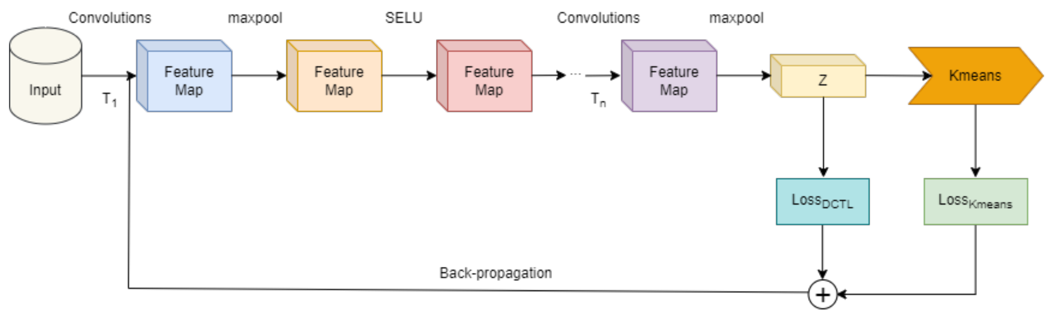


FIGURE 2.2: Schematic diagram of Deep Convolutional K-Means

Autoencoders and Variational Autoencoders

Autoencoders and Variational Autoencoders (VAEs) are two types of deep neural networks designed to learn compressed representations of data, commonly used in tasks such as dimensionality reduction, data reconstruction, and generative modeling. Autoencoders comprise two primary components: an encoder and a decoder. The encoder maps the input data to a lower-dimensional latent space, while the decoder reconstructs the data from this latent representation. The training process aims to minimize the difference between the input data and the reconstructed output, allowing the network to learn essential features of the data [267]. Variational Autoencoders (VAEs) extend the concept of autoencoders by incorporating Bayesian inference into the learning process. Instead of learning a fixed latent representation, VAEs learn the probability distribution of the latent space, allowing for the generation of new data by sampling from this distribution. This is achieved by minimizing the difference between the latent distribution and a prior distribution and the reconstruction loss between the input and output data [105]. Both models have been widely applied in various domains, including image processing, time-series analysis, and data generation, due to their ability to effectively learn and generate complex data [105].

Transformers

Transformers are a deep learning architecture first introduced in the paper "Attention is All You Need" by Vaswani et al. in 2017. Unlike previous models such as RNNs and LSTMs, Transformers leverage the attention mechanism to process sequential data without relying on traditional sequential structures. This enables the model to efficiently learn long-range dependencies in data. Since its introduction, Transformers has achieved remarkable success in various natural language processing tasks, including machine translation, classification, and generation. Models like BERT and GPT have demonstrated exceptional performance in understanding and generating natural language. Additionally, Transformers have been applied in other fields, such as computer vision and time-series analysis [219].

Vaswani et al. [219] introduced a novel architecture called Transformer for sequence-to-sequence learning. One of the key components of transformers is the attention mechanism. The attention mechanism examines an input sequence and determines at each step which other parts of the sequence are most important. Similar to LSTMs, a transformer transforms one sequence

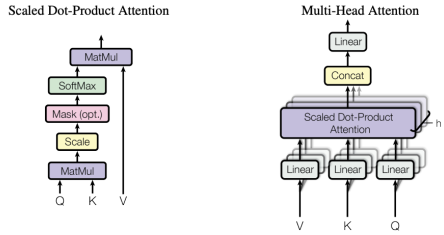


FIGURE 2.3: An illustrative diagram of the attention mechanism and its parallelization, regenerated from [219]. Left: the attention mechanism. Right: parallelization of the attention mechanism.

into another with the help of two parts: an encoder and a decoder. However, it differs from existing sequence-to-sequence methods in that it does not rely on any recurrent networks (GRU, LSTM, etc.). The encoder and decoder consist of modules that can be stacked on top of each other multiple times. Each module mainly consists of multi-head attention and feed-forward layers. The input and output are first embedded into an n-dimensional space since they cannot be used directly. Another part of the model is the positional encoding of different words. Since no recurrent networks can remember how a sequence is fed into the model, a relative position is encoded for every part of the input sequence. These positions are added to the embedded n-dimensional vector of each input subsequence.

The attention mechanism used in transformers can be described by the following equation:

$$\text{Attention}(Q, K, V) = \text{Sofmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V, \tag{2.25}$$

where Q is the query matrix (vector representation of input sub-sequence), K is all the keys (vector representations of all the sequences), and V is the values (vector representations of all the sequences). For the encoder and the decoder, the multi-head attention modules, V, consist of the same word sequence as Q. However, for the attention module that takes in the encoder and decoder sequences, V differs from the sequence represented by Q. In other words, V is multiplied and summed with the attention weights γ, defined by the following equation:

$$\gamma = \text{Sofmax}\left(\frac{QK^T}{\sqrt{d_k}}\right). \tag{2.26}$$

The self-attention mechanism is applied multiple times in parallel, along with the linear projections of Q, K, and V. It helps the system to learn from different representations of Q, K, and V. The weight matrices W that are learned during the training are multiplied by Q, K, and V to learn the linear representations. Figure 2.3 gives an illustrative diagram of the attention mechanism and its parallelization.

Moreover, positional encoding is used to track the input and output sequences. Finally, transformers employ feed-forward networks. These feed-forward networks have identical parameters for each position of the input sequence, which describes each element from a given sequence as a separate but identical linear transformation.

Transformers have various applications because they utilize attention mechanisms, which enable machine learning models to learn from data more effectively, thereby improving the performance of numerous machine learning tasks, such as those in natural language processing [174]. For example, a hybrid HAR classifier using CNNs and transformers was introduced in [116], which employs a two-streamed structure to capture both time-over-channel and channel-over-time features, and utilizes a multi-scale convolution augmented transformer to capture range-based patterns.

TabNet

TabNet is a deep learning model explicitly designed for tabular data, leveraging attention mechanisms to select relevant features for each instance during training [11]. Unlike traditional neural networks, which treat all features uniformly, TabNet dynamically focuses on the most informative features at each decision point, improving performance and interpretability.

TabNet uses a sequential attention mechanism defined as:

$$M^{(t)} = \sigma(\mathbf{W}_1^{(t)} f^{(t)} + b_1^{(t)}) \tag{2.27}$$

Where represents the mask that selects the most important features at this step.

It combines the strengths of decision trees and deep learning by allowing for efficient, hierarchical feature selection and reasoning.

2.3.3 Federated Learning and Cybersecurity

Federated Learning (FL) [139] is a concept in distributed machine learning where edge devices or independent organizations (such as hospitals, companies, etc.) collaborate to train a shared model, known as the global model. The training of the global model occurs without requiring participating edge devices to share their raw data with other nodes or a central server. Instead, each edge device trains a local model using its private data and only shares the trained parameters with a central server in centralized FL or with all other nodes in decentralized FL.

The aggregation of local models is conducted based on a specific aggregation algorithm to compute the parameters of the global model [256], among which the FedAvg algorithm [137] is the most widely used [199]. Mathematically, the FedAvg algorithm is expressed as follows:

$$AW = \frac{n_k}{n_K} \sum_{k=1}^{K} W_k, \tag{2.28}$$

where AW represents the globally aggregated weights, n_k and n_K denote the number of samples in an individual edge device and the total number of samples from all participating edge devices, respectively. W_k^t refers to the locally trained weights of the k-th edge device/client, and K represents the total number of edge devices/clients participating in the global round. The process of updating the global model is iterated until the desired performance level is achieved or the performance of the global model ceases to improve significantly.

In Federated Learning (FL), handling non-independent and identically distributed (non-i.i.d.) data presents a significant challenge, particularly in the context of poisoning attacks. A typical feature of FL is the collaboration of distributed clients to train a global model without sharing their local data, which ensures privacy. However, this distributed architecture exposes the system to various vulnerabilities, especially when malicious clients inject poisoned data into their local models. These attacks can range from data poisoning, where the local data is manipulated, to model poisoning, where the model parameters are altered after training. Non-i.i.d. data, where the distribution of data across clients varies significantly, exacerbates the difficulty in detecting poisoning attacks. Traditional detection methods often assume independent and identically distributed (i.i.d.) data, where all clients draw their data from the same distribution. When the data is non-i.i.d, the model updates from different clients might naturally differ due to these inherent data variations, making it harder to distinguish between legitimate updates and malicious ones.

Poipose a significant security threat that can severely compromises security threat that can severely impair the performance of the global model. These attacks can be categorized into data poisoning and model poisoning.

In data poisoning attacks, adversaries manipulate the training data on compromised devices. In contrast, in model poisoning, attackers manipulate the model parameters after training them on benign data but before uploading them to the global server [67]. These attacks can undermine the collective goal of FL, which is to train a robust global model without sharing sensitive data across clients. The challenge of detecting poisoning attacks arises from the nature of federated learning, where the detection system does not have access to the raw local training data of the edge devices. Consequently, traditional methods that rely on inspecting local data or models are ineffective. Researchers have proposed several detection mechanisms, but they often rely on assumptions such as the knowledge of the number of attackers or the use of independent and identically distributed (i.i.d.) data [67]. Furthermore, the computational complexity of existing methods is high, limiting their scalability and applicability in real-world scenarios. To address the above-mentioned attacks, many defense methods have been proposed. Hu et al. [85] surveyed the state-of-the-art defensive methods against Byzantine attacks in FL. They show that Byzantine attacks by malicious clients can significantly reduce the accuracy of the global model. Moreover, their results show that existing defense solutions cannot fully protect FL against such attacks. In [239], Xia et al. summarized poisoning attacks and defense strategies according to their methods and targets.

2.3.4 Explainable AI

Explainable Artificial Intelligence (XAI) plays a pivotal role in enhancing the transparency, trust, and interpretability of AI systems, particularly in critical sectors like healthcare and smart manufacturing. In healthcare, AI models are increasingly being used to assist in medical decision-making, diagnostics, and personalized treatment planning. However, the black-box nature of many AI algorithms, particularly deep learning models, raises concerns about the reliability and ethical implications of their use in sensitive areas where human lives are at stake.

In healthcare, the need for XAI is particularly significant. For example, in [4], the authors explore how XAI techniques can be used to improve the interpretability of AI models used for medical diagnostics. The application of SHAP and LIME helps provide both global and local explanations for predictions made by these models, allowing healthcare professionals to understand the rationale behind diagnostic results and treatment recommendations. This is crucial in building trust and ensuring that AI tools are used effectively in clinical settings. Furthermore, XAI enables clinicians to identify and correct potential biases in AI systems, ensuring fairness and reducing the risk of harm in decision-making processes.

Similarly, in smart manufacturing systems, XAI is essential for improving the security, efficiency, and reliability of AI-driven processes. Manufacturing systems are becoming increasingly interconnected, with machines, sensors, and control systems working in tandem to optimize production. In these environments, anomaly detection and predictive maintenance powered by AI models are crucial for ensuring smooth operations. However, the lack of explainability in these models can hinder their adoption and effectiveness. In [232], the authors discuss how XAI can be applied to intrusion detection systems (IDS) in manufacturing environments to explain detected anomalies and attacks. By using SHAP to generate both local and global explanations, the IDS models become more transparent, helping administrators understand the features influencing model decisions and enabling more effective mitigation of cyber threats.

XAI also plays an important role in the context of fault diagnosis in manufacturing systems. In [25], XAI is used to diagnose faults in rotating machinery, where it helps classify and analyze anomalies in critical components like rotors and bearings. This application of XAI ensures that the root causes of faults are identified, allowing for more precise and timely interventions. Overall, the integration of XAI into healthcare and smart manufacturing systems not only enhances the effectiveness of AI models but also addresses concerns related to transparency, fairness, and accountability.

Explaining the effect of features is crucial in machine learning because it helps us understand which variables are driving model predictions, making models more interpretable and transparent. This is especially important in areas where decisions impact people's lives, such as healthcare, finance, and law. When we know which features are most influential, we can verify that a model is making logical and fair decisions, adjust the model if it exhibits bias, and communicate its reasoning to stakeholders [4]. One popular method for feature explanation is SHAP (Shapley Additive exPlanations) values [203]. SHAP values use principles from game theory to allocate each feature's contribution to a prediction, giving a clear indication of each feature's positive or negative impact. SHAP values provide consistent, model-agnostic explanations, making them valuable for interpreting complex models like neural networks or ensemble methods. This approach helps increase trust in machine learning models by making their predictions more transparent and understandable.

2.4 Blockchain Background and related works on RUL prediction

Blockchain (BC) technology provides a robust solution to the challenges encountered in Federated Learning (FL). BC ensures trust, transparency, and security throughout the collaborative model training process by establishing a decentralized and immutable ledger. Its ability to reinforce data privacy, incentivize participation, and enhance scalability makes BC a crucial enabler for secure and efficient FL deployment across various dynamic and diverse environments. Additionally, integrating Artificial Intelligence (AI) with blockchain holds great promise. AI brings pattern recognition, machine learning, and decision-making capabilities, which, when combined with blockchain's transparency and security, can create highly efficient and trustworthy systems for sectors such as supply chain management, healthcare, and finance. The synergy between BC and AI can also address challenges such as ensuring data integrity in AI models and facilitating decentralized AI marketplaces. This section explores the fundamental aspects of BC, including its definition, smart contracts (SC), and architecture concerning FL and its integration with AI.

2.4.1 Blockchain

BC functions as a decentralized, distributed database [158]. Within this system, transactional records are linked sequentially into chains of blocks and stored in chronological order. Each transaction is secured using cryptographic techniques and Proof-of-Work (PoW) mechanisms, ensuring data integrity and preventing tampering or forgery [123]. Figure 2.4 illustrates the core BC structure and data flow, where each block contains a header with metadata and transactional records. These blocks are interconnected via cryptographic hash pointers, forming a comprehensive and immutable ledger. The BC architecture comprises multiple layers, including the data layer, incentive mechanism, consensus layer, network layer, and application layer. BC can be categorized into three main types: public, consortium, and private. The selection of a BC type depends on specific business requirements; however, only the public chain fully aligns with the original decentralized vision of BC. Moreover, integrating AI with blockchain offers new possibilities for enhancing blockchain systems. For example, AI can be used to optimize blockchain's scalability and performance, while blockchain ensures the integrity of AI model training and data collection processes [243]. Additionally, blockchain provides a secure and decentralized way to share data and AI models, overcoming the challenges of trust and centralization in traditional systems. The combination of these two technologies creates decentralized AI marketplaces, which can securely exchange data and models without the need for intermediaries [89]. This convergence of blockchain and AI technologies is paving the way for more robust, scalable, and transparent systems across multiple industries.

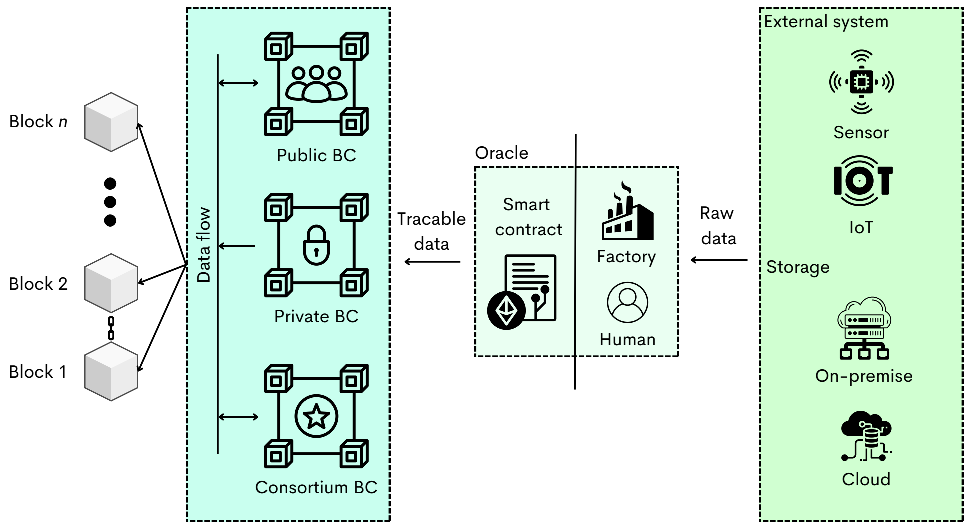


FIGURE 2.4: Basic concept of BC and its data flow from raw data to blocks.

2.4.2 Smart Contracts (SC)

SC is an essential application of Blockchain (BC) technology that enables automated, transparent, and trustless transactions, eliminating the need for intermediaries in many cases. A smart contract is a self-executing program that operates according to the terms defined in its code. It digitally verifies and automatically enforces the terms of an agreement, ensuring that the contract is executed as specified without human intervention or the involvement of a central authority [28]. These contracts are stored and processed on the blockchain, providing them with immutability and traceability, critical for secure and reliable execution [45].

In a Federated Learning (FL) context, SCs are crucial in improving the overall system by ensuring transparent and fair processes. As shown in Figure 2.4, SCs are used to manage the interactions between different participants in the FL ecosystem. They validate model updates, ensuring that only authorized participants can contribute to the training process and that their contributions are accurately recorded and compensated [123]. Moreover, SCs facilitate the creation of decentralized applications (dApps), where participants can interact with each other directly, further enhancing the efficiency of FL systems. By incorporating SCs, the FL process benefits from enhanced security, as every transaction and model update is recorded on the blockchain as transparent and immutable. This creates an auditable trail crucial for resolving disputes or ensuring compliance with the agreed-upon terms in FL-based applications [123]. Furthermore, SCs are instrumental in managing incentives for fair participation. By automating reward distribution based on contributions, they prevent the need for trust in a central authority and ensure that all participants are incentivized in a transparent and verifiable manner. This transparency in rewards and punishments is essential in environments where multiple parties, often with competing interests, are involved in the learning process.

2.4.3 RUL prediction

In this subsection, we provide an overview of RUL prediction, encompassing both traditional methods and the emerging FL approach.

Traditional RUL prediction approaches at a single site

Traditional RUL prediction approaches typically rely on various aspects, such as physical characteristics, structural attributes, historical data, sensor measurements, and the observed behaviors of components or systems to estimate the remaining operational lifespan at a single site. These conventional methodologies have been instrumental in predicting RUL, primarily emphasizing localized data analysis and predictive modeling. Specifically, data-driven approaches are increasingly favored for RUL predictions, eclipsing model-based methods due to their independence from knowledge of the underlying engineering system [114]. In industries, the inherent complexity of real-world systems makes it challenging to accurately represent all systems using solvable mathematical or physics-based approaches [81]. In addition, the proliferation of sensors has provided abundant data on system conditions. Concurrently, the maturation and widespread adoption of machine learning (ML) techniques have popularized ML-based models for RUL predictions, including approaches such as random forests and various neural networks. These models capture the intricate relationships between system health and RUL without necessitating an in-depth understanding of the degradation processes.

However, data-driven prognostics in decentralized industries face multiple challenges due to the sparse nature of the data and the specific requirements of the predictive tasks [186]. One primary concern is the decentralized nature of the condition monitoring data, which is typically collected from diverse sites across the globe [215]. These data sets often present high variance due to the differing operational environments, machine usage patterns, and maintenance practices at each site [58]. As a result, building a generic model that can accurately predict the RUL across all sites becomes a considerable challenge [63, 227]. Addressing these challenges requires a novel methodology that can leverage condition monitoring data from multiple sites while preserving each site's data privacy and trust. FL offers a promising solution to these challenges. In the next section, we discuss the FL-based approach for RUL prediction in detail.

FL-based approaches for RUL predictions across multiple sites

This section discusses how the FL overcomes problems with centralized methods. As a leader in collaborative machine learning, FL allows us to train models on many devices without sharing personal data. We will look at the basics, benefits, and uses of FL in RUL prediction. We will also talk about how FL can make a big difference in predictive maintenance by solving issues with old methods.

In an FL algorithm, a specific ML model is trained, distributed among some edge devices, and then aggregated in a server. Let d be the dimension of the model parameters; FL algorithm finds a model parameter set as $\boldsymbol{w} \in \mathbb{R}^d$ in each worker that can be expressed as:

$$\min_{\boldsymbol{w}} \{f(\boldsymbol{w})\}, \tag{2.29}$$

where

$$f(\boldsymbol{w}) = \sum_{i=1}^{K} \frac{n_i}{K} f_i(\boldsymbol{w}) \tag{2.30}$$

is the loss function to be minimized, K is the number of worker, $f_i(\boldsymbol{w})$ is the worker k's loss function, and n_i is size of worker's dataset. Various techniques such as learning federated averaging (FedAvg), federated stochastic gradient descent (FedSGD), and federated proximal (FedPro), can be used to facilitate collaborative model training across decentralized devices [122]. Particularly, FedAvg is lauded for its simplicity and interpretability but employs a fixed global learning rate. In contrast, FedSGD offers hyperparameter flexibility but may encounter privacy challenges. Finally, FedPro provides convergence guarantees under specific conditions but involves complex hyperparameter fine-tuning. In consideration of the objectives of our study, the FedAvg algorithm is chosen due to its simplicity and alignment with our research goals, focusing on FL's application in real-time RUL prediction, as detailed in [122].

In the FL-based approach, multiple ML algorithms can be used for RUL prediction, i.e., minimize loss function $f_i(\boldsymbol{w})$ between prediction and actual values. Multiple methods, including linear regression [234], radical basic functions [235], deep neural networks (DNN) [167], and support vector machine (SVM) [157] algorithms, can serve as ML models in the FL process. The figure 2.5 illustrates how ML models for RUL prediction are incorporated into the FL architecture across various sites. Each site (Factory 1 to Factory K) trains the RUL prediction models locally to maintain data privacy and security. These models' parameters are then transmitted to the aggregation server, which employs the FedAvg algorithm to integrate the individual contributions into a cohesive global model. Subsequently, this refined global model is redistributed to each site. Note that this study underscores the benefits of combining Blockchain (BC) technology with FL to enhance security and trust in the distributed learning process rather than improving the RUL prediction performance of the ML model utilized.

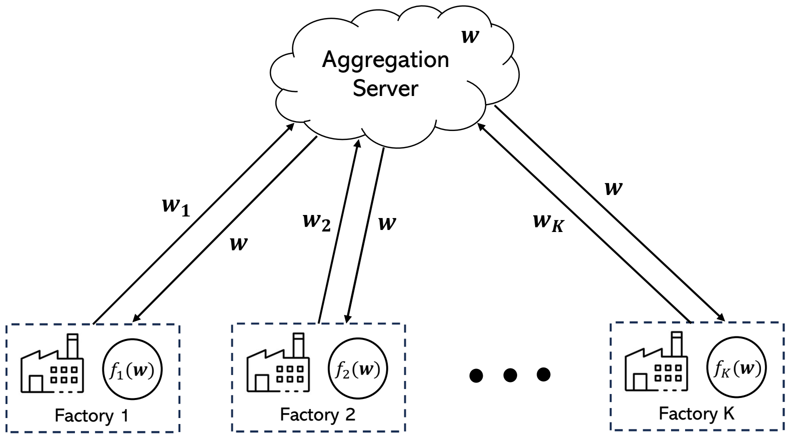


FIGURE 2.5: Architecture of the FL process using ML model.

Major problems of FL in RUL prediction

In the FL domain, the quintessential challenge is to derive a comprehensive statistical model leveraging datasets dispersed across numerous remote devices, ranging from a few to potentially millions [135, 121]. Such a process is encapsulated by Eq. (2.30), the local objective function $f_i(\boldsymbol{w})$ represents the empirical risk calculated from the data on each remote device. Although FL inherently integrates mechanisms designed to safeguard against unauthorized access and data breaches, it is not impervious to adversarial exploits, which could undermine the system's integrity and the data's confidentiality. As shown in Fig. 2.6, it succinctly enumerates the advantages and disadvantages of employing FL in the context of real-time RUL predictions, delineating them into four beneficial attributes juxtaposed against four potential drawbacks.

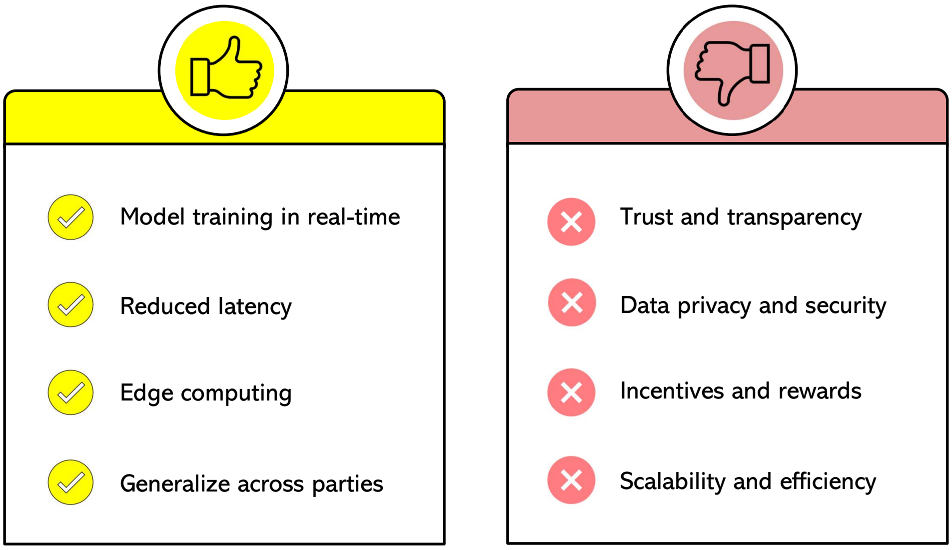


FIGURE 2.6: Pros (left) and cons (right) of FL in RUL prediction.

In the pursuit of enhancing the efficacy of Federated Learning (FL) for industrial Remaining Useful Life (RUL) predictions, the integration of blockchain (BC) technology emerges as a promising solution [131]. This amalgamation amplifies the inherent advantages of both FL and BC and adeptly navigates through the multifaceted challenges prevalent in this domain. The following section will delve into the intricacies of the proposed blockchain-enhanced FL framework, tailored explicitly for RUL prediction in industrial contexts.

2.5 Performance Evaluation

Control charts are evaluated based on their ability to detect process shifts efficiently (e.g., ARL, false alarm rate, detection probability), while machine learning models are assessed using predictive accuracy, robustness, and computational efficiency (e.g., precision, recall).

2.5.1 Performance Evaluation for Control Charts

The design of control charts serves two main objectives: i) minimizing the false alarm rate in an in-control process and ii) ensuring a higher false alarm rate in an out-of-control process. Various metrics have been proposed to assess the effectiveness of control charts. One such metric, introduced by Aronian and Levene (1950) [12], utilizes the Run Length (RL) distribution to evaluate the performance of control charts. The RL is defined as the number of points on a chart until a control chart signals an out-of-control condition.

The Average Run Length (ARL), which is the mean value of RL, is frequently used as a standard measure for control chart performance. When the process is in control, ARL is referred to as ARL_0, and when the process is out of control, it is denoted as ARL_1. To evaluate the performance of a chart, ARL_0 is set as a fixed value, while ARL_1 is used to determine the effectiveness of the chart. A smaller value of ARL_1 indicates a more effective chart.

The ARL in an in-control process is defined by the equation:

$$ARL_0 = \frac{1}{\alpha}$$

where α represents the Type I error. For an out-of-control process, ARL is defined as:

$$ARL_1 = \frac{1}{1-\beta}$$

where β is the Type II error. In instances where process parameters need to be estimated, the Expected Average Run Length (EARL) is considered to study control chart performance. Often, the distribution of RL is skewed, and thus, the Median Run Length (MRL) is preferred as a more accurate measure.

To evaluate the dispersion of the Run Length, we use the Standard Deviation of the Run Length (SDRL), which is calculated as:

$$SDRL = \sqrt{\frac{\beta}{1-\beta}}$$

In several cases, when there is no preference for any specific shift size, one may suggest assigning a distribution for the process shift in a predicted interval. The expected average run length ($EARL$) is used to evaluate the statistical performance of the corresponding chart, where

$$EARL = \int_{\Omega} ARL \times f_{\tau}(\tau)\mathrm{d}\tau, \tag{2.31}$$

$f_{\tau}(\tau)$ stands for the ditribution of the shift size τ in the interal Ω and ARL is as defined in (3.11). When there is no information about τ, a uniform distribution of τ could be applied, i.e. is the distribution of $f_{\tau}(\tau) = \frac{1}{b-a}$ for $\tau \in \Omega = [a, b]$.

2.5.2 Performance Evaluation for Machine Learning

To evaluate the classification performance of the proposed transformer-based classifier, we utilize the following four classification metrics, which are widely used for assessing machine learning models [64, 107].

1. **Accuracy** is defined as the correctly predicted observation divided by total observations, as given below:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}}, \tag{2.32}$$

   where TP, TN, FP, and FN are true positives, true negatives, false positives, and false negatives number of samples, respectively.

2. **Precision** is defined as the number of true positives divided by the total number of true positives plus the total number of false positives for a given class, given as follows:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}. \tag{2.33}$$

3. **Recall** is defined as the total number of true positives divided by total true positives plus false negatives for a given class, given as follows:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{2.34}$$

4. **F1-score** is defined as the weighted average of precision and recall, given as follows:

$$\text{F1-Score} = \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}. \tag{2.35}$$

All the above four performance metrics used are defined for binary classifiers only, so for multi-class HAR classifiers, we used the one-versus-rest strategy to calculate the performance metrics for each class.

2.6 Monitoring, Anomaly Detection, Classification, and their Applications in Smart Manufacturing and Healthcare: state of the art

The development of AI and statistical techniques has significantly advanced the fields of monitoring, anomaly detection, and classification, enabling intelligent decision-making and improving efficiency across various domains. Traditional statistical methods have long been the foundation of anomaly detection, focusing on probabilistic modeling and hypothesis testing to identify deviations in structured datasets. Meanwhile, ML approaches, especially deep learning models, have expanded these capabilities by enabling automated feature extraction and adaptive learning from complex, high-dimensional data [98, 59].

Statistical approaches, particularly statistical process control (SPC), have played a fundamental role in monitoring production processes and maintaining quality control in industries. Control charts, such as Shewhart, exponentially weighted moving average (EWMA), and cumulative sum (CUSUM) charts, have been widely used to track variations and detect shifts in production parameters [141, 237]. In addition, statistical anomaly detection techniques based on probabilistic models, Bayesian inference, and regression analysis have been successfully applied to detect irregularities in both industrial and healthcare data. These methods excel in environments where domain knowledge allows the definition of clear statistical thresholds for normal and abnormal behavior.

However, the increasing complexity of modern industrial and healthcare systems necessitates more adaptive and scalable techniques beyond traditional statistical methods. Machine learning, particularly unsupervised learning models, has revolutionized anomaly detection by identifying patterns without predefined labels. Clustering algorithms such as k-means and DBSCAN have been applied in cybersecurity, fraud detection, and manufacturing defect identification to detect unusual patterns indicative of system failures or security breaches [36]. Additionally, autoencoders and generative adversarial networks (GANs) have demonstrated strong performance in detecting anomalies in complex data streams, particularly in predictive maintenance and fault detection scenarios [88].

Classification models, another critical aspect of ML, have facilitated more effective decision-making in domains such as disease diagnosis, predictive maintenance, and industrial automation. Traditional classification techniques, including support vector machines (SVMs), decision trees, and logistic regression, have been successfully applied in structured data analysis for categorizing faults, diseases, and operational conditions [110]. However, deep learning-based classifiers, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have significantly improved accuracy in unstructured data applications, including medical imaging, speech recognition, and industrial automation[138]. Integrating federated learning (FL) has further enabled decentralized model training while preserving data privacy, a crucial requirement in healthcare and distributed manufacturing systems [176, 265].

Recent advancements in explainable AI (XAI) have sought to bridge the gap between the high accuracy of ML models and their interpretability. SHAP values, LIME, and counterfactual explanations are emerging techniques that provide insights into how ML models arrive at their decisions, increasing trust in AI-driven monitoring and classification systems [77]. This is particularly relevant in healthcare applications, where AI-based diagnostic and anomaly detection systems must align with medical best practices and regulatory requirements.

Overall, the synergy between statistical methods and machine learning has significantly improved monitoring, anomaly detection, and classification, addressing critical challenges such as data complexity, scalability, and interpretability. While statistical approaches remain indispensable for well-defined problems with structured data, ML techniques have expanded capabilities to unstructured, high-dimensional datasets, enabling automation and real-time decision-making across industries. Future research will continue to refine these methodologies, integrating advancements in federated learning, explainable AI, and hybrid statistical ML models to ensure transparency, security, and efficiency in critical domains.

2.6.1 Artificial Intelligence and Statistical Methods for Smart Manufacturing

Smart Manufacturing is characterized by integrating advanced technologies such as cyber-physical systems, the Internet of Things (IoT), cloud computing, and artificial intelligence with traditional manufacturing processes[68]. This approach enables real-time data collection, analysis, and decision-making, thereby enhancing the flexibility, efficiency, and responsiveness of production systems. The core of smart manufacturing lies in its ability to utilize data-driven models and predictive engineering to optimize operations, ensure sustainability, and facilitate resource sharing across manufacturing networks. As a key element of the next industrial revolution, smart manufacturing is poised to transform traditional production into highly automated, intelligent, and interconnected systems [110].AI and statistical techniques have significantly transformed the landscape of smart manufacturing, promising unprecedented efficiency, flexibility, and intelligence in industrial operations. At the heart of this transformation lies the capability of ML algorithms to analyze vast amounts of data, learn from it, and make informed decisions or predictions, leading to optimized processes and reduced downtimes. Integrating ML into manufacturing processes marks a pivotal shift towards more agile, smarter, and sustainable production systems. As highlighted in the document, machine learning-based anomaly detection plays a critical role in maintaining the integrity and performance of manufacturing systems. Anomaly Detection (AD), a process of identifying instances that deviate significantly from the norm, is essential for the early detection of potential failures, quality issues, or cybersecurity threats [36, 88]. Powered by ML, this early detection capability enables manufacturers to preemptively address issues, enhancing operational reliability and safeguarding against potential losses. Moreover, the evolution towards smart manufacturing is deeply intertwined with the concept of federated learning. This technique enables collaborative learning of a shared prediction model while keeping all training data on the device, effectively addressing concerns related to privacy, security, and data locality [138]. This approach not only democratizes the benefits of ML across various stakeholders in the manufacturing ecosystem but also opens new vistas for innovation and efficiency enhancement. In the era of Industry 4.0, where digitalization and interconnectivity define competitive advantage, the role of ML in smart manufacturing becomes even more pronounced. By harnessing the power of ML, manufacturers are not only able to optimize their operations but also drive toward a future where machines and humans collaborate more seamlessly. This collaboration is poised to unlock new levels of creativity, customization, and service excellence, ultimately realizing Industry 5.0's vision, where technology serves humanity in sustainable, resilient, and human-centric ways.

As we face this technological revolution, explainable artificial intelligence (XAI) becomes important. XAI ensures that the decisions made by ML models are transparent, understandable, and, most importantly, trustworthy. This trust is crucial for human operators who oversee and interact with these systems, ensuring that the integration of ML into manufacturing processes enhances efficiency and aligns with ethical standards and societal values [77]. Therefore, as smart manufacturing evolves, the synergy between ML, federated learning, and XAI will shape future factories and redefine the essence of industrial production in the digital age.

2.6.2 Industrial AI for Health and Wellbeing, Smart Healthcare

In the context of increasingly Smart healthcare, applying advanced technologies such as monitoring, anomaly detection, and classification has become critical in enhancing the quality of medical services and optimizing patient care processes. The advent of Artificial Intelligence (AI) in the healthcare sector represents a pivotal shift towards smarter, more efficient healthcare delivery systems. This transformation is primarily fueled by the integration of wearable technology and the Internet of Things (IoT), marking a significant leap from Industry 4.0 to Industry 5.0. This new era aims at optimizing resource efficiency, safety, and economic efficacy. Wearable IoT devices, in parallel with humans, optimize tasks and meet the evolving requirements of the new industrial era. The amalgamation of AI algorithms with IoT in wearable technologies, alongside advancements in sensor technology, has spearheaded significant innovations across various sectors, including manufacturing, healthcare, sports, etc., thereby enhancing the quality and accessibility of services [160, 162, 187, 111].

Many studies have utilized deep learning (DL) algorithms, such as Convolutional Neural Networks (CNN), Deep Belief Networks (DBN), Deep Neural Networks (DNN), and Multi-Layer Perceptrons (MLP), on the Pima Indian Diabetes (PID) dataset, which was collected in 1988. This data includes nine attributes and 768 records describing female patients. For this dataset, [191] achieved the highest accuracy of 76.30% from Naive Bayes among Decision Tree, Support Vector Machine (SVM). [104] used ensemble approach (90% of accuary) with explainable AI. [56] used Deep Neural Network (DNN), Support Vector Machine (SVM), and Random Forest (RF) for classification (around 96%). Most previous studies have been conducted on the PIMA dataset and have been successful with tabular data [100, 216]. However, a lack of studies uses a model-based-transformer architecture in predicting diabetes with tabular data. Recently, with the ubiquitous success of attention-based architecture, some studies have employed attention-like modules for tabular deep learning as well [86, 11, 193].

In the realm of healthcare, smart wearables, including blood pressure monitors, heart rate trackers, and various sensors, have made significant contributions to health monitoring and management. These devices support physicians in remotely monitoring patients' health conditions and enable individuals to proactively track their own health, facilitating the early detection of potential health issues. Moreover, applying AI and Deep Learning (DL) to analyze data from wearable devices opens new avenues for diagnosis and treatment, optimizes healthcare processes, and improves the quality of life for individuals. However, integrating AI into smart healthcare presents its own challenges. Issues such as data security, accuracy, latency in data processing, storage capacity, and battery life of devices pose significant hurdles. To address these challenges, Federated Learning (FL) has emerged as a practical solution, especially in enhancing privacy protection and optimizing the processing capabilities of wearable devices in healthcare applications. This approach enables collaborative model training across multiple devices while ensuring that sensitive data remains on the local device, thereby safeguarding patient privacy and enhancing the model's accuracy and efficiency [176, 265]. Despite the progress, design, security, and data management challenges remain critical areas for further research and development [251].

2.7 Motivation and Problem Statement

This section presents the motivation and problem statement for this Ph.D. thesis.

2.7.1 Motivation

As discussed above, the growing complexity of smart manufacturing and healthcare systems demands advanced techniques for monitoring, anomaly detection, and classification to maintain efficiency, reliability, and safety. Traditional rule-based and threshold-based methods struggle to manage high-dimensional data, dynamic environments, and real-time decision-making. Artificial Intelligence (AI) and statistical methods present powerful solutions by providing adaptive, data-driven insights, enabling early anomaly detection, and improving classification accuracy. However, challenges such as model interpretability, data heterogeneity, and real-time processing constraints limit the widespread application of these methods. In smart manufacturing, integrating machine learning with traditional monitoring approaches enhances real-time anomaly detection, predictive maintenance, and process optimization [171, 69]. Despite this, current models face difficulties with high-dimensional, noisy data and lack adaptability in rapidly changing environments. In healthcare, AI models aid in anomaly detection and disease classification but still encounter significant barriers, including data heterogeneity, privacy concerns, and the lack of model interpretability [179, 51, 35]. A unified approach that combines machine learning, statistical computing, and AI could significantly enhance monitoring, anomaly detection, and classification across both domains. However, scalability, generalizability, and real-time processing remain pressing limitations. This research aims to address these challenges by developing robust, AI-driven frameworks that integrate statistical methods, ultimately improving monitoring, early fault detection, and accurate classification in smart manufacturing and healthcare applications.

2.7.2 Problem Statement

Despite significant advancements in both statistical methodologies and machine learning, current systems in smart manufacturing and healthcare often operate in isolation, failing to fully leverage the complementary strengths of these approaches [59, 20, 228]. In smart manufacturing, traditional control charts and reliability models are limited in their ability to capture complex, non-linear patterns in data, while machine learning approaches face scalability and real-time processing challenges, particularly in dynamic environments where rapid fault detection is critical [59, 20]. In healthcare, centralized anomaly detection models are constrained by privacy concerns and the distributed nature of data, while many machine learning models lack interpretability, which undermines clinician trust and decision-making. The lack of integrated frameworks that combine advanced statistical computing with machine learning techniques results in suboptimal performance in both fields, hindering early fault detection, process optimization, and timely clinical interventions [20]. This highlights the urgent need for unified solutions to enhance anomaly detection in these complex, data-rich environments

2.8 Research objectives and questions

This section presents the research objectives and questions for this Ph.D. thesis.

2.8.1 Research objectives

To address these challenges, this research aims to develop and validate comprehensive frameworks that:

- Enhance industrial monitoring through the integration of statistical computing with control charts and reliability models.
- Leverage machine learning for robust classification and anomaly detection in smart manufacturing environments.
- Employ federated learning and explainable AI to create adaptive, privacy-preserving anomaly detection systems in smart healthcare.

By bridging these methodologies, the proposed work aims to make significant contributions to both industrial statistics and AI-driven health monitoring, thereby paving the way for more resilient, interpretable, and efficient systems in critical application areas.

2.8.2 Research questions

1. How can advanced statistical computing techniques be integrated with traditional industrial statistics to develop more robust control charts and reliability models for real-time process monitoring in manufacturing systems?

2. What machine learning strategies can be effectively employed for classification and anomaly detection in smart manufacturing environments, and how do these approaches compare with classical statistical methods in terms of accuracy, computational efficiency, and scalability?

3. How can explainable federated learning frameworks provide transparent, explainable AI solutions to enhance patient monitoring and overall health outcomes in smart healthcare systems?

2.9 Research Methodologies

This thesis examines the role of artificial intelligence (AI) and statistical methodologies in improving the reliability, efficiency, and predictive accuracy of complex systems. Monitoring techniques integrate statistical methods, machine learning models, and edge AI to analyze real-time data and detect deviations. Anomaly detection leverages unsupervised learning, supervised classification, and hybrid approaches to identify irregular patterns, improving system performance and security. Classification techniques, spanning traditional machine learning to deep learning models, facilitate accurate decision-making and forecasting, with an increasing emphasis on explainable AI for transparency and trust. Despite significant advancements, challenges remain in data quality, scalability, and ethical considerations. This Ph.D. thesis aims to address these issues by developing novel methodologies that enhance interpretability, optimize computational efficiency, and promote responsible AI deployment in real-world applications.

2.10 The organization of the thesis

The next part of this Ph.D. thesis is structured into four chapters. Chapter 3 explores statistical computing and industrial statistics, covering control charts, reliability analysis, and probabilistic modeling. Chapter 4 focuses on classification and anomaly detection using machine learning, with applications in smart manufacturing, predictive maintenance, and quality assurance. Chapter 5 delves into adaptive anomaly detection and explainability through federated learning, emphasizing applications in health, well-being, and smart healthcare. Finally, Chapter 6 summarizes key contributions, discusses challenges such as data quality and model interpretability, and outlines future research directions. This structure provides comprehensive contributions of AI and statistical methodologies for monitoring, anomaly detection, and classification across various domains.

2.11 Concluding remarks

The integration of artificial intelligence (AI) and statistical methods in monitoring, anomaly detection, and classification is revolutionizing critical domains, including smart manufacturing and healthcare. These approaches enhance system reliability, optimize efficiency, and improve decision-making accuracy by providing robust data-driven insights. The combination of Statistical Computing, Industrial Statistics, and Industrial AI ensures precise process monitoring and early detection of anomalies, mitigating risks and preventing failures. In healthcare, these methodologies contribute to real-time patient monitoring, early diagnosis, and personalized treatment, leading to improved patient outcomes and operational efficiency. In smart manufacturing, they enable predictive maintenance, quality control, and adaptive automation, reducing downtime and maximizing productivity. As these fields continue to evolve, the integration of AI-driven analytics with domain-specific statistical models will be crucial in advancing the next generation of intelligent monitoring systems. There are many challenges to be addressed, as analyzed in the above sections. Thus, as contributions, we focus on enhancing the interpretability, scalability, and real-time adaptability of these models to address complex and dynamic environments. By leveraging these advancements, industries can achieve greater resilience, sustainability, and precision in decision-making. We will present the major contributions in turn in the following chapters.

Chapter 3

Statistical Computing and Industrial Statistics with the applications in Control Charts and Reliability

The content of this chapter is based on the following publications, in which I am a co-author:

- K.D. Tran, H.D. Nguyen, T.H. Nguyen, K.P. Tran (2021). "Design of a variable sampling interval exponentially weighted moving average median control chart in the presence of measurement errors" *Quality and Reliability Engineering International*, vol. 37, pp. 374-390. http://dx.doi.org/10.1002/qre.2726

- K.D. Tran, A.A. Nadi, T.H. Nguyen, K.P. Tran (2021). "One-sided Shewhart control charts for monitoring the ratio of two normal variables in short production runs" *Journal of Manufacturing Processes*. Elsevier, vol. 69, pp. 273–289. http://dx.doi.org/10.1016/j.jmapro.2021.07.031

- H.D. Nguyen, A.A. Nadi, K.D. Tran*, P. Castagliola, G. Celano, K.P. Tran (2023). "The Shewhart-type RZ control chart for monitoring the ratio of autocorrelated variables" *International Journal of Production Research*. Taylor & Francis, pp. 6746-6771. http://dx.doi.org/10.1080/00207543.2022.2137594

- A.A. Nadi, B.S. Gildeh, J. Kazempoor, K.D. Tran, K.P. Tran (2023). “Cost-effective optimization strategies and sampling plan for Weibull quantiles under type-II censoring” *Applied Mathematical Modelling*. Elsevier, pp. 16–31. http://dx.doi.org/10.1016/j.apm.2022.11.004

- H.D. Nguyen, K.P. Tran, K.D. Tran(2021). "The effect of measurement errors on the performance of the Exponentially Weighted Moving Average control charts for the Ratio of Two Normally Distributed Variables" *European Journal of Operational Research*. https://doi.org/10.1016/j.ejor.2020.11.042

- Q.T. Nguyen, V. Giner-Bosch, K.D. Tran, C. Heuchenne, K.P. Tran (2021). “One-sided variable sampling interval EWMA control charts for monitoring the multivariate coefficient of variation in the presence of measurement errors” *The International Journal of Advanced Manufacturing Technology*. Springer London, vol. 115, pp. 1821-1851. https://link.springer.com/article/10.1007/s00170-021-07138-8

- T.T.V. Nguyen, T.H. Nguyen,K.D. Tran, C. Heuchenne, K.P. Tran (2023). “Monitoring the Ratio of Two Normal Variables and Compositional Data: A Literature Review and Perspective.” In *Advances of Computational Techniques for Smart Manufacturing in the Industry 5.0: Methods and Applications*, CRC Press. Accepted. https://hal.science/hal-04331557/

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, T.H. Truong, K.H. Phung, L.H. Nguyen, T.T.N. Le, K.P. Tran (2019). “One-Sided Synthetic-RZ control charts: a new method for anomaly detection”, Proceedings of the *6th NAFOSTED Conference on Information and Computer Science (NICS)*, IEEE, pp. 262-267. http://dx.doi.org/10.1109/NICS48868.2019.9023851

3.1 Introduction

Statistical Computing and Industrial Statistics, particularly in Control Charts and Reliability, are widely utilized in industrial applications to ensure process stability and identify deviations in manufacturing workflows [142]. Among the Statistical Process Control (SPC) tools, control charts are vital for distinguishing between common and special causes of variation, enabling practitioners to implement corrective actions when necessary [237, 127, 129, 178]. Traditional control charts, such as the Exponentially Weighted Moving Average (EWMA) chart, are effective for detecting small to moderate process shifts but may show limited sensitivity to larger variations [129]. Enhancements, such as Variable Sampling Intervals (VSI) schemes, have been proposed to improve detection performance [184, 26].

Control charts remain central to modern quality control, with applications extending to anomaly detection, fault detection, and reliability assessment [36]. The increasing complexity of industrial processes, particularly with the integration of Industrial Internet of Things (IIoT) technologies, has introduced challenges such as autocorrelation and cross-correlation in the data, requiring advanced statistical techniques for effective monitoring [106, 9, 102].

This study focuses on the phase II Shewhart-type RZ control chart for monitoring the ratio of two standard variables modeled using a bivariate vector autoregressive (VAR) time series. The VAR model captures both autocorrelation and cross-correlation, making it particularly suitable for high-frequency industrial data [24, 87]. The research aims to assess how the VAR model parameters influence control chart performance, providing valuable insights for robust industrial monitoring.

Specifically, the study evaluates the Phase II Shewhart-type RZ control chart under the assumption of a first-order bivariate VAR model for two quality characteristics. By analyzing the impact of VAR parameters on statistical performance, the research offers guidelines for selecting optimal control chart settings. A case study utilizing real-world furnace process data demonstrates the practical application of the proposed monitoring approach. The contributions in this chapter are to obtain the objective below:

- Objective 1.1: Develop advanced control charts by integrating sophisticated statistical computing methods with traditional industrial statistics to enhance real-time process monitoring in manufacturing environments.

- Objective 1.2: Formulate and validate reliability models that incorporate these advanced statistical techniques to improve early fault detection and ensure process stability.

- Objective 1.3: Implement and test the developed methods using real-world manufacturing data to evaluate improvements in accuracy and responsiveness over conventional methods.

3.2 Contributions about ratio control charts in the presence of autocorrelation

A large number of control charts monitoring the ratio have been investigated in the literature, assuming independent normal observations of the two quality characteristics. In practice, due to the high frequency of sensor data collection, both autocorrelation and cross-correlation between consecutive observations can exist for X and Y. They should be modeled to protect against inflation in the false alarm rate when implementing a control chart for monitoring the ratio $\frac{X}{Y}$. In this section, we address this problem by investigating the performance of the Phase II Shewhart-type RZ control chart, which monitors the ratio of two normal variables. The relationship between these variables is captured by a bivariate time series autoregressive model, VAR(1), that also accounts for the cross-correlation between the two quality characteristics. With the numerical study, we discuss how the design and the statistical performance of the Shewhart-type RZ control chart change with the VAR(1) model's parameters. We also provide an example to illustrate the use of the Shewhart-type RZ control chart with a bivariate time series of observations in a furnace process.

3.2.1 The Vector Autoregressive VAR(1) model for the sample of the ratio

The vector autoregressive VAR(1) model is one of the commonly used models to fit multivariate time series observations. Here, we consider the bivariate case, where two time series (i.e., the autocorrelated quality characteristics) X_t and Y_t can be modeled by a VAR(1) model. With this model for bivariate time series, each quality characteristic observation at time t not only linearly depends on the observation at time $t-1$ (autocorrelation), but it can also be linearly dependent on the observation of the other variable collected at time $t-1$, (cross-correlation). According to the VAR(1) model, the vector of the observations of the two quality characteristics at time t, say $\mathbf{W}_t = (X_t, Y_t)^\intercal$, depends on $\mathbf{W}_{t-1}$ through the following equation:

$$\mathbf{W}_t = \boldsymbol{\mu}_\mathbf{W} + \boldsymbol{\Phi}(\mathbf{W}_{t-1} - \boldsymbol{\mu}_\mathbf{W}) + \boldsymbol{\varepsilon}_t, \quad t = 0, \pm 1, \pm 2, ... \tag{3.1}$$

where

$$\boldsymbol{\mu}_{\mathbf{W}} = \begin{pmatrix} \mu_X \\ \mu_Y \end{pmatrix}$$

is the mean vector of $\mathbf{W}_t$,

$$\boldsymbol{\Phi} = \begin{pmatrix} \Phi_{XX} & \Phi_{XY} \\ \Phi_{YX} & \Phi_{YY} \end{pmatrix}$$

is a (2×2) correlation matrix that accounts for both autocorrelation, (Φ_{XX} and Φ_{YY}), and cross-correlation, (Φ_{XY} and Φ_{YX}), between X and Y; $\boldsymbol{\varepsilon}_t$ is the bivariate normal random noise with mean vector $\boldsymbol{\mu}_{\varepsilon} = \mathbf{0}$ and variance-covariance matrix

$$\boldsymbol{\Sigma}_{\varepsilon} = \begin{pmatrix} \sigma^2_{e_X} & \sigma_{e_{XY}} \\ \sigma_{e_{XY}} & \sigma^2_{e_Y} \end{pmatrix} = \begin{pmatrix} \sigma^2_{e_X} & \rho\sigma_{e_X}\sigma_{e_Y} \\ \rho\sigma_{e_X}\sigma_{e_Y} & \sigma^2_{e_Y} \end{pmatrix}.$$

By these notations, the equation. (3.1) can also be rewritten as the following system of two equations

$$X_t = \mu_X + \Phi_{XX}X_{t-1} + \Phi_{XY}Y_{t-1} + \epsilon_{X_t}$$
$$Y_t = \mu_Y + \Phi_{YX}X_{t-1} + \Phi_{YY}Y_{t-1} + \epsilon_{Y_t}.$$

Based on the above equations, Φ_{XY} shows the linear dependence of X_t on Y_{t-1} in the presence of X_{t-1}. Φ_{YX} can also be interpreted in the same way. Hence, the univariate time series X_t and Y_t are not cross-correlated if $\Phi_{XY} = \Phi_{YX} = 0$. From (3.1), [177] showed that the cross-covariance matrix $\boldsymbol{\Sigma}_{\mathbf{W}}$ of $\mathbf{W}_t$ is the solution to the equation $\boldsymbol{\Sigma}_{\mathbf{W}} = \boldsymbol{\Phi}\boldsymbol{\Sigma}_{\mathbf{W}}\boldsymbol{\Phi}^{\intercal} + \boldsymbol{\Sigma}_{\varepsilon}$. Then, it can be shown that

$$\mathrm{Vec}(\boldsymbol{\Sigma}_{\mathbf{W}}) = (\mathbf{I}_4 - \boldsymbol{\Phi} \otimes \boldsymbol{\Phi})^{-1}\mathrm{Vec}(\boldsymbol{\Sigma}_{\varepsilon}), \tag{3.2}$$

where $\mathbf{I}_p$ is the $p \times p$ identity matrix, $\otimes$ is the Kronecker product and Vec is the operator that transforms a matrix into a one-column vector by stacking its columns. Using (3.2), the cross-covariance matrix of the VAR(1) model in

(3.1) can be obtained as

$$\begin{aligned}\boldsymbol{\Sigma}_{\mathbf{W}} &= \begin{pmatrix} \sigma_X^2 & \sigma_{XY} \\ \sigma_{XY} & \sigma_Y^2 \end{pmatrix} \\ &= \begin{pmatrix} \frac{\Delta_{11}\sigma_{eX}^2+(\Delta_{12}+\Delta_{13})\sigma_{eXY}+\Delta_{14}\sigma_{eY}^2}{\Delta} & \frac{\Delta_{31}\sigma_{eX}^2+(\Delta_{32}+\Delta_{33})\sigma_{eXY}+\Delta_{34}\sigma_{eY}^2}{\Delta} \\ \frac{\Delta_{21}\sigma_{eX}^2+(\Delta_{22}+\Delta_{23})\sigma_{eXY}+\Delta_{24}\sigma_{eY}^2}{\Delta} & \frac{\Delta_{41}\sigma_{eX}^2+(\Delta_{42}+\Delta_{43})\sigma_{eXY}+\Delta_{44}\sigma_{eY}^2}{\Delta} \end{pmatrix}, \end{aligned} \tag{3.3}$$

where the quantities $\Delta_{s,k}$ for $s, k = 1, 2, 3, 4$ are given in Appendix A of [148].

In practice, the VAR(1) model parameters $\boldsymbol{\mu}, \boldsymbol{\Phi}$, and $\boldsymbol{\Sigma}_\varepsilon$ should be estimated from the Phase I observations. Several methods have been presented in the literature to obtain these estimated parameters, including the least squares (LS), maximum likelihood (ML), and Bayesian methods. [214] (Chapt. 2) provided a detailed discussion about the theoretical aspects of these estimation methods and studied their key properties. They showed that the Bayesian and LS methods produce close estimates, and under some conditions, the ML estimates are asymptotically equivalent to the LS ones. They also wrote several R functions included in the `MTS` package available in R for multivariate time series analysis. Other statistical software, such as SAS, with the `ARIMA` procedure, can also be used to perform estimation of VAR models, [148].

3.2.2 The implementation of the Shewhart-type RZ control chart with VAR(1) observations

Let us consider a process where a practitioner wants to monitor the ratio between two autocorrelated, and possibly cross-correlated, quality characteristics X and Y. At each inspection, n observations $(X_{i,j}, Y_{i,j})$, for $i = 1, ...,$ and $j = 1, ..., n$ are collected. Similar to [208], we suggest to monitor the ratio $\bar{Z}_i$ statistic defined as follows:

$$\bar{Z}_i = \frac{\bar{X}_i}{\bar{Y}_i} = \frac{\sum_{j=1}^{n} X_{i,j}}{\sum_{j=1}^{n} Y_{i,j}} \tag{3.4}$$

at each time $i = 1, 2, \ldots$. Let $\rho = \rho_0$ and $z = \frac{\mu_X}{\mu_Y} = z_0$ denote the coefficient of correlation between the two normal variables X and Y and the mean ratio when the process is in control, respectively. It is well known that the distribution of the ratio of two normal random variables has no moments. Thus, the control limits of the Shewhart-RZ control chart monitoring $\bar{Z}_i$ should be defined as probability control limits. Denoting as α the desired false alarm rate (FAR) for the control chart, the lower control limit (LCL), and the upper control limit (UCL) of the Shewhart-RZ are obtained as follows [148]:

$$LCL = F_Z^{-1}\left(\tfrac{\alpha}{2}\middle|\, \gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right), \tag{3.5}$$
$$UCL = F_Z^{-1}\left(1-\tfrac{\alpha}{2}\middle|\, \gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right), \tag{3.6}$$

where $\gamma_{\bar{X}}$, $\gamma_{\bar{Y}}$, $\bar{\omega}$, and $\bar{\rho}$ should be computed from mean vector $\boldsymbol{\mu}_{\overline{\mathbf{W}}}$ and the cross-covariance matrix $\boldsymbol{\Sigma}_{\overline{\mathbf{W}}}$ of the distribution of the bivariate sample mean vector $\bar{W}_i = (\bar{X}_i, \bar{Y}_i)$. It is proven in Appendix B that $\boldsymbol{\mu}_{\overline{\mathbf{W}}} = \boldsymbol{\mu}_{\mathbf{W}} = (\mu_X, \mu_Y)^\intercal$ and

$$\begin{aligned}\boldsymbol{\Sigma}_{\overline{\mathbf{W}}} &= \frac{1}{n}\left[\boldsymbol{\Sigma}_{\mathbf{W}}\left(\mathbf{I}_2 + \Lambda(\boldsymbol{\Phi}^\intercal) - \frac{1}{n}\Pi(\boldsymbol{\Phi}^\intercal)\right) + \left(\Lambda(\boldsymbol{\Phi}) - \frac{1}{n}\Pi(\boldsymbol{\Phi})\right)\boldsymbol{\Sigma}_{\mathbf{W}}^\intercal\right] \\ &= \begin{bmatrix} \sigma^2_{\bar{X}} & \bar{\rho}\sigma_{\bar{X}}\sigma_{\bar{Y}} \\ \sigma_{\bar{X}}\sigma_{\bar{Y}} & \sigma^2_{\bar{Y}} \end{bmatrix}\end{aligned} \tag{3.7}$$

where

$$\begin{aligned}\Lambda(\boldsymbol{\Phi}) &= (\boldsymbol{\Phi} - \boldsymbol{\Phi}^n)(\mathbf{I}_2 - \boldsymbol{\Phi})^{-1} \\ \Pi(\boldsymbol{\Phi}) &= (\boldsymbol{\Phi}^{-1} - \mathbf{I}_2)^{-1}\Big((\mathbf{I}_2 - \boldsymbol{\Phi}^{n-1})(\mathbf{I}_2 - \boldsymbol{\Phi})^{-1} - (n-1)\boldsymbol{\Phi}^{n-1}\Big).\end{aligned}$$

Thus, to obtain LCL and UCL in (3.5) and (3.6), one can calculate the coefficients of variations $\gamma_{\bar{X}}$ and $\gamma_{\bar{Y}}$, the coefficient of correlation $\bar{\rho}$ between $\bar{X}_i$ and $\bar{Y}_i$, and the standard-deviation ratio $\bar{\omega}$ as

$$\gamma_{\bar{X}} = \frac{\sigma_{\bar{X}}}{\mu_X}, \quad \gamma_{\bar{Y}} = \frac{\sigma_{\bar{Y}}}{\mu_Y}, \quad \bar{\rho} = \frac{\sigma_{\bar{X}\bar{Y}}}{\sigma_{\bar{X}}\sigma_{\bar{Y}}}, \quad \bar{\omega} = \frac{\sigma_{\bar{X}}}{\sigma_{\bar{Y}}}, \tag{3.8}$$

respectively. Here, we assume that the coefficient of variation remains constant for each variable X and Y, i.e., $\sigma_{e_{X,i}} = \gamma_X\mu_{X,i}$ and $\sigma_{e_{Y,i}} = \gamma_Y\mu_{Y,i}$ for every $i \geq 1$. This implies that the standard deviation of each sample changes proportionally to its mean. There are several quality characteristics in practice (such as weights, tensile strengths, and linear dimensions) that have a dispersion proportional to the population mean. Thus, if we define $z = \frac{\mu_X}{\mu_Y} = z_0$, then the in-control ratio $\bar{\omega}$ can also be rewritten as

$$\bar{\omega} = \frac{\gamma_{\bar{X}}}{\gamma_{\bar{Y}}} \times \frac{\mu_X}{\mu_Y} = \frac{\gamma_{\bar{X}}}{\gamma_{\bar{Y}}} \times z_0. \tag{3.9}$$

When the process runs in the out-of-control state, the in-control ratio z_0 is shifted to $z_1 = \tau \times z_0$, where $\tau > 0$ is the shift size, and the in-control coefficient of correlation $\rho = \rho_0$ is shifted to $\rho = \rho_1$. According to the discussion in [115], we can assume that the units within a sample are collected close together in time and at the same time, the length h The sampling interval is large enough to eliminate any dependence between successive values of the sample ratio statistics $\bar{Z}_1, \bar{Z}_2, \ldots$. That is to say, the observations in each subgroup of size n follow a VAR(1) model, but the ratio statistics $Z_i, i = 1, 2, \ldots$ are independent random variables. Under the assumption of known (or perfect estimation of) distribution parameters, the run length of the Shewhart-RZ control chart follows a geometric distribution with probability of *success* $p = 1 - \beta$, where

$$\beta = F_Z\left(UCL \,|\gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right) - F_Z\left(LCL \,|\gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right), \tag{3.10}$$

denotes the probability that at any inspection following the occurrence of the assignable cause, the control chart does not trigger any signal. The out-of-control parameters $\gamma_{\bar{X}}$, $\gamma_{\bar{Y}}$, $\bar{\omega}$, $\bar{\rho}$ in (3.10) are calculated based on equation (3.8) or equations (3.14)–(3.17) but with $\rho = \rho_1$ and $z = z_1$. Then, the out-of-control average run length (ARL_1) and the standard deviation of the run length (SDRL) of the Shewhart-RZ chart are computed as

$$ARL_1 = \frac{1}{1-\beta} \tag{3.11}$$

$$SDRL = \frac{\sqrt{\beta}}{1-\beta} \tag{3.12}$$

Consider a case where X and Y are not cross-correlated and the matrix $\mathbf{\Phi}$ is diagonal, i.e. $\Phi_{XY} = \Phi_{YX} = 0$, we aim to provide easier-to-use mathematical formulas for $\mathbf{\Sigma_W}, \mathbf{\Sigma_{\overline{W}}}, \gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\rho}$, and $\bar{\omega}$ when $n > 1$ observations are collected within each sample. The new results are helpful for practitioners to avoid time-consuming computations in the absence of cross-correlation. There are many examples in the SPM literature where the observations of one variable at a time $i, i = 2, 3, \ldots$ are not dependent on the observations of the other variable at time $i-1$, see, for example, [115]. As proved in [115], if $\Phi_{XY} = \Phi_{YX} = 0$ then, using (3.2), the cross-covariance matrix $\mathbf{\Sigma_W}$ of $\mathbf{W}_i$ is equal to

$$\begin{aligned}
\mathbf{\Sigma_W} &= \begin{pmatrix} \sigma_X^2 & \sigma_{XY} \\ \sigma_{XY} & \sigma_Y^2 \end{pmatrix} \\
&= \begin{pmatrix} (1-\Phi_{XX}^2)^{-1}\sigma_{eX}^2 & (1-\Phi_{XX}\Phi_{YY})^{-1}\sigma_{eXY} \\ (1-\Phi_{XX}\Phi_{YY})^{-1}\sigma_{eXY} & (1-\Phi_{YY}^2)^{-1}\sigma_{eY}^2 \end{pmatrix}. \qquad (3.13)
\end{aligned}$$

At time $i = 1, 2, \ldots$, the sample mean vector $\overline{\mathbf{W}}_i = (\bar{X}_i, \bar{Y}_i)$ is also a bivariate normal random vector with mean vector $\boldsymbol{\mu}_\mathbf{W}$ and cross-covariance matrix

$$\mathbf{\Sigma}_{\overline{\mathbf{W}}} = \begin{pmatrix} \sigma_{\bar{X}}^2 & \bar{\rho}\sigma_{\bar{X}}\sigma_{\bar{Y}} \\ \bar{\rho}\sigma_{\bar{X}}\sigma_{\bar{Y}} & \sigma_{\bar{Y}}^2 \end{pmatrix},$$

where

$$\begin{aligned}
\sigma_{\bar{X}}^2 &= \frac{\sigma_{e_X}^2}{n(1-\Phi_{XX}^2)}\left(1 + \frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k\right), \\
\sigma_{\bar{Y}}^2 &= \frac{\sigma_{e_Y}^2}{n(1-\Phi_{YY}^2)}\left(1 + \frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k\right), \\
\bar{\rho}\sigma_{\bar{X}}\sigma_{\bar{Y}} &= \frac{\rho\sigma_{e_X}\sigma_{e_Y}}{n(1-\Phi_{XX}\Phi_{YY})}\left(1 + \frac{1}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k + \frac{1}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k\right).
\end{aligned}$$

From these quantities, it is straightforward to obtain the coefficients of variations $\gamma_{\bar{X}} = \frac{\sigma_{\bar{X}}}{\mu_X}$ and $\gamma_{\bar{Y}} = \frac{\sigma_{\bar{Y}}}{\mu_Y}$ of $\bar{X}_i$ and $\bar{Y}_i$ as

$$\gamma_{\bar{X}} = \frac{\sigma_{e_X}\sqrt{1 + \frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k}}{\sqrt{n(1-\Phi_{XX}^2)}\mu_X} \qquad (3.14)$$

$$\gamma_{\bar{Y}} = \frac{\sigma_{e_Y}\sqrt{1 + \frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k}}{\sqrt{n(1-\Phi_{YY}^2)}\mu_Y}. \qquad (3.15)$$

Similarly, the coefficient of correlation $\bar{\rho}$ between $\bar{X}_i$ and $\bar{Y}_i$ is defined as

$$\bar{\rho} = \frac{\rho\sqrt{(1-\Phi_{XX}^2)(1-\Phi_{YY}^2)}\left(1+\frac{1}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k+\frac{1}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k\right)}{(1-\Phi_{XX}\Phi_{YY})\sqrt{\left(1+\frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k\right)\left(1+\frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k\right)}}, \tag{3.16}$$

and the standard-deviation ratio $\bar{\omega} = \frac{\sigma_{\bar{X}}}{\sigma_{\bar{Y}}}$ is

$$\bar{\omega} = \frac{\sigma_{e_X}\sqrt{1-\Phi_{YY}^2}}{\sigma_{e_Y}\sqrt{1-\Phi_{XX}^2}} \times \sqrt{\frac{1+\frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{XX}^k}{1+\frac{2}{n}\sum_{k=1}^{n-1}(n-k)\Phi_{YY}^k}}.$$

Concerning $\bar{\omega}$, it is important to note that if we let $z = \frac{\mu_X}{\mu_Y}$, it can also be rewritten as

$$\bar{\omega} = \frac{\gamma_{\bar{X}}}{\gamma_{\bar{Y}}} \times \frac{\mu_X}{\mu_Y} = \frac{\gamma_{\bar{X}}}{\gamma_{\bar{Y}}} \times z. \tag{3.17}$$

Now, the LCL and UCL in (3.5) and (3.6) can be recalculated based on equations (14)-(17). Finally, we summarize all the needed steps to estimate the control limits of the Shewhart-RZ control chart and implement it to perform online monitoring:

Algorithm 2: Shewhart-RZ Control Chart Algorithm for Estimating Control Limits and Online Monitoring.

Input:

- A Phase I dataset of size m with observations of the quality characteristics X and Y:

$$\mathbf{D}_{PhaseI} = \{\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m; \;\; \mathbf{X}_i = [X_i^{(1)}, X_i^{(2)}] \in \mathbb{R}^2\}.$$

- VAR(1) model parameters: $\boldsymbol{\mu}_{\bar{\mathbf{W}}}, \boldsymbol{\Phi}, \boldsymbol{\Sigma}_{\boldsymbol{\epsilon}}, \boldsymbol{\Sigma}_{\bar{\mathbf{W}}}$.
- Target ARL (Average Run Length) and FAR (False Alarm Rate): ARL_0, $\alpha = \frac{1}{ARL_0}$.
- RZ distribution parameters: $\gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\rho}, \bar{\omega}$.
- Sample size n for monitoring in Phase II.

Output:

- Control limits (LCL, UCL) for the Shewhart-RZ control chart.
- Out-of-control signals when $\bar{Z}_i < LCL$ or $\bar{Z}_i > UCL$.

- A control chart reporting in-control or out-of-control status based on the calculated ratios.

- **Phase I**

Step 1 Selects a Phase I dataset of size m (for example $m = 100$ observations of the two quality characteristics X and Y) to carry out a process stability study.

Step 2 Perform a multivariate time series study on the individual (X_t, Y_t) observations for $t = 1, ..., m$ to check that the VAR(1) is a suitable time series model based on the investigation of the sample ACF (autocorrelation function), PACF (partial autocorrelation function), and CCF (cross-correlation function).

Step 3 Estimate the VAR(1) parameters with the function VAR in the MTS package available in the R software.

Step 4 Check the normality of the residuals using a normal probability plot and an Anderson-Darling test.

Step 5 Investigate the stability of the residuals by using a bivariate control chart for individual observations.

Step 6 Set a sample size n such that the ratios are uncorrelated, even if the observations within each sample are VAR(1). The decision about the sample size is based on the sample ACF and PACF investigation for the Phase I ratios obtained with different values of n.

Step 7 Calculate the elements $\gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\rho}$, and $\bar{\omega}$ of $F_Z^{-1}(\cdot)$ based on eqns. (3.8) and (3.9) if Φ_{XY} and/or Φ_{YX} are non-zero, and based on eqns. (3.14), (3.15), (3.16), and (3.17) if $\Phi_{XY} = \Phi_{YX} = 0$.

Step 8 Set a target in-control average run length ALR_0 (for example $ARL_0 = 200$) and calculate its corresponding FAR $\alpha = \frac{1}{ARL_0}$.

Step 9 Compute the control limits (LCL, UCL) from eqns. (3.5) and (3.6).

Step 10 Split the Phase I dataset into s samples of size n such that $m = s * n$ and calculate the sample means $\bar{X}_i$ and $\bar{Y}_i$ and then the sample ratios $\bar{Z}_i$ for each sample $i = 1, 2, ..., s$.

Step 11 Plot the sample ratios $\bar{Z}_i$ on the control chart.

Step 12 If $LCL \leq \bar{Z}_i \leq UCL$ for all i, i.e., the Phase I dataset is stable, fix the control limits LCL and UCL and go to Phase II. Otherwise, if there are some out-of-control signals, remove the samples related to the signal conditions from the Phase I dataset and repeat Steps 2-11.

- **Phase II**

Step 1 Let the following parameters be the inputs to the algorithm.

- A prefixed sample size n (for example $n = 5$).
- A target ARL_0 and its corresponding FAR α such that $\alpha = \frac{1}{ARL_0}$ (for example $ARL_0 = 200$ and then $\alpha = 0.05$).
- The estimated VAR(1) model parameters $(\boldsymbol{\mu}_{\bar{\mathbf{W}}}, \boldsymbol{\Phi}, \boldsymbol{\Sigma}_{\boldsymbol{\epsilon}}, \boldsymbol{\Sigma}_{\bar{\mathbf{W}}})$.
- The calculated RZ distribution parameters $(\gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\rho}_0, \bar{\omega})$.

Step 2 Given the inputs in Step 1, solve the following equations to calculate the control limits LCL and UCL such that the average run length (ARL) of the control chart when the process is in-control is equal to ALR_0, i.e., $ARL = ARL_0$,

$$LCL = F_Z^{-1}\left(\tfrac{\alpha}{2}\middle|\, \gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right),$$
$$UCL = F_Z^{-1}\left(1 - \tfrac{\alpha}{2}\middle|\, \gamma_{\bar{X}}, \gamma_{\bar{Y}}, \bar{\omega}, \bar{\rho}\right),$$

where $F_Z^{-1}\left(\cdot|\gamma_X, \gamma_Y, \omega, \rho\right)$ is given in .

Step 3 Collect n observations at each inspection.

Step 4 Calculate the sample means $\bar{X}_i$ and $\bar{Y}_i$ and the sample ratios $\bar{Z}_i$ for each sample $i = 1, 2, ..., s$.

Step 5 Declare an out-of-control signal if $\bar{Z}_i < LCL$ or $\bar{Z}_i > UCL$. Otherwise, declare an in-control condition.

Without loss of generality, we assume that $z_0 = 1$. We also suppose that X and Y are not cross-correlated and the matrix $\boldsymbol{\Phi}$ is diagonal, i.e. $\Phi_{XY} = \Phi_{YX} = 0$. It allows reducing the bivariate stationary conditions to the simpler univariate stationary conditions for each variable, which has already been stated by [115]. The in-control ARL is set at $ARL_0 = 200$, corresponding to the false alarming rate $\alpha = 0.005$. In this study, we also assume $n \in \{2, 5, 7, 10, 15\}$, $\gamma_X \in \{0.01, 0.2\}$, $\gamma_Y \in \{0.01, 0.2\}$, $\rho_0 \in \{-0.9, -0.4, 0, 0.4, 0.9\}$, and $\Phi_{XX}, \Phi_{YY} \in \{0.1, 0.7\}$.

The effect of Φ_{XX} and Φ_{YY} on the overall performance of the Shewhart-RZ control chart in the presence of autocorrelation is displayed in Figure 3.1 ($\rho_0 = \rho_1 = -0.9$) and Figure 3.2 ($\rho_0 = -0.4$ and $\rho_1 = -0.8$) with the $EARL$ values for two possibilities of Ω, including $\Omega = \Omega_D = [0.9, 1)$ (decreasing case, denoted as (D)) and $\Omega = \Omega_I = (1, 1.1]$ (increasing case, denoted as (I)). We also consider several values of Φ_{XX} and Φ_{YY} as $\Phi_{XX} \in \{0.1, 0.2, \ldots, 0.7\}$

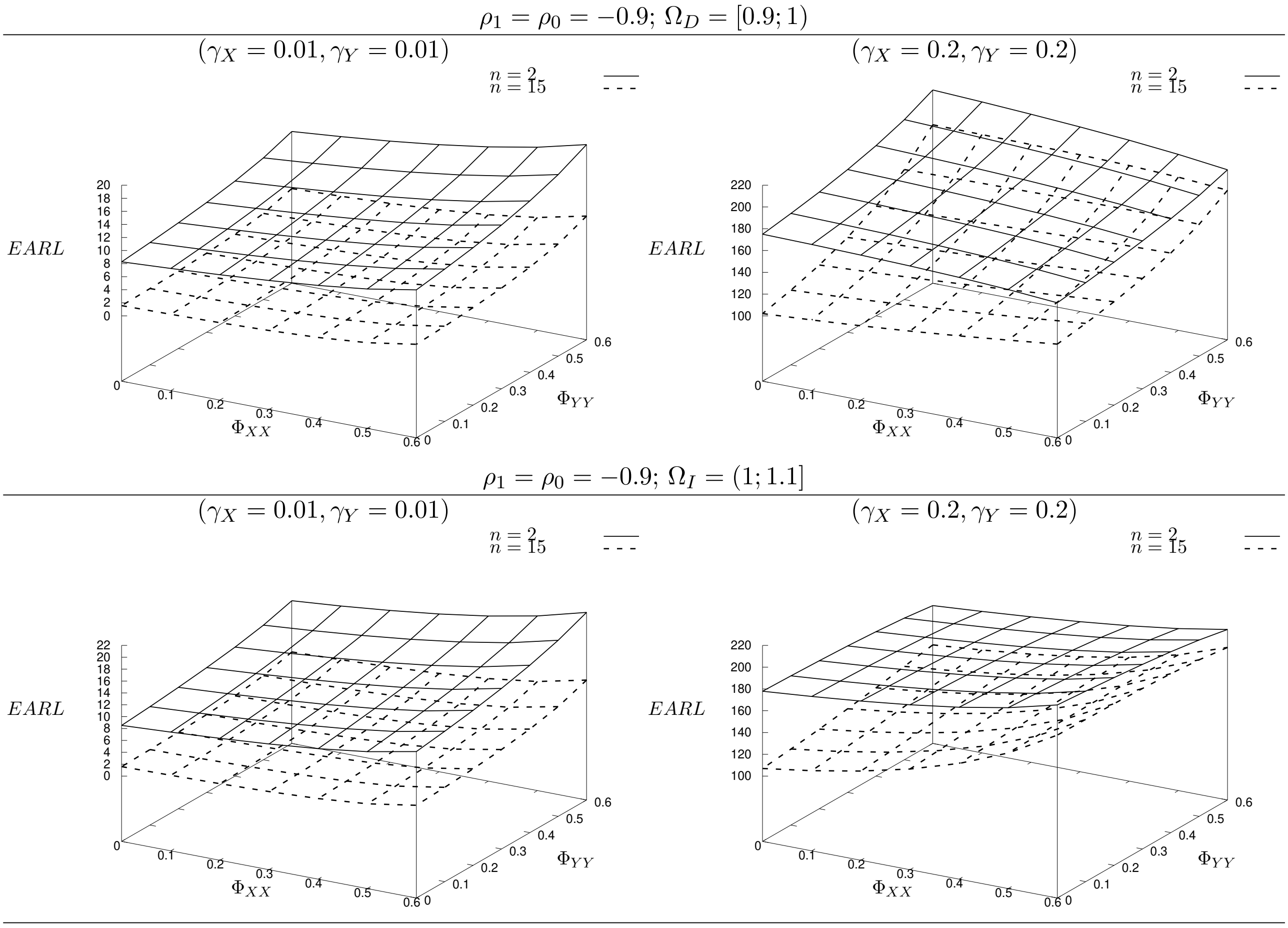


FIGURE 3.1: The effects of Φ_{XX} and Φ_{YY} on the overall performance of the Shewhart-RZ control in the presence of autocorrelation chart for $n \in \{2, 15\}$, $\gamma_X \in \{0.01, 0.2\}$, $\gamma_Y \in \{0.01, 0.2\}$, $\gamma_X = \gamma_Y$, $\rho_0 = \rho_1 = -0.9$ and $ARL_0 = 200$.

and $\Phi_{YY} \in \{0.1, 0.1, 0.2, \ldots, 0.7\}$. The values of other parameters are presented in the caption of each figure. In general, the obtained values of $EARL$ in these figures show a similar trend of the negative effect of Φ_{XX} and Φ_{YY} (representing the autocorrelation between observations) on the overall performance of the Shewhart-RZ chart as the specific shift size cases. In most cases, the larger the values of (Φ_{XX},Φ_{YY}), the larger the values of $EARL$, namely the slower the Shewhart-RZ control chart in detecting the out-of-control conditions. For example, in Figure 3.1 with $n = 15$, $\Omega = [0.9, 1)$, $\rho_0 = \rho_1 = -0.9$, $\gamma_X = \gamma_Y = 0.01$, we have $EARL = 1.87$ for $\Phi_{XX} = \Phi_{YY} = 0.1$, $EARL = 4.71$ for $\Phi_{XX} = \Phi_{YY} = 0.5$, and $EARL = 6.52$ for $\Phi_{XX} = \Phi_{YY} = 0.7$. These values are all larger than $EARL = 1.4$ for $\Phi_{XX} = \Phi_{YY} =$ (the process is free of autocorrelation) as presented in [32] (Table 6).

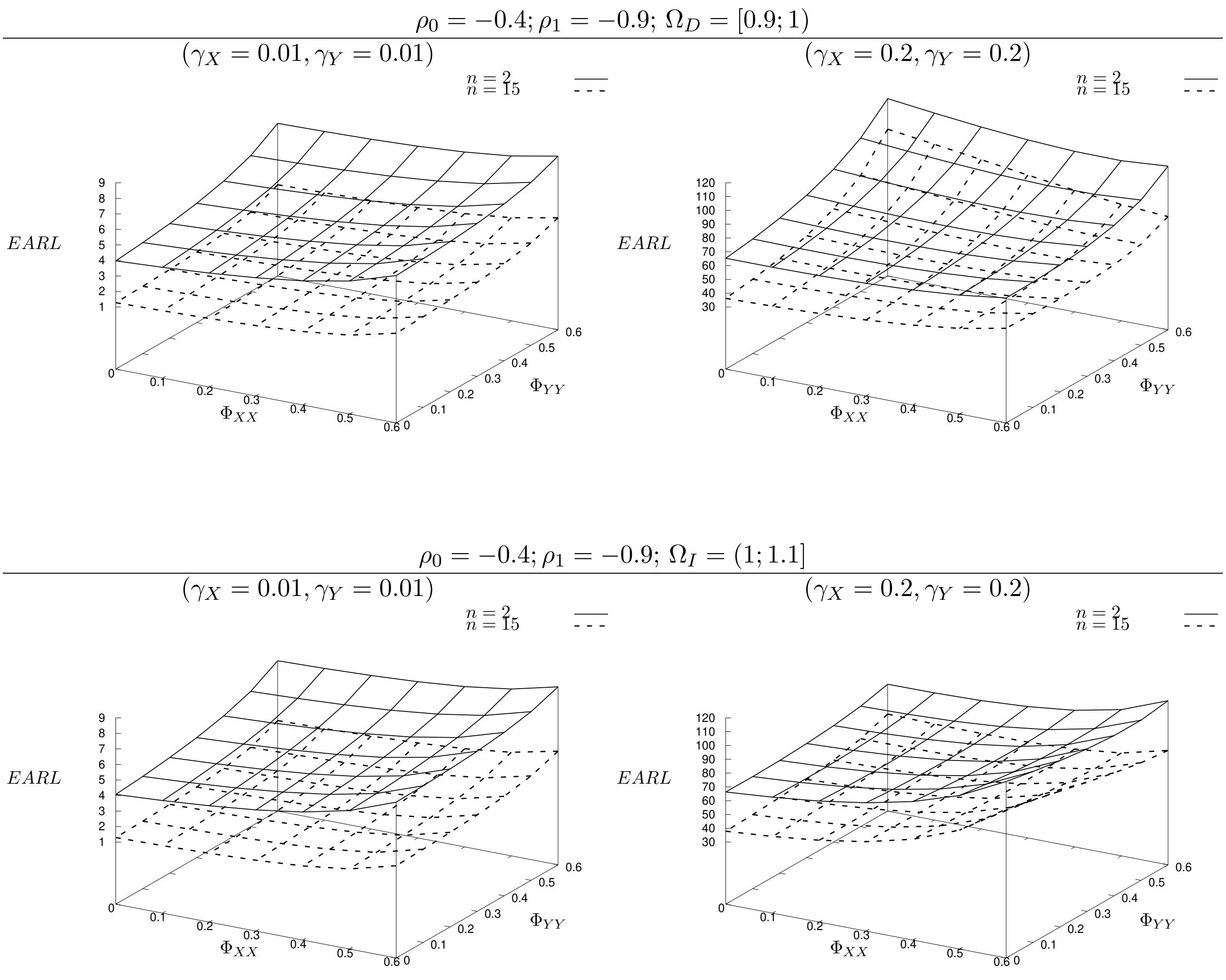


FIGURE 3.2: The effects of Φ_{XX} and Φ_{YY} on the overall performance of the Shewhart-RZ control chart in the presence of autocorrelation for $n \in \{2, 15\}$, $\gamma_X \in \{0.01, 0.2\}$, $\gamma_Y \in \{0.01, 0.2\}$, $\gamma_X = \gamma_Y$, $\rho_0 = -0.4$, $\rho_1 = -0.9$ and $ARL_0 = 200$.

3.3 Contributions about ratio control charts in the presence of measurement errors

In practice, measurement error almost always exists in all processes. Ignoring the presence of the measurement error in designing control charts may lead to a misunderstanding about the statistical properties of the designed control charts. Recent studies related to this problem can be seen in [211],[103, 183, 82, 49, 195, 194]and [182]. For the case of control charts monitoring the ratio, [211] used a quite strict assumption that $z_1^* = \tau * z_0^*$ where z_1^* and z_0^* are the out-of-control ratios, respectively, and the in-control ratio in the presence of measurement error, and τ is the shift size. This assumption is not reasonable in practice. [150] extended this study by easing this assumption to make it more realistic. The authors provided an exact change of the process parameters from an in-control condition to an out-of-control status under measurement errors.

In this section, we aim to develop a new measurement error model to fully describe the impact of measurement errors on the EWMA-RZ control chart. The use of the Exponentially Weighted Moving Average (EWMA) control chart has become increasingly popular in SPC literature. One of the reasons for the wide use of this type of chart is that it has "memory": it monitors a process based on information from the entire process, rather than just the current condition. As a result, it is often more effective than several others in detecting process shifts. Recently, the EWMA control charts for monitoring the ratio of two normal variables (denoted by EWMA-RZ control chart) were proposed by [210]. Instead of assuming an identity matrix in the linear covariate model, we consider a more general situation with a diagonal matrix. The motivation of this study is (1) to ease the strict assumption about the relation between the out-of-control ratio and the in-control ratio in [211] as well as to extend the assumption of identity matrix in the linear covariate model applied in [150], and (2) to investigate the impact of measurement errors on the EWMA-RZ control chart, and then to propose the ways to reduce the impact of measurement errors on the performance of this control chart when applied in practice. These improvements enable this study to overcome the limitations of previous studies on control charts for monitoring the ratio in the presence of measurement error, making it more efficient and realistic, which could be useful for practitioners.

3.3.1 Linear covariate error model for the sample of the ratio

In [211], the authors supposed that the relation between the out-of-control ratio and the in-control ratio is independent of measurement errors (see equation (36) in [211] and the corresponding explanation). In practice, measurement errors may affect the true observations of the ratio. As a result, this relation should change with measurement errors. We will accurately model the change of parameters of a process after being shifted under the presence of measurement errors to see this variation more clearly. Let us assume that, at time $i = 1, 2, \ldots$, a set of n consecutive items $\{\mathbf{W}_{i,1}, \mathbf{W}_{i,2}, ..., \mathbf{W}_{i,n}\}$ of the quality characteristic $\mathbf{W}$ is collected, where $\mathbf{W}_{i,j} = (X_{i,j}, Y_{i,j})^T \sim N(\boldsymbol{\mu}_{\mathbf{W}}, \boldsymbol{\Sigma}_{\mathbf{W}})$ is a bivariate normal vector with mean $\boldsymbol{\mu}_{\mathbf{W}}$ and variance-covariacne matrix $\boldsymbol{\Sigma}_{\mathbf{W}}$ defined as in (2.1). Due to measurement errors, the *true* quality characteristics $\mathbf{W}_{i,j}$ is unobservable. Instead, it is assessed from a set of $m \geq 1$ measurement operations, $\{\mathbf{W}^*_{i,j,1}, \mathbf{W}^*_{i,j,2}, ..., \mathbf{W}^*_{i,j,m}\}$. According to the linear covariate error model ([125]), we have

$$\mathbf{W}^*_{i,j,k} = \mathbf{A} + \mathbf{B}\mathbf{W}_{i,j} + \boldsymbol{\varepsilon}_{i,j,k}, k = 1, \ldots, m, \tag{3.18}$$

where $\mathbf{A}$ is a (2×1) vector of constants,

$$\mathbf{A} = \begin{pmatrix} a_X \\ a_Y \end{pmatrix}, \tag{3.19}$$

$\mathbf{B}$ is a (2×2) matrix, $\boldsymbol{\varepsilon} \sim N(\mathbf{0}, \boldsymbol{\Sigma}_M)$ is a centered bivariate normal random vector assumed to be independent of $\mathbf{W}$. The variance-covariance matrix in the distribution of $\boldsymbol{\varepsilon}$ is denoted by

$$\boldsymbol{\Sigma}_M = \begin{pmatrix} \sigma^2_{MX} & \rho_M \sigma_{MX} \sigma_{our} \\ \rho_M \sigma_{MX} \sigma_{our} & \sigma^2_{our} \end{pmatrix}, \tag{3.20}$$

where σ_{MX} (resp. σ_{our}) is the standard deviation of measurement errors of X (resp. Y), and $\rho_M \in (-1, +1)$ is the corresponding coefficient of correlation.

In [125], the authors recommended an invertible $p \times p$ matrix of constants, often diagonal, for the matrix $\mathbf{B}$. Therefore, we assume that $\mathbf{B} = b\mathbf{I}_{2\times 2}$, where b is a constant, i.e.

$$\mathbf{B} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}. \tag{3.21}$$

In practice, the mean $\overline{\mathbf{W}}^*_{i,j} = (\bar{X}^*_{i,j}, \bar{Y}^*_{i,j})$ of the observable quantities $\{\mathbf{W}^*_{i,j,1}, \mathbf{W}^*_{i,j,2}, ..., \mathbf{W}^*_{i,j,m}\}$ is often considered as a represented value for the true value $\mathbf{W}_{i,j}$. This mean is calculated by

$$\begin{aligned} \overline{\mathbf{W}}^*_{i,j} &= \frac{1}{m}\sum_{k=1}^{m} \mathbf{W}^*_{i,j,k} \\ &= \frac{1}{m}\sum_{k=1}^{m}(\mathbf{A} + \mathbf{B}\mathbf{W}_{i,j} + \boldsymbol{\varepsilon}_{i,j,k}) \\ &= \mathbf{A} + \mathbf{B}\mathbf{W}_{i,j} + \frac{1}{m}\sum_{k=1}^{m} \boldsymbol{\varepsilon}_{i,j,k}. \end{aligned} \tag{3.22}$$

That is, $\overline{\mathbf{W}}^*_{i,j}$ is also a bivariate normal random vector with the mean vector and the variance-covariance matrix defined by

$$\boldsymbol{\mu}_{\mathbf{W}^*} = \mathbf{A} + \mathbf{B}\boldsymbol{\mu}_W, \tag{3.23}$$

$$\boldsymbol{\Sigma}_{\mathbf{W}^*} = \mathbf{B}\boldsymbol{\Sigma}_W\mathbf{B}^T + \frac{1}{m}\boldsymbol{\Sigma}_M = b^2\boldsymbol{\Sigma}_W + \frac{1}{m}\boldsymbol{\Sigma}_M. \tag{3.24}$$

Let $\mu_{X^*}, \mu_{Y^*}, \sigma^2_{X^*}, \sigma^2_{Y^*}$ and ρ^* denote the mean, the variance and the coefficient of correlation of the two components $(\bar{X}^*_{i,j}, \bar{Y}^*_{i,j})$ of the vector $\overline{\mathbf{W}}^*_{i,j}$, respectively. Then, the equations (3.23) and (3.24) lead to

$$\mu_{X^*} = a_X + b\mu_X \tag{3.25}$$

$$\mu_{Y^*} = a_Y + b\mu_Y \tag{3.26}$$

$$\sigma^2_{X^*} = b^2\sigma^2_X + \frac{\sigma^2_{MX}}{m}, \tag{3.27}$$

$$\sigma^2_{Y^*} = b^2\sigma^2_Y + \frac{\sigma^2_{our}}{m}, \tag{3.28}$$

$$\rho^* = \frac{b^2\rho\sigma_X\sigma_Y + \rho_M\frac{\sigma_{MX}\sigma_{our}}{m}}{\sigma_{X^*}\sigma_{Y^*}}. \tag{3.29}$$

The equations (3.25)-(3.29) show a general change of $\mu_X, \mu_Y, \sigma^2_X, \sigma^2_Y$ and ρ

under the presence of the measurement errors. In the sequel, we will represent these changes when the process is shifted from an in-control condition to an out-of-control status.

Let $\boldsymbol{\mu_{0,W}} = (\mu_{0,X}, \mu_{0,Y})^T$ and $\rho = \rho_0$ denote the mean vector and the coefficient of correlation between the two normal variables $X_{i,j}$ and $Y_{i,j}$ of when the process is in-control. The mean ratio is now $z_0 = \frac{\mu_{0,X}}{\mu_{0,Y}}$. Suppose that an abnormal condition shifts the in-control ratio z_0 to $z_1 = \tau z_0$, where τ is the shift size, and the in-control coefficient of correlation $\rho = \rho_0$ to $\rho = \rho_1$. In particular, we suppose that the in-control $\boldsymbol{\mu_{0,W}}$ is shifted to $\boldsymbol{\mu_{1,W}} = (\mu_{0,X} + \delta_X\sigma_X, \mu_{0,Y} + \delta_Y\sigma_Y)^T$ where δ_X and δ_Y represent the mean shift of $X_{i,j}$ and $Y_{i,j}$. Then, the equation $z_1 = \tau z_0$ becomes

$$\frac{\mu_{0,X} + \delta_X\sigma_X}{\mu_{0,Y} + \delta_Y\sigma_Y} = \tau \times \frac{\mu_{0,X}}{\mu_{0,Y}},$$

and we obtain the following formula:

$$1 + \delta_X\gamma_X = \tau(1 + \delta_Y\gamma_Y). \tag{3.30}$$

According to the equations (3.25)-(3.28), under the presence of measurement errors, the coefficients of variation $\gamma_{X^*} = \frac{\sigma_{X^*}}{\mu_{X^*}}$ and $\gamma_{Y^*} = \frac{\sigma_{Y^*}}{\mu_{Y^*}}$ of $\bar{X}^*_{i,j}$ and $\bar{Y}^*_{i,j}$ are equal to

$$\gamma_{X^*} = \frac{\sqrt{b^2\sigma_X^2 + \frac{\sigma_{MX}^2}{m}}}{a_X + b(\mu_{0,X} + \delta_X\sigma_X)}, \tag{3.31}$$

$$\gamma_{Y^*} = \frac{\sqrt{b^2\sigma_Y^2 + \frac{\sigma_{MY}^2}{m}}}{a_Y + b(\mu_{0,Y} + \delta_Y\sigma_Y)}. \tag{3.32}$$

Considering the fraction in (3.31), if we divide its numerator by σ_X, its denominator by $\mu_{0,X}$ and then use (3.30), the coefficient of variation γ_{X^*} can be rewritten by

$$\gamma_{X^*} = \frac{\sqrt{b^2 + \frac{\eta_X^2}{m}}}{b(1 + \delta_X\gamma_X) + \theta_X} \times \gamma_X = \frac{\sqrt{b^2 + \frac{\eta_X^2}{m}}}{b\tau(1 + \delta_Y\gamma_Y) + \theta_X} \times \gamma_X \tag{3.33}$$

where $\eta_X = \frac{\sigma_{MX}}{\sigma_X}$, $\theta_X = \frac{a_X}{\mu_{0,X}}$, and $\gamma_X = \frac{\sigma_X}{\mu_{0,X}}$.
In a similar way, the coefficients of variation γ_{Y^*} in (3.32), the coefficient of correlation ρ^* in (3.29) and the standard-deviation ratio $\omega^* = \frac{\sigma_{X^*}}{\sigma_{Y^*}}$ can be

expressed as

$$\gamma_{Y^*} = \frac{\sqrt{b^2 + \frac{\eta_Y^2}{m}}}{b(1+\delta_Y\gamma_Y)+\theta_Y} \times \gamma_Y, \tag{3.34}$$

$$\rho^* = \frac{b^2\rho + \rho_M \frac{\eta_X\eta_Y}{m}}{\sqrt{b^2+\eta_X^2/m}\sqrt{b^2+\eta_Y^2/m}}, \tag{3.35}$$

$$\omega^* = \sqrt{\frac{b^2 + \frac{\eta_X^2}{m}}{b^2 + \frac{\eta_Y^2}{m}}} \times \omega, \tag{3.36}$$

where $\eta_Y = \frac{\sigma_{MY}}{\sigma_Y}$, $\theta_Y = \frac{a_Y}{\mu_{0,Y}}$, $\gamma_Y = \frac{\sigma_Y}{\mu_{0,Y}}$ and $\omega = \frac{\sigma_X}{\sigma_Y}$.

It should be considered that the in-control and out-of-control ratios under the presence of measurement errors are

$$z_0^* = \frac{\mu_{0,X^*}}{\mu_{0,Y^*}} = \frac{b\mu_{0,X}+a_X}{b\mu_{0,Y}+a_Y} = \frac{b+\theta_X}{b+\theta_Y} \times z_0, \tag{3.37}$$

$$\begin{aligned} z_1^* &= \frac{\mu_{1,X^*}}{\mu_{1,Y^*}} = \frac{a_X + b(\mu_{0,X}+\delta_X\sigma_X)}{a_Y+b(\mu_{0,Y}+\delta_Y\sigma_Y)} = \frac{\theta_X+b(1+\delta_X\gamma_X)}{\theta_Y+(1+\delta_Y\gamma_Y)} \times z_0 \\ &= \frac{\theta_X+\tau(1+\delta_Y\gamma_Y)}{\theta_Y+(1+\delta_Y\gamma_Y)} \times z_0. \end{aligned} \tag{3.38}$$

Thus, in general, we have $z_1^* \neq \tau z_0^*$.

3.3.2 Implementation of the EWMA-RZ control chart with measurement error

Consider a process with the same assumptions and notations as in the previous section. Suppose that the process is considered in control as long as the ratio $Z = X/Y$ is still in an acceptable range. Similar to [211], after collecting the samples $\{\mathbf{W}^*_{i,j,1}, \mathbf{W}^*_{i,j,2}, ..., \mathbf{W}^*_{i,j,m}\}$ at each sampling period $i = 1, 2, \ldots,$ we suggest to monitor the statistic

$$\hat{Z}_i^* = \frac{\hat{\mu}_{X_i^*}}{\hat{\mu}_{Y_i^*}} = \frac{\bar{\bar{X}}_i^*}{\bar{\bar{Y}}_i^*} = \frac{\sum_{j=1}^n \bar{X}^*_{i,j}}{\sum_{j=1}^n \bar{Y}^*_{i,j}}, \tag{3.39}$$

where $\bar{\bar{X}}_i^* = \frac{1}{n}\sum_{j=1}^n \bar{X}^*_{i,j}$, $\bar{\bar{Y}}_i^* = \frac{1}{n}\sum_{j=1}^n \bar{Y}^*_{i,j}$, $\bar{X}^*_{i,j}$ and $\bar{Y}^*_{i,j}$ are two components of the bivariate normal vector $\overline{\mathbf{W}}^*_{i,j}$ in (3.22).

It can be seen from their definition that $\bar{\bar{X}}_i^* \sim N(\mu_{X^*}, \frac{\sigma_{X^*}}{\sqrt{n}})$ and $\bar{\bar{Y}}^* \sim N(\mu_{Y^*}, \frac{\sigma_{Y^*}}{\sqrt{n}})$. Therefore, the coefficients of variations $\gamma_{\bar{X}^*}$ and $\gamma_{\bar{Y}^*}$ of $\bar{X}_i^*$ and $\bar{Y}_i^*$, the standard-deviation ratio $\omega_{\hat{Z}^*}$ at each sampling period $i = 1, 2, \ldots$ are, respectively, equal to

$$\gamma_{\bar{\bar{X}}^*} = \frac{\sigma_{X^*}}{\mu_{X^*}\sqrt{n}} = \frac{\gamma_{X^*}}{\sqrt{n}}, \tag{3.40}$$

$$\gamma_{\bar{\bar{Y}}^*} = \frac{\sigma_{Y^*}}{\mu_{Y^*}\sqrt{n}} = \frac{\gamma_{Y^*}}{\sqrt{n}}, \tag{3.41}$$

$$\omega_{\hat{Z}^*} = \frac{\sigma_{X^*}/\sqrt{n}}{\sigma_{Y^*}/\sqrt{n}} = \frac{\sigma_{X^*}}{\sigma_{Y^*}} = \omega^* \tag{3.42}$$

The *p.d.f* and the *c.d.f* of $\hat{Z}_i^*$ now can be obtained where γ_X, γ_Y, ω and ρ are replaced by $\gamma_{\bar{\bar{X}}^*}$, $\gamma_{\bar{\bar{Y}}^*}$, ω^* and ρ^* as defined in (3.40), (3.41), (3.42) and (3.35).

Since the distribution of $\hat{Z}_i^*$ is not symmetric, similar to [210], two one-sided charts will be considered to monitor $\hat{Z}_i^*$. In the design of a one-sided EWMA control chart, the statistic $\hat{Z}_i^*$ is not monitored directly. Instead, the following statistic will be monitored:

- in an upward EWMA chart (denoted as "EWMA-RZ$^+$" in the remainder of this section) that aims at detecting an increase in the ratio,

$$Y_i^{*+} = \max(z_0^*, (1-\lambda^+)Y_{i-1}^{*+} + \lambda^+\hat{Z}_i^*) \tag{3.43}$$

  where $Y_0^{*+} = z_0^*$ is an initial value. The corresponding upper control limit is $UCL^+ = K^+ \times z_0^*$ ($K^+ > 1$), and by the construction the lower control limit is $LCL^+ = z_0^*$.

- in a downward EWMA chart (denoted as "EWMA-RZ$^-$" in the remainder of this section) that aims at detecting a decrease in the ratio,

$$Y_i^{*-} = \min(z_0^*, (1-\lambda^-)Y_{i-1}^{*-} + \lambda^-\hat{Z}_i^*) \tag{3.44}$$

  where $Y_0^{*-} = z_0^*$ is an initial value. The corresponding lower control limit is $LCL^- = K^- \times z_0^*$ ($K^- < 1$), and by the construction, the upper control limit is $UCL^- = z_0^*$.

It should be considered that the control limits are considered in these forms rather than the general ones involving the mean and the standard deviation of Z_i because the distribution of $\hat{Z}_i^*$ has no moments. The two EWMA-RZ$^-$

and EWMA-RZ$^+$ charts above are defined when the smoothings $\lambda^+ \in (0,1]$, $\lambda^- \in (0,1]$ and the chart parameters K^+, K^- are defined.

3.3.3 Design of optimal EWMA-RZ Control Charts with measurement error

In practice, when an exact value of the shift size of τ is predicted at the design stage, the EWMA-RZ charts can be optimally designed in terms of ARL. However, this is not always the case, as the size cannot be anticipated exactly. This may lead to the poor performance of the designed chart. Therefore, in this study, we suggest optimally designing the EWMA-RZ charts under the presence of the measurement errors in terms of expected average run length ($EARL$), which is defined as

$$EARL = \int_{\Omega} ARL \times f_{\tau}(\tau)\mathrm{d}\tau, \tag{3.45}$$

where $f_\tau(\tau)$ is a $p.d.f$ of the random shift size τ over a support Ω and ARL is the average run length. In the SPC literature, a uniform distribution has been proposed to τ over a respecified interval $[a,b]$ (see, for example, [31] and [210]). That is, $f_\tau(\tau) = \frac{1}{b-a}$ for $\tau \in \Omega = [a,b]$.

Concerning this measure, the optimal design of the proposed charts consists of finding optimal couples (K^{*-},λ^{*-}) or (K^{*+},λ^{*+}) such that:

- for the EWMA-RZ$^-$ chart,

$$(K^{*-},\lambda^{*-}) = \underset{(K^-,\lambda^-)}{\operatorname{argmin}} EARL(n,K^-,\lambda^-,\rho_1,\gamma_{X^*},\gamma_{Y^*},\rho^*,\omega^*)$$

  subject to the constraint

$$ARL(n,K^-,\lambda^-,\gamma_{X^*},\gamma_{Y^*},\rho^*,\omega^*,\rho_1=\rho_0,\tau=1) = ARL_0,$$

- for the EWMA-RZ$^+$ chart:

$$(K^{*+},\lambda^{*+}) = \underset{(K^+,\lambda^+)}{\operatorname{argmin}} EARL(n,K^+,\lambda^+,\rho_1,\gamma_{X^*},\gamma_{Y^*},\rho^*,\omega^*)$$

subject to the constraint

$$ARL(n, K^+, \lambda^+, \gamma_{X^*}, \gamma_{Y^*}, \rho^*, \omega^*, \rho_1 = \rho_0, \tau = 1) = ARL_0.$$

The numerical results show that although the precision error and the accuracy error have negative influences on the proposed chart performance, when these errors are not large, these influences are not significant.

3.4 Contributions about Reliability sampling plans

Reliability sampling plans (RSPs) for Weibull quantiles under progressive Type-II censoring play a crucial role in assessing product lifespan and process stability. These methods can be effectively adapted for control charts, particularly in applications that require robust quality monitoring, such as smart textiles and IoT-based healthcare systems. Unlike traditional mean-based approaches, Weibull quantiles offer a more comprehensive evaluation of process variability, making them well-suited for early failure detection in wearable sensors. By leveraging fraction nonconforming ($f_n c$) and log-Weibull transformations, a Weibull quantile control chart can track sensor degradation over time, ensuring proactive maintenance and improved reliability. Furthermore, the cost optimization models (CF1, CF2, CF3) presented in the literature provide a framework for setting optimal control limits and balancing monitoring expenses and failure risks. This method facilitates the quick and accurate testing of reliability, enhancing the lifespan and performance of smart textile systems, wearable sensors, and IoT healthcare applications.

3.4.1 Life model and sampling plan

Suppose that X follows the two-parameter Weibull distribution, $X \sim \mathrm{We}(\lambda, \tau)$, with the probability density function (PDF):

$$f_X(x; \lambda, \tau) = \frac{\lambda x^{\lambda-1} \exp\left(-\left(\frac{x}{\tau}\right)^{\lambda}\right)}{\tau^{\lambda}}, \qquad x > 0, \tag{3.46}$$

where $\lambda > 0$ and $\tau > 0$ are the shape and scale parameters, respectively. The life model (3.46) covers the exponential and Rayleigh distributions with

$\lambda = 1$ and $\lambda = 2$, respectively. The p quantile of the Weibull distribution is:

$$x_p = \tau[-\log(1-p)]^{1/\lambda}, \quad 0 < p < 1. \tag{3.47}$$

It is known that the transformed variable $Y = \log(X)$ follows the smallest extreme value (SEV) distribution, $Y \sim \text{SEV}(\mu, \sigma)$, with PDF:

$$f_Y(y;\mu,\sigma) = \frac{1}{\sigma}\exp\left(\frac{y-\mu}{\sigma} - \exp(\frac{y-\mu}{\sigma})\right), y \in (-\infty, \infty) \tag{3.48}$$

and the cumulative distribution function (CDF):

$$F_Y(y;\mu,\sigma) = 1 - \exp\left(-\exp(\frac{y-\mu}{\sigma})\right), \tag{3.49}$$

where $\mu = \log(\tau) \in (-\infty, \infty)$ and $\sigma = (1/\lambda) > 0$ are the location and scale parameters, respectively. The p quantile of the SEV distribution is:

$$y_p = \mu + \sigma s_p, \tag{3.50}$$

where $s_p = \log(-\log(1-p))$ is the p quantile of standard SEV distribution with $\mu = 0$ and $\sigma = 1$. Since $x_p = \exp(y_p)$, any quality assurance activity based on y_p will be equivalent to the effort based on x_p. Hence, in what follows, we will work with the transformed lifetime Y. This approach is also used to develop control charts for quantiles of the Weibull distribution (Pascual et al. [163]). An advantage of working with a transformed model is that the shape and scale parameters, respectively, are reinterpreted as scale and location parameters.

To construct a decision rule, a random sample should be taken from the lot. In this Section, we consider a P-II censored sample that is observed as follows. Suppose that n items, whose log-lifetimes follow (3.48), are put to the test at time zero. At the time of the first failure time, $y_{1:m:n}$, R_1 surviving units are removed randomly from the life test. Then, R_2 items are randomly removed immediately after the second failure, i.e., observing $y_{2:m:n}$. This process would be repeated until m failure times are recorded from the life test. The censoring parameters m and $\mathbf{R} = (R_1, R_2, ..., R_m)$ are known before starting the life test, and they are chosen such that $n = m + \sum_{i=1}^{m} R_i$. At the end of inspection, m ordered failure times (complete data) $y_{1:m:n} \le y_{2:m:n} \le ... \le y_{m:m:n}$ and $\sum_{i=1}^{m} R_i$ censored failure times (incomplete data) are gathered. The likelihood function for the P-II censored sample is given by:

$$L(\mu,\sigma) = \prod_{i=1}^{m} \gamma_i f_Y(y_{i:m:n};\mu,\sigma) \left(1 - F_Y(y_{i:m:n};\mu,\sigma)\right)^{R_i}, \tag{3.51}$$

where

$$\gamma_i = \sum_{j=i}^{m}(R_j+1), \qquad i = 1,2,...,m, \tag{3.52}$$

and $f_Y(.)$ and $F_Y(.)$ are given in (3.48) and (3.49). The MLEs of the location parameter $\hat{\mu}$ and scale parameter $\hat{\sigma}$ can be obtained by maximizing $L(\mu,\sigma)$. The estimates $\hat{\mu}$ and $\hat{\sigma}$ can not be derived analytically, and one should calculate them using available numerical methods in programs such as R or MATLAB. The MLEs of y_p and x_p are also obtained by invariant:

$$\hat{y}_p = \hat{\mu} + \hat{\sigma} s_p, \quad \hat{x}_p = \exp(\hat{y}_p).$$

reducedIn what follows, we describe the operating procedure of the proposed CRSP under an observed P-II censored sample. Let y_p^0 be the minimum allowable value for the considered p quantile, which is known in advance. The proposed CRSP includes the following steps:

- Based on the specified quality levels and inspection risks of the buyer-supplier purchasing contract, choose the appropriate sample size n and censoring plan parameters m and **R**.
- Take a random sample of size n from the submitted lot and put the items in a life test to obtain the failure times $x_{1:m:n}, x_{2:m:n}, ..., x_{m:m:n}$ according to the known censoring reducedscheme.
- Take the logarithm of data, i.e., $y_{i:m:n} = \log(x_{i:m:n})$ for $i = 1,2,...,m$, and then calculate the MLEs $\hat{\mu}$, $\hat{\sigma}$, and $\hat{y}_p$ based on transformed data and relation (3.51).
- Accept the lot if $Q_p = \dfrac{\hat{y}_p - y_p^0}{\hat{\sigma}} > c_0$. Otherwise, reject the lot.

The suggested CRSP has $m+3$ operational parameters that should be determined before starting the inspectionreduced; they are $n, m, R_1, ..., R_m$, and c_0. It is reminded that $y_p = \mu + \sigma s_p$ is the true p quantile of the process due to the true μ and σ. This means that y_p is sensitive to any changes in the location and scale parameters. To express the lot quality, we use the free-scale distance $\rho_p = \frac{y_p - y_p^0}{\sigma}$. By the invariance property of MLE, Q_p is the MLE of ρ_p. The parameter ρ_p measures how far the actual process quantile is from the minimum allowable value in reducedunits of actual standard deviation. Note that $\rho_p \geq 0$ shows that the lot meets the least desired. Consequently, it should be emphasized that the larger the ρ_p value, the higher the quality. By extending the results of Lawless [112], reducedViveros and Balakrishnan [223], and Haghighi et al. [79], we derived the conditional CDF of Q_p given the ancillary vector $\mathbf{a}$ and the parameter ρ_p under P-II censoring scheme as:

$$F_{Q_p}(q|\mathbf{a},\rho_p) = C\int_0^{\infty} h(w|\mathbf{a})G_m\Big(g(\mathbf{a},p,q,\rho_p,w)\Big)dw, \tag{3.53}$$

where reduced

$$\begin{aligned} C &= \left(\int_0^{\infty} \frac{w^{m-2}\exp(w\sum_{j=1}^m a_j)}{[\sum_{j=1}^m (R_j+1)\exp(wa_j)]^m}dw\right)^{-1}, \qquad (3.54)\\ h(w|\mathbf{a}) &= \frac{w^{m-2}\exp(w\sum_{j=1}^m a_j)}{[\sum_{j=1}^m (R_j+1)\exp(wa_j)]^m},\\ G_m(s) &= \frac{1}{(m-1)!}\int_0^s t^{m-1}\exp(-t)dt,\\ g(\mathbf{a},p,q,\rho_p,w) &= \exp\Big(s_p - w(s_p-q) - \rho_p\Big)\Big(\sum_{j=1}^m (R_j+1)\exp(wa_j)\Big), \end{aligned}$$

and

$$\mathbf{a} = \left(a_1 = \frac{y_{1:m:n} - \hat{\mu}}{\hat{\sigma}}, a_2 = \frac{y_{2:m:n} - \hat{\mu}}{\hat{\sigma}}, ..., a_m = \frac{y_{m:m:n} - \hat{\mu}}{\hat{\sigma}}\right),$$

is the vector of ancillary statistics, functions of data so that their distribution is free of parameters μ and σ. The conditional CDF in (3.53) depends reducedon the ancillary vector $\mathbf{a}$, and so its values vary from one observed vector to another. Hence, an adequate approximation will be reducedconstructive. We adapt the idea of Haghighi et al. [79] to approximate $F_{Q_p}(q|\mathbf{a},\rho_p)$ by $F_{Q_p}(q|\mathbf{a}_0,\rho_p)$ for an appropriately chosen $\mathbf{a}_0$. This approach is also considered in Pascual et al. [163] and Wang et al.[231]. In this regard, let the "fixed sample" $y_i^0 = s_{p_i}$ for $i = 1,2,...,n$ where $p_i = \frac{i-0.375}{n+0.25}$. Implementing the P-II censoring plan on $y_1^0, y_2^0, ..., y_n^0$, we have:

$$\mathbf{a}_0 = \big(a_1 = \frac{y^0_{1:m:n} - \hat{\mu}^0}{\hat{\sigma}^0}, a_2 = \frac{y^0_{2:m:n} - \hat{\mu}^0}{\hat{\sigma}^0}, ..., a_m = \frac{y^0_{m:m:n} - \hat{\mu}^0}{\hat{\sigma}^0}\big), \tag{3.55}$$

where $\hat{\mu}^0$ and $\hat{\sigma}^0$ are the MLEs based on the P-II censored sample $y^0_{1:m:m}, y^0_{2:m:m}, ..., y^0_{m:m:n}$. Hence, the COC of the proposed CRSP, which provides the conditional lot acceptance probability in terms of the quality level ρ_p given $\mathbf{a}_0$, is as follows:

$$\begin{aligned} COC(\rho_p|\mathbf{a}_0) &= Pr(Q_p > c_0|\mathbf{a}_0, \rho_p) \\ &= 1 - F_{Q_p}(c_0|\mathbf{a}_0, \rho_p). \end{aligned}$$

The reducedfirst order derivative of $COC(\rho_p|\mathbf{a}_0)$ with respect to ρ_p can be obtained as:

$$\frac{d}{d\rho_p} COC(\rho_p|\mathbf{a}_0) = C \int_0^\infty \Big[h(w|\mathbf{a}_0)\big(g(\mathbf{a}_0, p, c_0, \rho_p, w)\big)^m \times \exp\big(-g(\mathbf{a}_0, p, c_0, \rho_p, w)\Big] dw. \tag{3.56}$$

Relation (3.56) shows that for fixed $n, m, \mathbf{R}$, and c_0, $\frac{d}{d\rho_p} COC(\rho_p|\mathbf{a}_0) > 0$. This means that the lot acceptance probability increases with ρ_p, as expected.

3.4.2 Optimization strategies

This subsection is devoted to finding the operating parameters of the new CRSP, including the number of test units n, the number of observed failures m, the number of reducedremoved items at the failure times $R_1, R_2, ..., R_m$, and the decision constant c_0. In what follows, we will determine the plan parameters based on some economic criteria. This is usually solved through constrained optimization problems with constraints related to the producer's and the consumer's demands. Producers prefer a sampling plan with a probability of lot acceptance of at least $1 - \alpha$ when the actual quality level is at AQL, while consumers would rather have a plan with a probability of lot acceptance of at most β in LQL. In literature, $\alpha, 1 - \alpha$, and β are called the producer's risk, the producer's confidence, and the consumer's risk, respectively. Hereinafter, we denote the level of acceptable quality by ρ_p^{AQL} and the limiting level by ρ_p^{LQL}. Thus, the conditions $COC(\rho_p^{\mathrm{AQL}}|\mathbf{a}_0) \geq 1 - \alpha$ and $COC(\rho_p^{\mathrm{LQL}}|\mathbf{a}_0) \leq \beta$ would be considered as the constraints in the optimal design of the plan. Several combinations of the plan parameters may reducedsatisfy the protecting conditions, but we look for those that impose the minimum cost. In this way, we define three cost functions. reducedThe first cost function (CF_1) is constructed based on the inspection cost, the second cost function (CF_2) accounts for the inaccurate estimation cost, and the third cost function (CF_3) is a weighted-relative combination of CF_1 and CF_2. They are described in detail in the following three subsections.

First strategy: Optimal design based on inspection cost

The first approach to finding the optimal set of plan parameters is based on the expected cost of the inspection. Minimizing such costs is desirable for suppliers or manufacturers. Since the inspection is a life test, we consider the following components in the cost function CF_1:

- Installation cost. The cost of installing all gathered items in the test is C_0, which does not depend on the number of items.
- Failed items cost. Let C_f be the cost of each completely failed item. Then, the total cost of failing items would be mC_f.
- Censored items Cost. Let each censored item have a cost C_c (less than C_f). Hence, the total cost of removed items is $(n-m)C_c$.
- Operation cost. This is the total cost of the test, from start to finish. It includes the salary of operators, utility, depreciation of test equipment, and so on. Let C_o be the operation cost for each time unit. In addition, the life test would be terminated at the random time of m-th failure, $X_{m:m:n}$ where $X_{m:m:n}$ is the m-th order statistic from a Weibull distribution (3.46). Then, the expected operation cost will be $C_o E(X_{m:m:n})$.

Consequently, CF_1 is presented as the accumulation of all the cost components as:

$$\mathrm{CF}_1 = C_0 + mC_f + (n-m)C_c + C_o E(X_{m:m:n}).$$

Based on the moment generating function of $Z_{m:m:n}$, the m-th order statistics from the standard SEV distribution under a P-II censoring plan (Ng et al.

[145]), the expected test time is as follows:

$$\begin{aligned} E(X_{m:m:n}) &= E(e^{Y_{m:m:n}}) \\ &= E(e^{\mu+\sigma Z_{m:m:n}}) \\ &= e^{\mu} c_{m-1} \Gamma(\sigma+1) \sum_{i=1}^{m} a_{i,m} \gamma_i^{-(\sigma+1)}, \end{aligned}$$

where $\Gamma(.)$ is the complete Gamma function, γ_i is given in (3.52), and

$$c_{m-1} = \prod_{i=1}^{m} \gamma_i, \qquad a_{i,m} = \prod_{k=1;k\neq i}^{m} \frac{1}{\gamma_k - \gamma_i}, \qquad i = 1, 2, ..., m.$$

Hence, the first procedure to find the optimal plans based on inspection cost would be expressed as follows:

$$\begin{aligned} \text{minimize} \quad & \text{CF}_1 = C_0 + mC_f + (n-m)C_c + C_o E(X_{m:m:n}) \qquad (3.57) \\ \text{subject to} \quad & COC(\rho_p^{\text{AQL}} | \mathbf{a}_0) \geq 1 - \alpha, \\ & COC(\rho_p^{\text{LQL}} | \mathbf{a}_0) \leq \beta, \\ & n \geq m > 0, (n, m) \in N^2, (R_1, R_2, ..., R_m) \in Z^{+^m}, \\ & n = m + \sum_{i=1}^{m} R_i, c_0 \in R, \end{aligned}$$

where N, Z^+, and R are the sets of natural numbers, non-negative integer numbers, and real numbers, respectively.

Second strategy: Optimal design based on the inaccurate estimation cost with limitation of inspection budget

In experimental design, the accuracy of estimators is a serious concern as far as suggested by Balakrishnan and Cramer [14] as an optimal benchmark to find optimal censoring plans. In reliability tests, the deviation of an estimator from the true-life parameter regarding the magnitude of deviation could result in incurring undesired costs. For example, when the interesting parameter is the mean life, underestimating it may result in a loss of sales due to customers' unwillingness to purchase the product, while overestimating it may increase post-sale services and lead to a loss of brand (Budhiraja and Pradhan [27]). In the RSP problem, when the lot's quality is described by a lower quantile, underestimating true quality at AQL may lead to rejecting a high-quality lot, and overestimating quality at LQL may result in accepting a low-quality lot. It is known that larger sample sizes provide more information and, hence, increase the accuracy of estimation. While larger sample sizes impose reducedhigher inspection costs and time, in practice, quality inspections reducedoften have a limited budget and time. Therefore, one needs a procedure that findreduceds the most accurate plan in the class of plans with a limited budget. Let C_b, C_a, and C_r be the inspection budget, the cost per unit positive deviation of estimated quality from ρ_p^{LQL} and the cost per unit negative deviation of estimated quality from ρ_p^{AQL}, respectively. The second optimization strategy for finding the optimal plans can be mathematically formulated as the following non-linear problem:

$$
\begin{aligned}
\text{minimize} \quad & \text{CF}_2 = C_a E[(Q_p - \rho_p^{\text{LQL}})^+|\mathbf{a}_0] + C_r E[(\rho_p^{\text{AQL}} - Q_p)^+|\mathbf{a}_0] \quad (3.58)\\
\text{subject to} \quad & \text{CF}_1 < C_b,\\
& COC(\rho_p^{\text{AQL}}|\mathbf{a}_0) \geq 1-\alpha,\\
& COC(\rho_p^{\text{LQL}}|\mathbf{a}_0) \leq \beta,\\
& n \geq m > 0, (n,m) \in N^2, (R_1, R_2, ..., R_m) \in Z^{+^m},\\
& n = m + \sum_{i=1}^{m} R_i, c_0 \in R,
\end{aligned}
$$

where $f^+ = max\{0, f\}$. The acquired plan parameters, based on the above optimization, ensure that while the inspection cost does not exceed the fixed budget C_b, the lot is inspected with maximum accuracy at both the extreme quality levels and the desired confidence levels. The conditional expectations in CF_2 can be obtained based on the conditional PDF of Q_p. By taking the first derivative of (3.53) concerning q, the conditional PDF is obtained as follows:

$$
f_{Q_p}(q|\mathbf{a}_0, \rho_p) = \frac{C}{(m-1)!} \int_0^\infty \Big[wh(w|\mathbf{a}_0) \big(g(\mathbf{a}_0, p, q, \rho_p, w) \big)^m \times \exp\big(-g(\mathbf{a}_0, p, q, \rho_p, w) \big) \Big] dw,
$$

TABLE 3.1: The optimal CRSP parameters based on the first and second strategies with $\alpha = 0.05$ and $\beta = 0.1$.

The first strategy									
ρ_p^{LQL}	ρ_p^{AQL}	n	m	R_1	R_2	R_{m-1}	R_m	c_0	CF_1^*
0	4	16	4	0	4	3	5	2.0677	63.9583
	6	10	4	0	0	1	5	3.1686	59.0778
	8	8	4	0	0	0	4	4.0599	58.3452
2	6	18	16	0	0	0	2	3.9312	93.9511
	8	19	5	7	3	3	1	5.0809	73.5306
	10	16	6	0	2	0	8	6.1375	66.6512
4	8	31	26	0	2	0	3	5.9023	118.2371
	10	21	15	0	1	0	5	6.9210	89.0939
	12	18	10	0	2	1	5	7.9847	77.3975
The second strategy									
ρ_p^{LQL}	ρ_p^{AQL}	n	m	R_1	R_2	R_{m-1}	R_m	c_0	CF_2^*
0	4	18	17	0	0	0	1	1.8846	103.9806
	6	17	16	0	0	0	1	2.6798	117.1134
	8	15	14	0	0	1	0	3.4867	133.5700
2	6	19	16	2	0	0	1	4.0110	164.8695
	8	19	16	2	0	0	1	4.9016	173.9768
	10	19	16	2	0	0	1	5.7124	183.1301
4	8	-	-	-	-	-	-	-	-
	10	22	17	0	3	0	2	7.0419	228.2381
	12	20	18	0	0	0	2	7.9101	244.2318

where C, $h(w|\mathbf{a})$, and $g(\mathbf{a}, p, q, \rho_p, w)$ are given in (3.54). Thus, this yields the following representations of the conditional expectations appeared in CF_2:

$$E[(Q_p - \rho_p^{\text{LQL}})^+|\mathbf{a}_0] = \int_{\rho_p^{\text{LQL}}}^{\infty} (q - \rho_p^{\text{LQL}}) \times f_{Q_p}(q|\mathbf{a}_0, \rho_p^{\text{LQL}})dq$$

$$E[(\rho_p^{\text{AQL}} - Q_p)^+|\mathbf{a}_0] = \int_{-\infty}^{\rho_p^{\text{AQL}}} (\rho_p^{\text{AQL}} - q) \times f_{Q_p}(q|\mathbf{a}_0, \rho_p^{\text{AQL}})dq.$$

Third strategy: Optimal design based on a unified cost

reducedWe concentrate on the inspection and the inaccurate estimation costs in the previous two subsections. The third approach is to consider both objectives simultaneously. Suppose that the optimal parameters of optimizations (3.57) and (3.58) lead to minimal costs CF_1^* and CF_2^*. As the minimal costs are the most desirable, it is natural to approach them as closely as possible in the sense of relative least distance. Hence, we propose the following objective function as a weighted relative combination of the previous objectives to reach the optimal parameters:

$$
\begin{aligned}
\text{minimize} \quad & w\left|\frac{\mathrm{CF}_1-\mathrm{CF}_1^*}{\mathrm{CF}_1^*}\right|+(1-w)\left|\frac{\mathrm{CF}_2-\mathrm{CF}_2^*}{\mathrm{CF}_2^*}\right| \\
\text{subject to} \quad & \mathrm{CF}_1 < C_b, \\
& COC(\rho_p^{\mathrm{AQL}}|\mathbf{a}_0) \geq 1-\alpha, \\
& COC(\rho_p^{\mathrm{LQL}}|\mathbf{a}_0) \leq \beta, \\
& n \geq m > 0, (n,m) \in N^2, (R_1, R_2, ..., R_m) \in Z^{+^m}, \\
& n = m + \sum_{i=1}^{m} R_i, c_0 \in R,
\end{aligned}
\tag{3.59}
$$

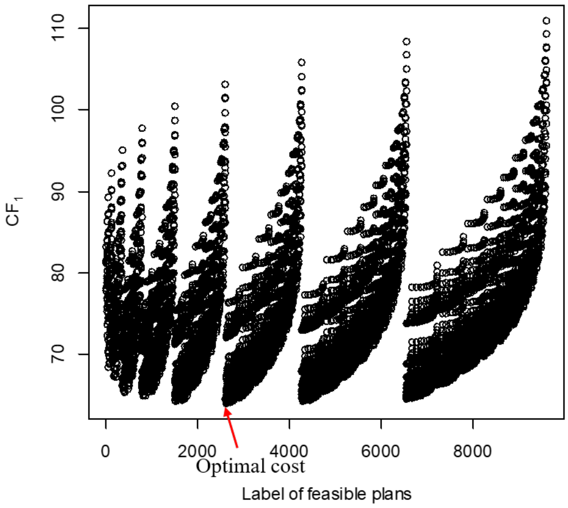
where w $(0 < w < 1)$ denotes the positive weight of the first objective and $1-w$ is for the second one, and also $|.|$ is the absolute value function. See more details about such techniques in Lin [124]. For example, $w = \frac{2}{3}$ means the inspection cost reducedis twice as important as estimation accuracy. The outputs of (3.59) ensure minimal costs will be attained with a minimum miss.

3.4.3 Obtaining the optimal parameters

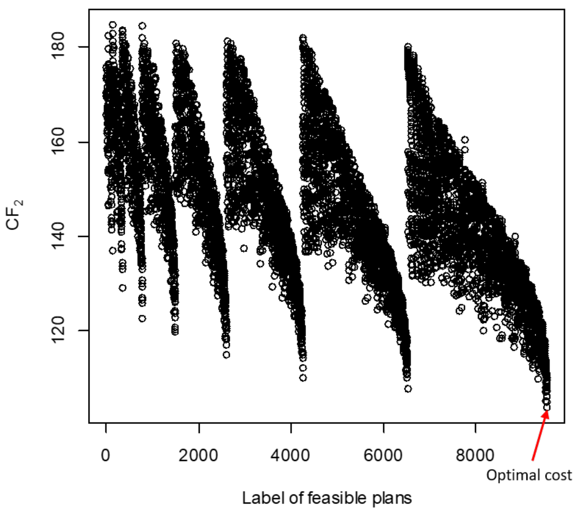
From the previous discussion, the plan parameters are $n, m, R_1, ..., R_m$, and c_0, which should be known in advance when using the proposed CRSP. This encompasses the optimal experimental design of progressive censoring plans in reliability theory, where n and m are fixed, and the experimenter seeks optimal censoring plans $R_1, R_2, ..., R_m$ based on a specific scientific criterion. It is known that for fixed n and m, there exist $\binom{n-1}{m-1}$ censoring schemes. Although the number of censoring schemes reducedis finite, it can be quite large even for moderate n and m. For example when $n = 30$ and $m = 15$, it is $\binom{30-1}{15-1} = 77,558,760$, which is quite large. Hence, a general answer to our problem cannot be expected, and we must restrict ourselves to searching within a subclass of parameters. Here, we follow the Balasooriya et al. [15] approach in which the removals have only occurred at the first, second, $m-1$th, and mth failures, i.e., R_1, R_2, R_{m-1}, R_m are non-negative, and $R_i = 0$ for $i = 3, 4, ..., m-2$. Hence, the remaining parameters will be the integer sampling parameters $n, m, R_1, R_2, R_{m-1}, R_m$ where $n = m + R_1 + R_2 + R_{m-1} + R_m$, and the real decision number c_0. Since

TABLE 3.2: The optimal CRSP parameters based on the third strategy with $w = \frac{1}{3}, \frac{2}{3}, \alpha = 0.05$ and $\beta = 0.1$.

		$w = \frac{1}{3}$								
ρ_p^{LQL}	ρ_p^{AQL}	n	m	R_1	R_2	R_{m-1}	R_m	c_0	CF_1	CF_2
0	4	18	15	0	0	0	3	1.8911	89.6178	110.7738
	6	17	14	0	0	0	3	2.6800	87.0621	125.2729
	8	15	13	0	0	0	2	3.4492	86.1823	141.856
2	6	19	16	2	0	0	1	4.0110	99.3336	164.8695
	8	19	16	2	0	0	1	4.9016	99.3336	173.9768
	10	19	16	2	0	0	1	5.7124	99.3336	183.1301
4	8		-	-	-	-	-	-	-	-
	10	22	17	0	3	0	2	7.0419	99.3263	228.2381
	12	20	18	0	0	0	2	7.9101	98.9774	244.2318
		$w = \frac{2}{3}$								
ρ_p^{LQL}	ρ_p^{AQL}	n	m	R_1	R_2	R_{m-1}	R_m	c_0	CF_1	CF_2
0	4	19	4	2	5	7	1	1.9545	70.1513	135.8328
	6	18	4	0	7	5	2	2.8110	67.5882	157.6126
	8	15	4	3	5	1	2	3.6129	65.9091	186.8106
2	6	19	16	1	0	0	2	3.9483	94.9218	171.0720
	8	20	11	0	4	3	2	4.9914	83.3753	204.6334
	10	19	10	2	2	3	2	5.8438	80.7860	227.4983
4	8	-	-	-	-	-	-	-	-	-
	10	21	14	0	4	0	3	6.9896	90.8251	256.1530
	12	20	11	0	4	3	2	8.0846	83.3753	301.5816



(a) CF_1 values.



(b) CF_2 values.

FIGURE 3.3: Cost functions when $\rho_p^{\text{LQL}} = 0$ and $\rho_p^{\text{AQL}} = 4$ for the plan parameters in feasible set.

the objective functions and constraints are non-linear functions of plan parameters, nonlinear mixed-integer programming should be used to find the optimal plans. We use an extended, simple, exhaustive search algorithm to solve the problem. Throughout the optimization procedure, for a sufficiently large n (for example $n = 50$), we have searched along with all the possible values of $4 \leq m \leq n$ and $0 \leq R_1, R_2, R_{m-1}, R_m \leq n - m$ such that $R_1 + R_2 + R_{m-1} + R_m = n - m$. Then, for each combination of integer parameters, we sought the optimal c_0 that satisfies the supporting constraints. There exists an infinite number of such c_0. We chose the optimal c_0 such that $COC(\rho_p^{\text{AQL}}|\mathbf{a}) - COC(\rho_p^{\text{LQL}}|\mathbf{a})$ to be maximized while $COC(\rho_p^{\text{AQL}}|\mathbf{a}) \geq 1 - \alpha$ and $COC(\rho_p^{\text{LQL}}|\mathbf{a}) \leq \beta$. This is solved via the prominent package *DEoptim* available in R software version 3.6.0, which implements the differential evolution algorithm for the global optimization of real-valued functions of real-valued parameters. Ultimately, the system selects the optimal plan with the lowest cost and the best decision number. Parallelization is a beneficial technique that able users to speed up computations by using different cores of the computer. This is available in R packages such as *parallel* and *foreach*. The *DEoptim* function also has an option to make optimizations parallel (argument *parallelType*). By using parallelization, we decreased the computation time to $\frac{1}{4}$.

For industrial applications, we calculated the optimal parameters based on commonly used inspection risk, some quality requirements, inspection cost, and the cost of inaccurate reduceddecision-making. To make the tables and figures more self-contained, let us remind you that CF_1 and CF_2 arereduced, respectivelyreduced, the costs regarding the inspection (see eq. (3.57)) and the inaccurate estimation (see eq. (3.58)) as well as CF_3 is an integrated version of both preceding costs (see eq. (3.59)). For the first and second optimization strategies, the parameters are presented in Table reduced1 and for the third one in Table reduced2. The optimal costs CF_1^* and CF_2^* related to the optimal parameters are also presented in Table reduced1. In Table reduced2, we calculated also the costs CF_1 and CF_2 corresponding to the optimal parameters of the third strategy. The tables are constructed based on $\tau = 1 (\mu = 0), \lambda = 1 (\sigma = 1), p = 0.1, \alpha = 0.05, \beta = 0.1, \rho_p^{\text{LQL}} = 0, 2, 4, \rho_p^{\text{AQL}} = 4, 6, 8, 10, 12, C_0 = 40, C_f = 2, C_c = 1, C_o = 10, C_a = 200, C_r = 100, C_b = 100$, and $w = \frac{1}{3}, \frac{2}{3}$. The results are interpreted as:

- Table reduced1 (Upper part): The table shows that the inspection becomes cheaper (CF_1^* decreases) when ρ_p^{LQL} and ρ_p^{AQL} tend to getaway. This means that when ρ_p^{LQL} and ρ_p^{AQL} are relatively far, fewer items need to be inspected (based on this approach) for discriminating between a satisfactory lot and an unsatisfactory one.

- Figure 3.3(a): The figure shows the reducedbehavior of CF_1 for some combinations of the plan parameters within the feasible set. More precisely, it presents the CF_1 cost values based on more than 8,000 combinations of operating parameters $n, m, R_1, R_2, R_{m-1}, R_m$, and c_0 that meet the supporting constraints $COC(\rho_p^{\mathrm{AQL}}|\mathbf{a}_0) \geq 1-\alpha$ and $COC(\rho_p^{\mathrm{LQL}}|\mathbf{a}_0) \leq \beta$ when $\rho_p^{\mathrm{LQL}} = 0$ and $\rho_p^{\mathrm{AQL}} = 4$. From the figure, it can be said that CF_1 increases when n and/or m are on increase. This is expected due to the mathematical structure of CF_1.

- Table reduced1 (Lower part): The table indicates that when ρ_p^{LQL} and ρ_p^{AQL} tend to reducedget away, the inspection becomes expensive. This is because of ρ_p^{LQL} and ρ_p^{AQL} are the 0.1 and 0.95 quantiles of $COC(\rho_p|\mathbf{a}_0)$. The more reduceddistance between these extreme quantiles is equivalent to the more dispersed $COC(\rho_p|\mathbf{a}_0)$. In this case, larger sample sizes are needed reducedto estimate these extreme quantiles accurately. Moreover, it is known from the table that the effective sample size m of each optimal plan tends to be close to its corresponding total sample size n. This is because the complete observations provide more information than the censored ones, and hence, for a fixed n, the larger m leads to the smaller CF_2.

- Figure 3.3(b): Analogous to Figure 3.3(a), this figure depicts the CF_2 cost values corresponding to more than 8,000 combinations of operating parameters $n, m, R_1, R_2, R_{m-1}, R_m$, and c_0 that meet the supporting constraints $COC(\rho_p^{\mathrm{AQL}}|\mathbf{a}_0) \geq 1-\alpha, \quad COC(\rho_p^{\mathrm{LQL}}|\mathbf{a}_0) \leq \beta$ and $\mathrm{CF}_1 < C_b$ when $\rho_p^{\mathrm{LQL}} = 0$ and $\rho_p^{\mathrm{AQL}} = 4$. This figure demonstrates that CF_2 decreases when n and/or m are on increase. As mentioned earlier, this trend is consistent with the nature of the cost function CF_2.

- Table reduced2: For $w = \frac{1}{3}$, the results are close to the reported outcomes of the second strategy (the lower part of Table reduced1) and for $w = \frac{2}{3}$, they are close to the parameters of the first strategy (the upper part of Table reduced1). Moreover, the inspection costs CF_1 and CF_2 in this table are larger than or equal to the optimal cost CF_1^* and CF_2^* reported in Table reduced1. reducedThese results are consistent with the structure of cost function CF_3.

3.5 Conclusion

In industrial production processes, product quality is often assessed by the ratio of two quality attributes, X and Y, which are typically monitored using control charts. Traditional control charts presume independent normal observations; however, frequent sensor data collection typically results in autocorrelation and cross-correlation between successive observations of X and Y, necessitating modeling to prevent false alarms. This chapter examines the efficacy of the Phase II Shewhart-type RZ control chart in monitoring the ratio of two normal variables, employing a bivariate autoregressive model (VAR(1)) to address the correlations. A numerical investigation examines the alterations in the design and statistical efficacy of the control chart with respect to the parameters of the VAR(1) model, illustrated through an example in a furnace operation. The chapter analyzes the influence of measurement errors on chart performance, broadening prior error models into a more comprehensive framework. It demonstrates that although precision and accuracy flaws affect performance, their impact is negligible until the errors are substantial. A conditional reliability sampling plan (CRSP) is developed, employing a progressive type-II censoring scheme and conditional operational characteristic functions, optimized through cost-effective procedures for inspection and imprecise lot sentencing. The chapter ultimately proposes further research avenues, such as the formulation of sophisticated reliability sampling plans, the utilization of the suggested choice statistic for alternative distributions, and the adoption of a Bayesian methodology employing MCMC techniques for intricate likelihood functions.

Furthermore, significant research has been conducted in statistical process control, particularly regarding the application of machine learning to improve anomaly detection in control charts. This research suggests incorporating machine learning into statistical process control charts to enhance the phases of design, pattern recognition, and interpretation [213]. We have developed an EWMA chart employing a measurement error approach to assess performance in the presence of measurement errors while monitoring the ratio of two normal variables [55]. Additionally, we examined one-sided synthetic RZ control charts for anomaly detection, which are especially beneficial in contexts involving measurement errors [152]. The application of a one-sided Shewhart control chart for monitoring the ratio of two normal variables in short production runs has been enhanced to align more closely with practical needs [209]. These studies enhance theoretical understanding and offer practical benefits in industrial applications, facilitating the optimization of manufacturing processes and the improvement of product quality [153, 149].

Chapter 4

Enhancing Anomaly Detection and Prognostics in Smart Manufacturing through Machine Learning, Federated Learning, and Blockchain for Security, Fair, and Transparent Industrial Systems

The content of this chapter is based on the following publications, in which I am a co-author:

- T.T.V. Nguyen, C. Heuchenne , K.D. Tran, G. Tartare, K.P. Tran. (2024). "SVDD Control Charts Based on Mewma Technique for Monitoring Compositional Data," Computers & Industrial Engineering, Elsevier,https://doi.org/10.1016/j.cie.2025.110865

- H.C Vu,K.D. Tran*, V.H Tran, K.P. Tran (2024). "Predictive Maintenance Optimization based on Genetic Algorithms for Future Industrial Systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_3

- T.Q.D. Pham, K.D. Tran*, K.T.P. Nguyen, X.V. Tran,L. Köehl, and K.P. Tran (2024). "A new framework for prognostics in decentralized industries: Enhancing fairness, security, and transparency through Blockchain and Federated Learning" Book: *Human-Centered Explainable Anomaly Detection for Smart Manufacturing in Industry 5.0*, Springer Nature Switzerland AG. Submitted.

- T.H. Nguyen, A. Saghir, K.D. Tran*,D.H. Nguyen,N.A. Luong, K.P. Tran (2024). "Safety and Reliability of Artificial Intelligence systems" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_9

- T. Nguyen, D.H. Nguyen, Q.T. Nguyen, K.D. Tran*, K.P. Tran (2024). "Human-Centered Edge AI and Wearable Technology for Workplace Health and Safety in Industry 5.0" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_8

- D.H Nguyen, T.H. Nguyen,K.D. Tran*, K.P. Tran (2024). "Physics-informed Machine Learning for Industrial Reliability and Safety Engineering: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_2

- L.H Nguyen, K.D. Tran*, X. Zeng, K.P. Tran (2024). "Human-Centered Edge Artificial Intelligence for Smart Factory Applications in Industry 5.0: A Review and Perspective" Book: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges*, Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-031-71495-5_5

- T.P. Bac, D.T. Ha, K.D. Tran*, K.P. Tran (2023). "Explainable Artificial Intelligence for Cybersecurity in Smart Manufacturing" Book: *Artificial Intelligence for Smart Manufacturing: Methods, Applications, and Challenges*. Springer International Publishing, pp. 199-223. http://dx.doi.org/10.1007/978-3-031-30510-8_10

- T.H. Nguyen, H.D. Nguyen, K.D. Tran, D.D.K. Nguyen, K.P. Tran (2022). "Enabling smart supply chain management with artificial intelligence" Book: *Machine Learning and Probabilistic Graphical Models for Decision*

Support Systems. CRC Press, pp. 294-310. http://dx.doi.org/10.1201/9781003189886-12

- P.H. Tran, A.A. Nadi, T.H. Nguyen, K.D. Tran, K.P. Tran (2022). "Application of machine learning in statistical process control charts: A survey and perspective" Book: *Control Charts and Machine Learning for Anomaly Detection in Manufacturing*. Springer Cham, pp. 7–42. https://link.springer.com/chapter/10.1007/978-3-030-83819-5_2

- L.H. Nguyen, Q.T. Nguyen, K.D. Tran*, H.D. Nguyen, S. Thomassey, X.Zeng, K.P. Tran, (2024), "Deep CNN for Remaining Useful Life Prediction: An XAI Approach Using SHAP for Model Interpretation," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- D.H. Nguyen, K.D. Tran*, N.A. Luong, M.A. Luong, K.P. Tran, (2024), "Artificial Intelligence for Human Resource Management: A Review, Perspective, and Case Study," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- T. Nguyen, K.D. Tran*, A. Raza, Q.T. Nguyen, H.M. Bui, K.P. Tran (2023). "Wearable Technology for Smart Manufacturing in Industry 5.0: Applications, Challenges, and Case Studies" proceeding of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283956_Wearable_Technology_for_Smart_Manufacturing_in_Industry_50_Applications_Challenges_and_Case_Studies

- T.H. Nguyen, H.D. Nguyen,K.D. Tran*, D.D.K. Nguyen, P.H. Tran, K.P. Tran (2023). "Smart Supply Chain Management with Artificial Intelligence: A Survey and Perspective", Proceedings of the *ISSAT International Conference on Data Science in Business, Finance, and Industry (DSBFI 2023)*, Da Nang, Vietnam. https://www.researchgate.net/publication/368283704_Smart_Supply_Chain_Management_with_Artificial_Intelligence_a_survey_and_perspective

4.1 Introduction

In the rapidly evolving global industry landscape, enterprises across various sectors, including aerospace, automotive, and manufacturing, are undergoing significant transformations driven by the principles of Industry

5.0, which emphasizes human-machine collaboration, resilience, sustainability, and personalized, human-centered manufacturing. Artificial Intelligence (AI) has become integral in enhancing smart manufacturing environments, enabling real-time monitoring, process optimization, and predictive maintenance (PM). PM is particularly critical in industries with diverse and dynamic machine operations, as it reduces downtime and enhances cost-effectiveness [204]. However, AI-driven PM models face challenges stemming from centralized data systems, which pose risks related to data privacy, high costs associated with data transfer, and difficulties in accounting for unique operational conditions across factories. Federated Learning (FL) provides a decentralized solution by enabling model training on local data, thereby mitigating privacy concerns and reducing transfer costs. While FL provides significant advantages, it also introduces new complexities, such as managing diverse data formats and ensuring privacy during the exchange of model parameters. To address these issues, integrating Blockchain (BC) technology into the FL framework enhances security by ensuring immutable, transparent model updates and parameter exchanges across decentralized manufacturing sites. Despite the early stages of BC-based FL applications in PM, this combined approach promises secure, transparent, and efficient predictive maintenance systems aligned with the principles of Industry 5.0. Additionally, challenges in monitoring compositional data (CoDa) in industrial processes are also addressed through the use of specialized control charts. Traditional Statistical Process Control (SPC) charts are ill-suited for CoDa, which involves strict positive vectors of component proportions, necessitating the development of customized methods such as Dirichlet density transformations and Support Vector Data Description (SVDD) charts [16, 164]. Recent advancements include combining SVDD with the Multivariate Exponentially Weighted Moving Average (MEWMA) technique for practical Phase II monitoring of CoDa, offering a flexible and adaptable solution for industries with varying requirements. These innovations in CoDa monitoring complement the decentralization and security principles of Industry 5.0, demonstrating the potential for AI-driven, human-centered systems to revolutionize manufacturing environments through secure, transparent, and adaptable frameworks [260, 198, 132, 201].

To further enhance these efforts, the following objectives are identified:

- Objective 2.1: Investigate and implement various machine learning algorithms for effective classification and anomaly detection within smart manufacturing systems.

- Objective 2.2: Perform comparative analyses between machine learning approaches and traditional statistical methods (such as control charts) to evaluate performance metrics like accuracy, computational efficiency, and scalability.

- Objective 2.3: Validate the developed machine learning frameworks through case studies or simulations to ensure their robustness and practical viability in complex manufacturing settings. These objectives aim to integrate machine learning innovations with traditional manufacturing approaches to establish more robust, efficient, and scalable solutions for modern industrial challenges.

4.2 Contributions about Anomaly detection with Machine learning in CoDa

In this section, we introduce two approaches for monitoring and Anomaly Detection in CoDa using an SVDD control chart combined with the MEWMA technique, with a specific emphasis on the Phase II monitoring process, where the ongoing process is monitored to quickly detect deviations from normal conditions. Our work not only explores the performance of control charts using various transformation techniques but also emphasizes their practical adaptability in response to specific context requirements. These contributions highlight our efforts to enhance the monitoring of CoDa and its capacity to adapt to diverse industrial contexts. For example, simpler control charts may be preferred in environments where cost efficiency is essential, such as basic manufacturing. Conversely, in industries requiring high levels of quality control, like semiconductor or pharmaceutical manufacturing, more complex and accurate charts are necessary. This highlights the importance of selecting control charts tailored to specific operational contexts, allowing companies to strike a balance between cost and quality.

4.2.1 SVDD based approaches for monitoring and Anomaly Detection in CoDa

In ML, SVDD is a well-known algorithm for detecting anomalies (outliers). SVDD was first introduced by [204] and has been widely used in anomaly detection due to its assumption-free approach to the distribution of the observed data ([16], [164], and [260]). Although many studies on SVDD and its applications have been conducted, most have been developed for use with normal data. Due to the constraints of CoDa, this research cannot be applied directly without handling these constraints.

SVDD using MEWMA-based vectors

Recall that SVDD is a one-class classification algorithm used to detect abnormal observations by modeling the normal ones. This algorithm constructs a spherical-shaped boundary around the dataset, specified by its center $\mathbf{a}$ and radius R. The primary objective is to minimize the radius R, thereby minimizing the volume of the sphere while ensuring that it contains the majority of training objects. SVDD is widely utilized in practical applications to identify novel data points or outliers. Consider a training dataset collected over N sampling periods, where at each period $i = 1, \ldots, N$, a sample of m observations of p features is gathered. The dataset is denoted as $S = \{\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N\}$, where each $\mathbf{X}_i$ is an $m \times p$ matrix. To construct our model, we first compute the sample mean $\bar{\mathbf{x}}_i$ of each $\mathbf{X}_i$. This process yields a series of mean feature vectors, represented by $\bar{S} = \{\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2, \ldots, \bar{\mathbf{x}}_N\}$. We then generate the MEWMA vectors $\mathbf{w}_i$ using the formula:

$$\mathbf{w}_i = r(\bar{\mathbf{x}}_i - \boldsymbol{\mu}_0) + (1-r)\mathbf{w}_{i-1},\ i = 1, 2, \ldots, N \tag{4.1}$$

where $\boldsymbol{\mu}_0$ is the mean vector of the whole dataset, $\mathbf{w}_0 = \mathbf{0}$, $r \in (0, 1]$ is a fixed smoothing parameter, $\mathbf{w}_i$ has dimension p. These MEWMA vectors will be used to train the SVDD model. The SVDD optimization problem to obtain a description of the dataset using MEWMA-based vectors can be described by:

$$\begin{aligned} \min_{R,\mathbf{a}} \quad & R^2 + C\sum_{i=1}^{N} \xi_i \qquad (4.2)\\ \text{subject to} \quad & \|\mathbf{w}_i - \mathbf{a}\|^2 \le R^2 + \xi_i, \quad \xi_i \ge 0, \quad i = 1, \ldots, N. \end{aligned}$$

where C is the trade-off parameter introduced to control the balance between the volume of the sphere and the errors. Introducing two Lagrange multipliers α_i, γ_i, the dual problem of problem (4.2) will be:

$$\max_{\alpha} \left(\sum_{i=1}^{N} \alpha_i \langle \mathbf{w}_i, \mathbf{w}_+ \rangle - \sum_{i,j=1}^{N} \alpha_i \alpha_j \langle \mathbf{w}_i, \mathbf{w}_j \rangle \right) \tag{4.3}$$

$$\text{subject to} \begin{cases} \sum_{i=1}^{N} \alpha_i = 1, \\ 0 \leq \alpha_i \leq C, \quad \text{for } i = 1, \ldots, N. \end{cases}$$

The dual problem, being convex quadratic, is significantly more tractable than the original problem (4.2). Solving this problem and noting that the parameters γ_i are omitted during the solving process, we obtain the center $\mathbf{a}$ and the radius R of the sphere as follows:

$$\mathbf{a} = \sum_{SV} \alpha_s \mathbf{w}_s, \quad R^2 = \langle \mathbf{w}_k, \mathbf{w}_k \rangle - 2 \sum_{i=1}^{N} \alpha_i \langle \mathbf{w}_i, \mathbf{w}_k \rangle + \sum_{i,j=1}^{N} \alpha_i \alpha_j \langle \mathbf{w}_i, \mathbf{w}_j \rangle \tag{4.4}$$

where SV denotes the index set of the support vectors and $\mathbf{w}_k$ in the radius formula is any object that satisfies $\mathbf{w}_k \in SV_{<C}$, the set of support vectors having $\alpha_k < C$, see [204] for more details.

In general, to monitor new samples $\mathbf{Z}_1, \mathbf{Z}_2, \ldots,$ where each sample $\mathbf{Z}_t$ consists of m observations collected at time step t, we first compute their sample mean vectors $\bar{\mathbf{z}}_1, \bar{\mathbf{z}}_2, \ldots,$ and then transform them to the MEWMA vectors $\mathbf{w}'_1, \mathbf{w}'_2, \ldots,$ using formula (4.1). Following this transformation, we calculate the squared distance between these MEWMA vectors and the center $\mathbf{a}$ of the sphere, which can be computed as follows:

$$\mathbf{w}'_t - \mathbf{a}^2 = \langle \mathbf{w}'_t, \mathbf{w}'_t \rangle - 2 \sum_{i=1}^{N} \alpha_i \langle \mathbf{w}'_t, \mathbf{w}_i \rangle + \sum_{i,j=1}^{N} \alpha_i \alpha_j \langle \mathbf{w}_i, \mathbf{w}_j \rangle. \tag{4.5}$$

In practice, instead of using the inner product in the above formulas, we often use the kernel functions to obtain a more flexible data description. [218, 192] proposed some kernel functions for the Support Vector Classifier. One of the most popular kernel functions can be mentioned is the Gaussian kernel function $\mathrm{K}(\mathbf{w}_i, \mathbf{w}_j)$, which is defined by $\mathrm{K}_{\mathrm{G}}(\mathbf{w}_i, \mathbf{w}_j) = \exp(-\mathbf{w}_i - \mathbf{w}_j{}^2/\sigma^2)$ where σ is used to control the complexity of the SVDD boundary. If the kernel function $\mathrm{K}(\mathbf{x}, \mathbf{y})$ is used, the squared distance in Equation (4.5), denoted by

$\mathrm{D}_{\mathbf{a}}(\mathbf{w}')$, will be:

$$\mathrm{D}_{\mathbf{a}}(\mathbf{w}'_t) = \mathrm{K}(\mathbf{w}'_t, \mathbf{w}'_t) - 2\sum_{i=1}^{N} \alpha_i \mathrm{K}(\mathbf{w}'_t, \mathbf{w}_i) + \sum_{i,j=1}^{N} \alpha_i \alpha_j \mathrm{K}(\mathbf{w}_i, \mathbf{w}_j). \tag{4.6}$$

Support Vector Data Description control chart

To construct the SVDD control chart, [198], [132], and [201], among other authors, proposed using the kernel distance defined in Equation (4.6) as the chart statistic. The radius R of the sphere is a candidate for the upper control limit threshold. However, in the framework of SPC, the upper limit h based on pre-specified in-control ARL (denoted by ARL_0) is more appropriate. In this case, the control chart would give an out-of-control signal if the kernel distance $\mathrm{D}_{\mathbf{a}}(\mathbf{w}_t)$ between the MEWMA vector $\mathbf{w}_t$ of the current sample mean $\bar{\mathbf{z}}_t$ and the center $\mathbf{a}$ of the SVDD sphere is greater than h.

Since the chart statistic $\mathrm{D}_{\mathbf{a}}$ does not have a known standard distribution, obtaining an appropriate value of h to achieve the pre-specified ARL_0 is challenging. To address this problem, [201], among others, suggested determining the value of h by simulation, employing bootstrap percentile techniques. These methods help us to find the adjusted control limit to assure that the probability of ARL_0 attaining or exceeding the desired value is close to a high specified value $(1-\epsilon)\cdot 100\%$, where ϵ is a small specified constant, e.g., $\epsilon = 0.1$. In this work, we adopt the bootstrap percentile approach proposed by [201] to establish the control limit for our SVDD control charts. Consider a training data set of size N: $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$, where each $\mathbf{x}_i$ is a vector in $\mathbb{R}^n$. The procedure to obtain the upper limit threshold h using the bootstrap percentile method is summarized as follows:

Algorithm 3: Determining the upper limit threshold h for the SVDD control chart.
Input: Training data set of size N: $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N$.
Output: Upper limit threshold h of SVDD control chart.

Step 1: Generate M independent bootstrap samples of size N from the training set.

Step 2: **For** each bootstrap sample j^{th} where $j = 1, \ldots, M$ **do**

Step 3: Execute the SVDD algorithm to determine the SVDD sphere for the bootstrap sample.

Step 4: Use formula (4.6) to compute N statistics $\mathrm{D}_{\mathbf{a}^{(j)}}(\mathbf{x}_1^{(j)}), \ldots, \mathrm{D}_{\mathbf{a}^{(j)}}(\mathbf{x}_N^{(j)})$ from j^{th} bootstrap sample, where $\mathbf{a}^{(j)}$ is the center of sphere obtained from j^{th} bootstrap sample.

Step 5: Let ARL_0 be the pre-specified in-control ARL and $\beta = \frac{1}{\mathrm{ARL}_0}$ be the desired false alarm rate. Calculate $100 \times (1-\beta)^{th}$ percentile of the set of N statistics. This value presents the estimated limit threshold obtained from the current bootstrap sample, denoted by $h^{(j)}$.

Step 6: **End for**

Step 7: Determine the final control limit h by identifying the $100 \times (1 - \epsilon)$ percentile of estimated limit thresholds $h^{(j)}, j = 1, \ldots, M$, where ϵ is a small predetermined constant.

This established limit threshold h will be used to monitor new objects. An out-of-control signal is issued if the monitoring statistic for the new object exceeds h. This method ensures a consistent approach to finding the threshold that balances sensitivity and specificity in the SVDD model [132].

SVDD-EWMA control charts for monitoring multivariate CoDa

In this subsection, we detail the construction of two SVDD control charts based on MEWMA-transformed vectors, using the transformation methods. Let's consider an in-control multivariate CoDa set of size N, represented by $\mathbf{X}_1, \ldots, \mathbf{X}_N$, each $\mathbf{X}_i$ encompasses l CoDa vectors $\mathbf{x}_i^{(1)}, \ldots, \mathbf{x}_i^{(l)}$ with the number of parts $p_1, p_2, \ldots, p_l$, Chaque observation $\mathbf{X}_i$ can be expressed as:

$$\mathbf{X}_i = \left[\mathbf{x}_i^{(1)}, \ldots, \mathbf{x}_i^{(l)}\right] = \left[x_{i1}^{(1)}, x_{i2}^{(1)}, \ldots, x_{ip_1}^{(1)}, \ldots, x_{i1}^{(l)}, x_{i2}^{(l)}, \ldots, x_{ip_l}^{(l)}\right].$$

We also assume that the constraint on each CoDa vector is equal to 1, i.e., $\sum_{k=1}^{p_q} x_{ik}^{(q)} = 1$ for $i = 1, \ldots, N$ and $q = 1, \ldots, l$. The procedure for designing the SVDD control chart for monitoring the multivariate CoDa using the Dirichlet density transformation method (denoted by $\mathrm{S}_{\mathrm{Dir}}$) is given in [217]

4.2.2 Performance of the SVDD-EWMA approaches for monitoring and Anomaly detection in CoDa

This section compares the performance of the two proposed control charts for monitoring multivariate CoDa: the SVDD-MEWMA control chart using

Dirichlet density transformation S_{Dir}, the SVDD-MEWMA control chart using ilr transformation S_{ilr}, with the traditional MEWMA control chart $MEWMA_C$ proposed by [207]. Designed based on the assumption that CoDa follows a normal distribution within the Simplex space and employing the ilr transformation, $MEWMA_C$ has demonstrated superiority over T^2-CoDa charts. Incorporating the $MEWMA_C$ control chart as a comparison provides a benchmark for evaluating the performance of our proposed SVDD-based control charts. To perform the comparison, we simulate scenarios using a single CoDa feature to demonstrate the effectiveness of our proposed charts. This approach reduces computational costs and enhances practical applicability, especially for engineers and practitioners. The methodologies presented here can be readily extended to multivariate CoDa scenarios, allowing for flexible adaptation to specific practical contexts, as discussed in the sections above. Our comparison is conducted through a simulation involving CoDa datasets generated from Dirichlet distributions, assessing the charts based on the zero-state out-of-control average run length (ARL_1) while constraining on the same pre-specified in-control value (ARL_0). The zero-state ARL_1 assumes that when a process shift occurs, we start monitoring from scratch, with control chart statistics reset to their initial values. This approach provides a theoretical measure of the chart's responsiveness to shifts. In contrast, the steady-state ARL_1 considers all prior data and reflects the chart's performance during ongoing monitoring when control statistics have stabilized over time. A control chart with a smaller zero-state ARL_1 indicates better performance, as it signifies a quicker and more effective detection of out-of-control conditions. This approach aligns with numerous studies that consider zero-state ARL_1 in evaluating control chart performance (see [95], among others). For brevity and convenience, we will hereafter refer to the zero-state ARL_1 simply as ARL_1 throughout this work.

In summary, our comparative analysis reveals that S_{ilr} generally outperforms the other control charts in detecting shifts in CoDa, offering higher sensitivity across most tested scenarios. It also has the smallest SDRL and MRL in almost all scenarios, making it the most reliable and responsive option for consistent and timely process monitoring. Besides, the efficiency of S_{Dir} and $MEWMA_C$ charts can vary depending on the specific process shifts and the chosen smoothing parameter r. Notably, at higher r values, S_{Dir} tends to outperform MEWMA, especially when the shifts involve an increase in the smallest component of CoDa. This suggests that S_{Dir} may be better at detecting certain types of shifts within the data. Practitioners can integrate the proposed approaches into their quality control systems by considering the following key points:

- Computational resources: Evaluate the available computational infrastructure. S_{ilr} requires more computational power due to higher data dimensionality and complex SVDD training. If resources are limited, S_{Dir} or the traditional $MEWMA_C$ may be more practical choices.

- Data characteristics: Check the distribution of the dataset to choose the most suitable control chart.

- Sensitivity requirements: Determine the level of sensitivity needed for detecting deviations in the process. S_{ilr} provides rapid and sensitive detection, hence suitable for critical processes where early intervention is essential. S_{Dir} and $MEWMA_C$, while less sensitive, offer simplicity and lower computational costs, making them suitable for processes where high-quality controls are not required.

- Implementation complexity: Assess the technical expertise of the team and the ease of integrating new tools. SVDD-based charts as S_{ilr} and S_{Dir} may require higher experiment engineers and modern software for handling advanced computations, while $MEWMA_C$ is easier to implement and may be more accessible for teams without specialized machine learning experience.

4.3 Contributions about Reliability Prediction and Predictive Maintenance

In the rapidly evolving landscape of global industries, enterprises across sectors such as aerospace, automotive, and manufacturing are undergoing significant transformations driven by Industry 5.0 [263, 181]. While Industry 4.0 focuses on automation, data exchange, and cyber-physical systems, Industry 5.0 emphasizes the collaboration between humans and intelligent machines, fostering a more personalized, human-centered approach to manufacturing. This paradigm shift prioritizes resilience, sustainability, and human-machine symbiosis, with Artificial Intelligence (AI) and advanced technologies playing central roles in creating smart manufacturing environments.

AI's integration into smart manufacturing brings enhanced efficiency and predictive capabilities, enabling real-time monitoring, process optimization, and more effective decision-making. Within this context, predictive maintenance (PM) [114, 81, 63] has emerged as a key application, particularly in industries that manage an extensive array of machines, each operating under distinct and dynamic conditions. Predictive maintenance not only reduces unplanned downtime and enhances cost-effectiveness but also aligns with the core principles of Industry 5.0, which focuses on adaptability, efficiency, and human-centered innovations.

However, the adoption of AI-driven PM introduces a significant challenge: the centralized data models that traditionally power AI [114, 81]. Centralized models require vast amounts of data to be transferred to a central server for training. This poses concerns related to high costs, data privacy, and the specific operational conditions unique to each facility or organization. These issues become more pronounced as industries grow increasingly interconnected, making the need for decentralized data management solutions critical. In summary, these issues can be summarised as:

- **Data Privacy and Security**: Centralized data systems require sensitive information to be transferred and stored in a single location, increasing vulnerability to breaches and misuse. Securing this data without relying on centralized repositories is crucial in a decentralized industrial ecosystem.

- **Cost and Efficiency**: Transferring vast amounts of data to centralized servers incurs high costs in terms of bandwidth and storage, which may negate the efficiency gains promised by AI.

- **Diverse Operating Conditions**: Centralized models struggle to account for the unique operating environments of individual manufacturing sites. Each factory or machine may face different stressors and maintenance needs, which are not easily generalized in a centralized framework.

Federated Learning (FL) [8, 257] addresses these challenges by offering a decentralized approach to model training. Instead of transferring all data to a central server, FL allows each entity (i.e., a factory) to train predictive models on its local data. The model parameters, not the data itself, are then shared with a central server, where they are aggregated to create a more generalized model. This approach ensures data privacy, reduces transfer costs, and reflects the diverse operating conditions across all participating entities. However, as Industry 5.0 brings further complexity to manufacturing systems, even FL presents challenges [135, 121, 101]. These include managing diverse data formats, minimizing communication overhead, ensuring privacy during parameter exchanges, and accounting for the varied data characteristics of each participant.

An efficient way to resolve the problem is to integrate blockchain (BC) technology [158, 53] into the FL framework. This advantage highlights both technologies' potential benefits and addresses the complex obstacles that arise [123, 128]. Including BC's immutable and transparent system within FL adds an extra layer of security, ensuring the integrity and verifiability of model updates and parameter exchanges across the distributed network of manufacturing sites. This, in turn, mitigates concerns over potential data breaches and unauthorized access, gaining trust within the collaborative ecosystem [147]. BC's decentralized nature also matches with FL's philosophy, as each site's locally trained models can be securely aggregated without a centralized authority. This integration facilitates secure and efficient model aggregation, amplifying the decentralized essence of FL itself [131, 18].

Currently, BC-based FL in RUL prediction is still in its early stages. Particularly, BC-based FL is mainly focused on the IoT and healthcare fields [117, 84], which are outside the scope of our work. Furthermore, these studies tend to concentrate on either intricate statistical and federated learning principles or on relatively complex industrial models, which may not be readily understandable to individuals new to the field.

Based on these backgrounds, the combination of BC and FL is particularly promising for Industry 5.0, where human-machine collaboration is key and personalized, context-aware systems need to be built on secure, transparent, and decentralized infrastructures. BC-empowered FL frameworks foster human-centric AI by enabling secure, adaptive learning across diverse manufacturing settings while maintaining strict privacy and security standards. Despite the early stage of BC-based FL applications in PM and RUL prediction, their potential is immense. While initial research has primarily focused on IoT and healthcare, this section aims to extend these advancements to smart manufacturing, thereby bridging a gap in the existing literature. This section presents a novel framework that leverages the combined potential of FL and BC technologies to enable efficient RUL predictions in decentralized industries. The primary goal is to facilitate secure, privacy-preserving, and cost-effective PM while ensuring full transparency and trust. In doing so, we address the key challenges posed by centralized data models, bringing the decentralized essence of Industry 5.0 to PM systems. Moreover, we are committed to transparency and collaboration; thus, all the code related to this research is open-source on GitHub, inviting engagement and contributions from the broader community.

Proposed Framework for BC-based Federated Learning in Remaining Useful Life Predictions

Blockchain is the fundamental component in creating a completely decentralized and secure architecture designed for federated learning systems in our proposed framework. This integration provides robust measures for safeguarding sensitive data, fostering trust among stakeholders, and reducing security vulnerabilities. Thus, it holds significant importance in applications related to remote machinery monitoring, anomaly detection, problem diagnosis, and, importantly, Remaining Useful Life (RUL) assessment for essential and safety-critical systems.

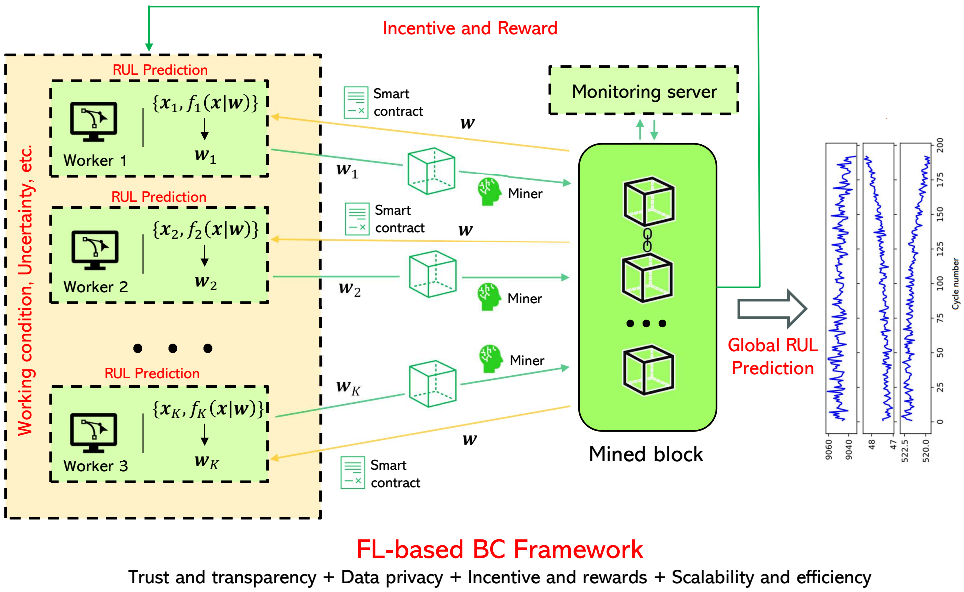


FIGURE 4.1: Proposed architecture for blockchain-based federated learning in remaining useful life prediction.

The proposed BC-integrated FL framework for RUL predictions, illustrated in Figure 4, is systematically organized into six essential components: (1) worker i, (2) smart contract, (3) active miners $\mathcal{M}_j$, (4) mined block, (5) consensus algorithm, and (6) monitoring server. These components work collaboratively to enhance RUL predictions across various industrial sectors, including manufacturing, automotive, and aerospace. As seen in the Figure. Figure 4.1 illustrates the Remaining Useful Life (RUL) forecast utilizing a Blockchain-based architecture for Federated Learning, which consists of six essential components: (1) worker i, (2) smart contract, (3) active miners $\mathcal{M}_j$, (4) mined block, (5) consensus method, and (6) monitoring server.

- **The following items:**

(1) **Worker** i**:** Each worker signifies a participating entity in the federated learning process. It retains local data, such as condition monitoring records from industrial machinery or airplanes, and facilitates the enhancement of predictive models. This approach ensures that the exact specifics of Remaining Useful Life under various operating conditions are fully understood and taken into account.

(2) **Smart Contract:** It serves as the digital foundation of the FL framework, encapsulating the regulations and protocols that dictate the joint endeavor. In Remaining Useful Life projections, the system might, for instance, autonomously verify the precision of data from a jet engine's sensors. Should the data satisfy established conditions, the model will be revised. It also oversees the allocation of incentives, motivating factories or aircraft systems to deliver high-quality data by awarding them tokens or credits in exchange. The SC is the unbiased enforcer that guarantees all activities, from data submission to model update, comply with the prescribed procedures. The SC functions as a self-executing contract, with the terms and conditions of the FL process embedded inside it. It automates several facets of federated learning, encompassing model updates, incentive allocation, and consensus protocols.

(3) **Active Miners** $\mathcal{M}_j$**:** Miners within the blockchain serve as custodians of data integrity and security. In the realm of Remaining Useful Life predictions, miners verify the sensor data or predictive model updates provided by each worker before they are permanently recorded on the blockchain. This procedure is essential to prevent the incorporation of erroneous or malicious data that could lead to inaccurate RUL projections, potentially resulting in premature component failure or unwarranted maintenance downtime. Miners are specialized nodes tasked with verifying transactions and generating new blocks on the blockchain. In the realm of federated learning, they are essential for maintaining the integrity and security of the federated learning process. Miners authenticate the model changes from factories and incorporate them into the blockchain, ensuring the precision of the decentralized ledger.

(4) **Mined Block:** Each mined block constitutes a compilation of verified updates, resembling a time-stamped aggregation of RUL insights from the network, which may include parameters of prognostic models. The distinctive cryptographic hash in each block serves as a seal, securing its position in the blockchain ledger and connecting it to the prior

block, therefore establishing an immutable chain of RUL predictions and model enhancements. A mined block is a collection of verified transactions that are included in the blockchain. In the context of federated learning, this encompasses the model updates provided by factories. Every block contains a distinct cryptographic hash, which connects it to the preceding block and ensures the immutability of the FL process. This document contains a comprehensive record of all actions inside the FL network.

(5) **Consensus Algorithm:** This protocol guarantees agreement among nodes in the blockchain network over the legitimacy of transactions and the sequence in which they are incorporated into the blockchain. Within the framework of federated learning, the consensus algorithm determines whether to accept or reject model updates based on established criteria. The global model for Remaining Useful Life projections is updated just when a majority of nodes concur that the information provided by a worker, including the parameters of the prognostic model, is accurate and aligns with the requirements of the entire system. This collective validation procedure enhances the reliability of the RUL predictions.

(6) **Monitoring Server:** The monitoring server is essential for supervising and orchestrating the FL process. It offers insights into the performance of participating personnel, guaranteeing that their information contributions are prompt and accurately represent their status. It also tracks the model's learning advancement, guaranteeing that the RUL predictions are as accurate as possible. Moreover, it enhances the transmission of information across the various components of the FL network, guaranteeing efficient operations and dependable RUL predictions.

The six components collectively provide the framework of the BC-enhanced FL system. This configuration facilitates the secure, confidential, and collaborative training of models across autonomous production locations. The process persists, iterating through updates and validations, until the comprehensive prognostic model has stabilized or reached the requisite degree of accuracy. This is vital for Remaining Useful Life (RUL) prediction, as accurate model convergence guarantees dependable projections of equipment longevity, which is critical for maintenance scheduling and resource allocation. The precise functionality of the BC-supported FL algorithm is extensively elucidated in the algorithm

Technical Aspects of How BC Mitigates Key Challenges in FL for RUL Prediction Context

The integration of blockchain technology with federated learning presents significant potential for predicting the remaining useful life of components or systems. BC guarantees data privacy, encourages data contributions, and facilitates scalability. It protects sensitive RUL data, promotes data interchange, and accommodates various systems. Our proposed BC-FL architecture addresses these elements to enhance the precision and reliability of RUL predictions. The specifics are as follows:

- **Trust and transparency:** Blockchain technology provides an immutable ledger for documenting and validating each modification to the Remaining Useful Life prediction model. This transparency fosters confidence among participants and delineates a clear history of contributions. Smart contracts used on the blockchain may enforce predetermined rules, ensuring equity and transparency in the fuzzy logic-based rule prediction process. Let i represent a participating worker (i.e., from a factory or aerospace firm) in the BC-based FL process. The architectural foundation for worker i's participation in the FL-based RUL prediction training process is illustrated in Figure 4.2.

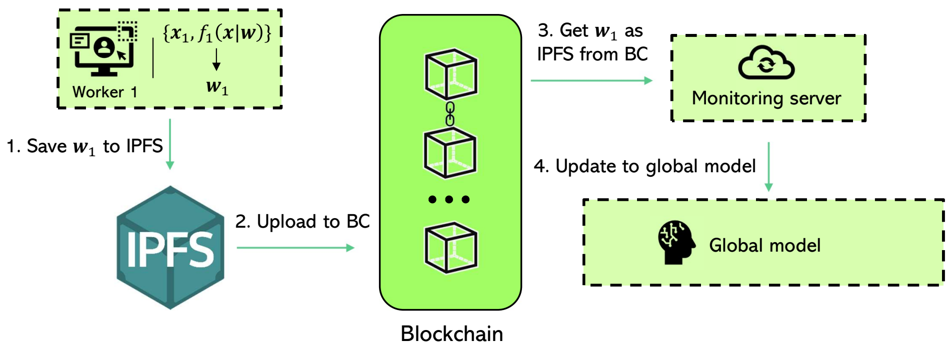


FIGURE 4.2: Architecture for the participation of worker i in the training process of Remaining Useful Life (RUL) prediction.

This procedure encompasses the subsequent steps:
(i) *Store w_1 on IPFS*: Assume that worker 1 has effectively trained a machine learning model for remaining useful life prediction. The worker can thereafter save the model parameters, namely w_1, in the InterPlanetary File System (IPFS) [48]. This phase minimizes the data format when uploading to BC, utilizing a hash link rather than a large file. This section utilizes the NFT. Storage gateway for data retention in decentralized networks.

(ii) *Upload to BC*: After successfully storing the model weights w_1 on IPFS, the subsequent essential step in the context of RUL predictions is to document the associated hash on the blockchain using a smart contract. This smart contract serves as an immutable ledger, thereby securing the model's state on the blockchain. In doing so, we provide a permanent record of the model's weights, enhancing transparency and traceability in the FL process, which is particularly crucial for assessing the RUL of systems. This unalterable record guarantees the integrity of the RUL prediction model throughout its existence, facilitating dependable and verifiable RUL predictions.
(iii) Updating the global model: Upon acquiring the model weights w_1, the central server, responsible for maintaining the global model, is prepared to integrate these new weights. This Florida-based Remaining Useful Life estimation technique is crucial. It integrates the collective expertise obtained from diverse laborers (e.g., factories or aerospace firms), a vital component in assessing the Remaining Useful Life (RUL) of machinery or aircraft. This joint initiative enhances and improves the accuracy of the global model, thereby increasing the precision of RUL predictions.

- **Data privacy and security:** Blockchain technology employs advanced cryptographic methods that are essential for enhancing security in the realm of systems' Remaining Useful Life estimates. These cryptographic techniques provide data encryption, further enhanced by documenting access permissions on the blockchain. This integrated method enhances the safeguarding of sensitive RUL data. The decentralized security protocol intrinsic to the blockchain, together with its immutable characteristics, is crucial for managing RUL predictions. Consequently, it adeptly addresses the persistent issue of maintaining data privacy and security in federated learning methodologies, which aim to assess the remaining useful life of systems. When integrating blockchain with federated learning to enhance data privacy and security, it is essential to recognize the inherent privacy and security attributes of blockchain, even in a public blockchain context. This attribute guarantees that uploaded data, including FL model weights, are intrinsically safeguarded. Nonetheless, supplementary security measures are essential when tailored to the unique demands of RUL prediction. To enhance data security in RUL prediction, we offer a proactive method. We propose incorporating RSA encryption and decryption methods, as outlined in Hamza et al. (2020) [80], alongside the hash value before uploading data to the blockchain. Figure 4.3 illustrates that this method encodes data as an IPFS hash link. This robust security technique ensures that RUL prediction data is meticulously protected throughout the FL process, in accordance with the rigorous privacy and security requirements of estimating systems' RUL.

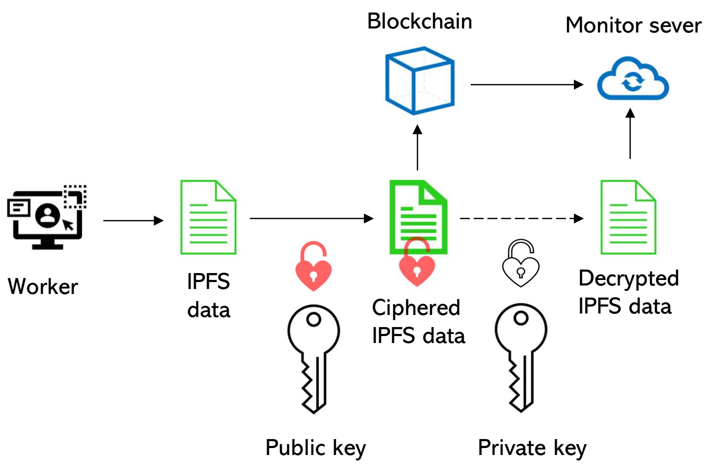


FIGURE 4.3: Integration of RSA encryption and decryption with the hash value before uploading data to the blockchain as an IPFS hash link.

This method enhances data security and provides an extra layer of protection. It guarantees that unauthorized individuals cannot interpret the data without the requisite private key, even if they have access. This supplementary security measure is especially vital when assessing the Remaining Useful Life of essential safety devices. This stage, depicted in Figure 4.3, ensures that only the central server, tasked with global model updates, can decode the IPFS hash link and access the data. In the realm of RUL prediction, this level of data security is essential, as it protects the integrity and confidentiality of vital information during the FL-based RUL estimation process. The Python code example illustrates the aforementioned procedure.

- **Incentives and rewards:** BC-based tokens or cryptocurrencies may be utilized to mitigate this issue. Smart contracts can automate the allocation of incentives based on the quality and quantity of contributions. Moreover, a public record of contributions and rewards on the blockchain guarantees fair remuneration for participants. This method guarantees that factories or aviation businesses receive fair compensation for their significant contributions when evaluating machinery or an aircraft's Remaining Useful Life (RUL). In addition to financial incentives, it encourages active engagement. It cultivates a self-sustaining ecosystem surrounding the federated learning process, hence improving the precision and efficacy of Remaining Useful Life estimates. The use of blockchain technology presents a distinctive potential to establish transparent and immutable incentive frameworks, tackling a crucial challenge frequently faced in collaborative machine learning projects. Figure 4.4 depicts the architecture that facilitates worker i in the automated and smooth uploading and receipt of incentives from the blockchain.

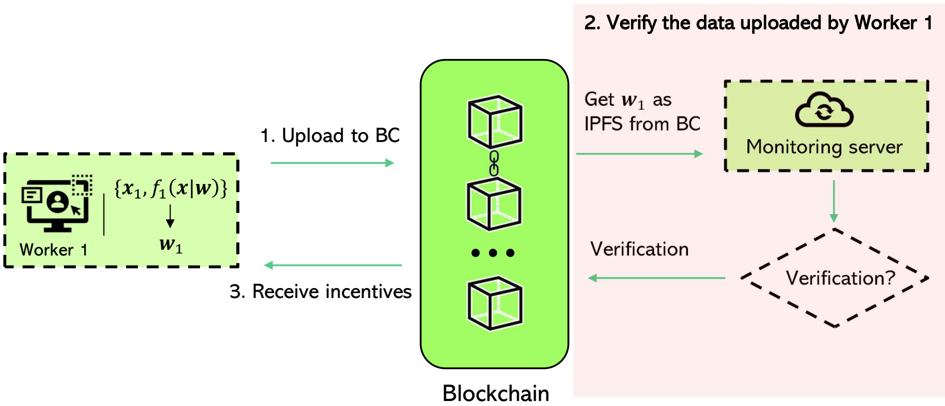


FIGURE 4.4: Architecture facilitating the automated and smooth upload of data by worker i and the receipt of rewards from the blockchain.

This procedure encompasses the subsequent steps:

(i) *Upload to BC:* Initiate the upload of pre-trained weights w_1 to the BC. It is essential to highlight that, to enhance the security and privacy of employee data, we recommend implementing the RSA key before uploading the IPFS hash to the blockchain.

(ii) *Authenticate the data sent by a worker:* In the realm of Remaining Useful Life projections for critical safety systems, it is imperative to mitigate the risks associated with malicious data submissions and unintentional errors. Such acts may alter the global model update, profoundly affecting the precision of RUL predictions. Although FL's training process provides certain safeguards against these issues, it may not encompass all potential attack paths that attackers can use. To mitigate the risk of inaccurate or deceptive data uploads, we propose implementing an automated verification service overseen by a backend monitoring server. This service is essential in the RUL prediction process, as seen in Figure 4.4. The process includes implementing the new weights in the global model and evaluating their impact on predicted accuracy enhancement.

Should the revised weights improve the global model's accuracy, they activate processes within the blockchain system, resulting in the distribution of incentives to the corresponding worker. This not only encourages authentic contributions but also protects against malicious efforts to distort the RUL prediction process, thereby enhancing the precision and dependability of RUL predictions in essential safety systems.

(iii) *Receive incentives:* Motivated by the strong cryptographic foundations of blockchain, factories engaged in the Remaining Useful Life prediction process can be incentivized with tokens [221] or Non-Fungible Tokens (NFTs) [233] on the blockchain platform. This new method serves as a significant incentive, prompting factories to undertake essential duties such as validating and preserving data integrity. Our approach integrates a monitoring server to evaluate the quality of prognostic parameters given by workers for global model updates in the context of Remaining Useful Life estimates for essential safety devices. A token or NFT enhances the worker via blockchain transactivation. This incentive system fosters confidence while also enhancing involvement and responsibility. Consequently, employees may use these tokens or NFTs as vouchers or for various relevant prizes provided by the central entity managing the FL process, thereby reinforcing their dedication to precise and dependable RUL predictions.

- **Scalability and efficiency:** BC technology, with its consensus methods like sharding or sidechains, offers substantial improvements in scalability and efficiency. The responsibilities related to RUL prediction, encompassing computation and validation, may be efficiently allocated throughout the BC network. This distribution mitigates the burden on a centralized server. It facilitates the effective processing of extensive data sets. Moreover, BC's integration with SC enhances the efficiency of the aggregation process, as seen in Figure 4.5. These SCs automate and improve data aggregation, markedly improving the efficiency of FL. This automation is essential for executing FL in large and varied environments, where RUL predictions are crucial for optimizing maintenance schedules and resource distribution.

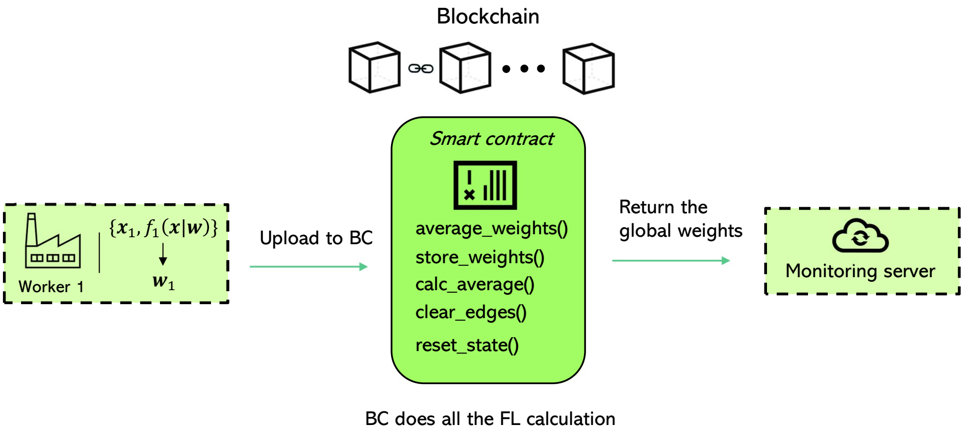


FIGURE 4.5: Proposed blockchain architecture for scalability and efficiency: Federated Learning-based blockchain.

Specifically, Figure 4.5 illustrates the suggested blockchain infrastructure designed to enhance the scalability and efficiency of the federated learning-based blockchain. The fundamental concept is creating a blockchain infrastructure that can accept uploaded weights from participating factories via IPFS hashes and/or a numerical array. The complete range of FL calculations is independently performed within this BC network. This includes weight averaging, accuracy evaluation, and the distribution of global weights. Incorporating the Remaining Useful Life forecast into this process improves operational efficiency and scalability. By integrating these intricate computations into the BC network, as seen in Figure 4.5, we expect a substantial improvement in the scalability and operational efficiency of FL initiatives focused on RUL predictions. This method enhances workflow efficiency, maximizes resource use, and leads to more precise and dependable Remaining Useful Life predictions in varied and extensive industrial settings.

4.3.1 Case Study

This section epresents a case study that illustrates how the proposed framework, integrating BC and FL, effectively addresses significant issues, particularly concerning RUL predictions for critical safety, leveraging the intrinsic advantages of both platforms, we aim to address critical challenges such as trust, data privacy, incentives, and scalability, all of which are essential for accurate and reliable dependable RUL predictions.

Our use case leverages the synergy between BC's immutable ledger and FL's privacy-preserving methodology, emphasizing their significance in RUL predictions for aviation systems. These applications signify a transition towards a transparent, safe, and efficient machine learning environment designed for remaining useful life prediction. Our discourse is systematically organized for widespread accessibility and influence, providing insights into the possibilities of this integrated strategy in enhancing RUL predictions.

Case study description

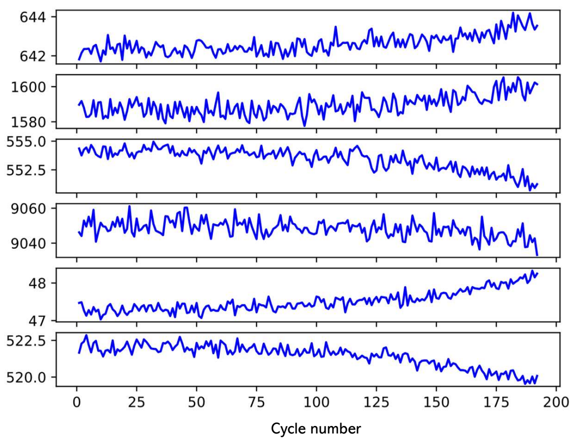
This case study utilizes the Commercial Modular Aero-Propulsion System Simulation (CMAPSS) dataset, created by the NASA Army Research Lab, to illustrate the effective application of the suggested framework to essential safety systems such as aircraft engines. This dataset is esteemed as a standard for Remaining Useful Life (RUL) prediction [175, 227].

The C-MAPSS dataset has four sub-datasets: FD001, FD002, FD003, and FD004, each reflecting distinct operational circumstances and fault patterns. Each sub-dataset has both training and testing datasets. Figure 4.6 presents an explanation of the CMAPSS dataset features and depicts six random samples throughout the entire life cycle.

Certain column properties do not yield valuable information for the Remaining Useful Life calculation. Consequently, 14 of the 21 sensor data points and two of the three operational conditions, amounting to 16 features, are selected as the raw input features for the model, consistent with previous research [175, 97, 229]. The selected columns are 3, 4, 6, 7, 8, 11, 12, 13, 15, 16, 17, 18, and 1presents the RUL prediction outcomes using the proposed BC-based FL, as mentioned in Subsection.

Data explanation	
Column	Definition
1	Engine unit
2	Cycle number
3-5	Working conditions
6-26	21 raw sensor data

(a)



(b)

FIGURE 4.6: (a) Explanation of features in the CMAPSS dataset and (b) Depiction of six random sensor data during a whole life cycle.

RUL prediction outcome

This section presents the RUL prediction outcomes using the proposed BC-based FL, as mentioned in Subsection. 4.3. This study employs the SV in the federated learning process, utilizing the Binance Smart Chain (BSC test-net) blockchain to illustrate the rate of the blockchain-based federated learning architecture. To evaluate forecast accuracy, we employ the root mean squared error (RMSE) metric, a commonly used standard in remaining useful life (RUL) prediction research [114, 63].

Figure 4.11 depicts the Remaining Useful Life predictions for testing engine units with the FL-based BC throughout many periods of CMAPSS. To clarify, we randomly picked one unit from FD001, FD002, FD003, and FD004 to illustrate the findings. The synchronous FL-based BC has a notable capacity to precisely identify maintenance needs, particularly for FD002 and FD004, contingent upon the machine being stopped at the first sign of the red line.

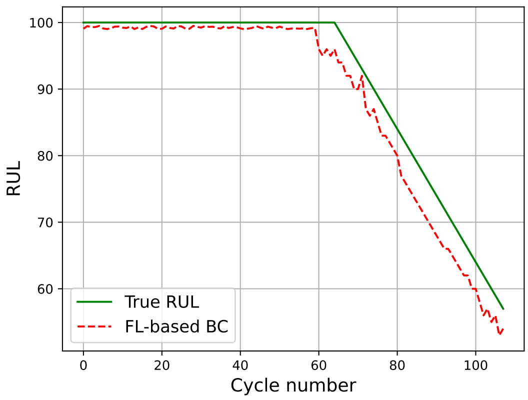


FIGURE 4.7: FD001

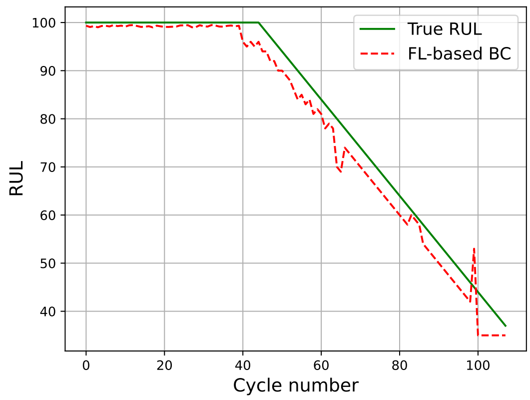


FIGURE 4.8: FD002

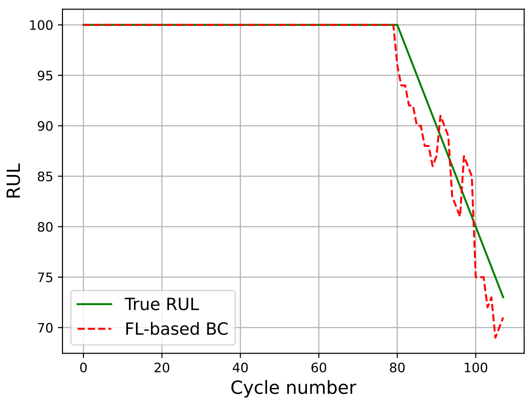


FIGURE 4.9: FD003

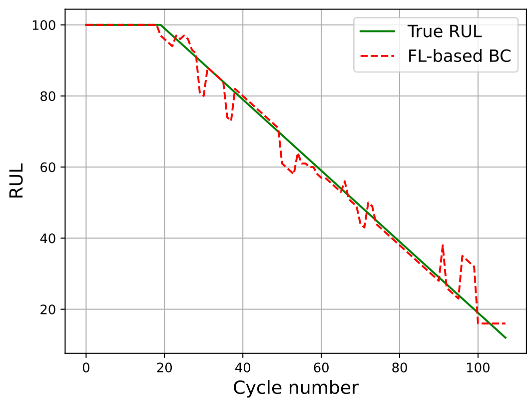


FIGURE 4.10: FD004

FIGURE 4.11: RUL predictions for testing engine units based on the FL-based BC across various time series of CMAPSS.

The root mean square errors (RMSE) for each dataset are 24.76, 32.25, 25.17, and 28.54. The BC-based FL has commendable predictive accuracy, as substantiated by previous research on RMSE [262, 60, 43]. The framework addresses the primary issues related to FL and demonstrates its RUL prediction capabilities.

The primary objective is to present a novel approach for integrating Blockchain (BC) with Federated Learning (FL) in the context of Remaining Useful Life (RUL) prediction, emphasizing the benefits of BC for data security and integrity. We aim to enhance the accuracy of Federated Learning in Remaining Useful Life prediction compared to previous research employing Deep Learning. The integration of federated learning into blockchain presents considerable obstacles, including huge computational and financial expenditures. For instance, uploading and retrieving weights from BC may require up to one minute, particularly when employing complex training models, which can potentially prolong the process to several weeks due to congestion. Moreover, each weight upload incurs financial expenses in the form of gas fees. Therefore, we use a more straightforward machine learning model, such as SVM, to capitalize on its benefits of simplicity, rapid training durations, and reduced weight size. This suffices in the academic realm to illustrate the notion. Consequently, juxtaposing BC-based RUL with those derived from more intricate models, as demonstrated in prior research [262, 60, 43], is not pertinent. In industrial contexts, it is imperative to investigate powerful, rapid, and efficient deep learning models that can be integrated with blockchain technology, utilizing platforms such as Oracle or private chains to improve computing precision and minimize financial expenditure.

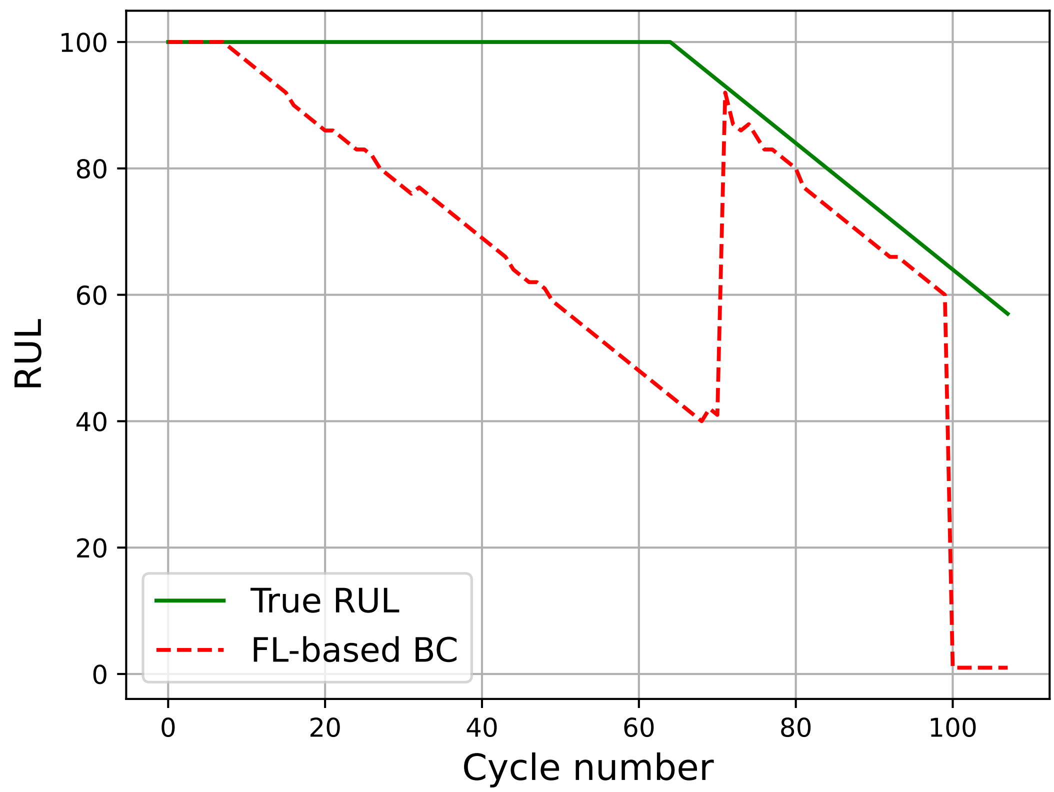


FIGURE 4.12: First iteration

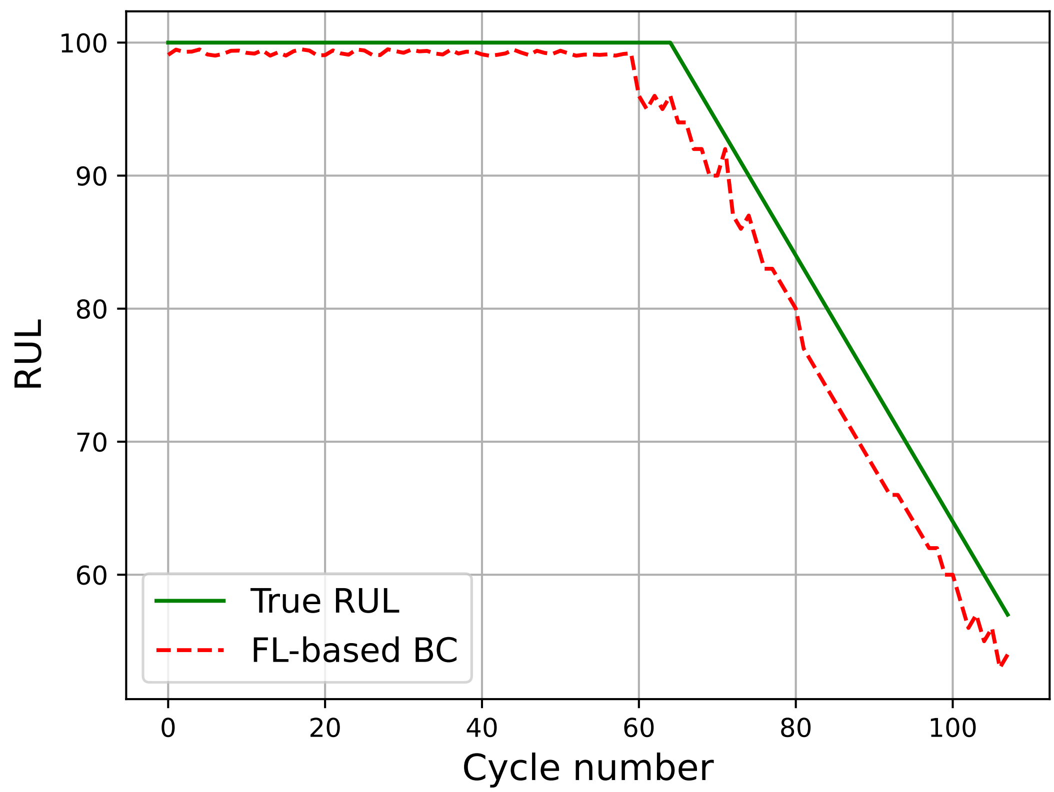


FIGURE 4.13: Final iteration

FIGURE 4.14: The performance of RUL prediction on the dataset during a first and final iteration of FL-based BC.

Utilizing the FD001 dataset as an illustration, Figure 4.14 depicts the initial performance of Remaining Useful Life (RUL) prediction on the dataset before the Federated Learning (FL)-based Bayesian Classification (BC). It subsequently showcases the improved RUL prediction accuracy after the contribution of model weights by workers to the FL process, utilizing the BC application. The outcome demonstrates a significant enhancement in Remaining Useful Life (RUL) forecast accuracy, as part-specific issues encountered in RUL prediction present a practical case, demonstrating how our Bayesian Classification-based Federated Learning framework provides a relevant solution. This section demonstrates the efficacy of our BC-based FL framework in tackling the critical issues identified for RUL prediction. We explore the specific issues encountered in Remaining Useful Life (RUL) prediction, present a practical case, and demonstrate how our Bayesian Classification-based Federated Learning framework provides a relevant solution, grounded in the functionalities of Bayesian Classification technology.

Trust and transparency

Establishing trust and openness is a crucial condition for collaborative model training. The complexities of this task have been comprehensively analyzed. Real-world problem statement: Envision a situation in which many aviation corporations seek to collaborate on a federated learning initiative to improve predictive maintenance for their assets. Every organization holds rich data that, when integrated, might substantially enhance the precision of prediction models for Remaining Useful Life assessment. Nonetheless, the subsequent issues may arise from the process:

- Insufficient Trust among Corporations: Owing to competitive apprehensions, these entities are hesitant to exchange their confidential data directly. There is a deficiency of confidence among corporations in the protection of their sensitive information. Concerns Regarding Transparency: The involved firms may be reluctant to completely reveal their internal model modifications or operational insights. Concerns about the disclosure of excessive information about their procedures, which may compromise or jeopardize their competitive advantage.

BC solution: The incorporation of blockchain into the federated learning architecture establishes a decentralized and highly secure environment, which is especially vital for remaining useful life predictions in airplanes. Smart contracts (SC) are essential in regulating data access and use, as well as safeguarding sensitive information. This secure method facilitates the collaborative essence of federated learning while protecting sensitive information. Moreover, the blockchain's transparent and immutable characteristics substantially bolster trust in the RUL prediction process. provides a verifiable record of model modifications and data inputs, while safeguarding proprietary information, as outlined in Subsection. 4.3. This transparency is illustrated in Figure 4.15, which demonstrates the longevity of recorded transactions within the blockchain. This continuous record enables firms to accurately monitor the data given and uploaded by each participating organization, promoting openness and accountability in the FL process, which is crucial for correct RUL predictions.

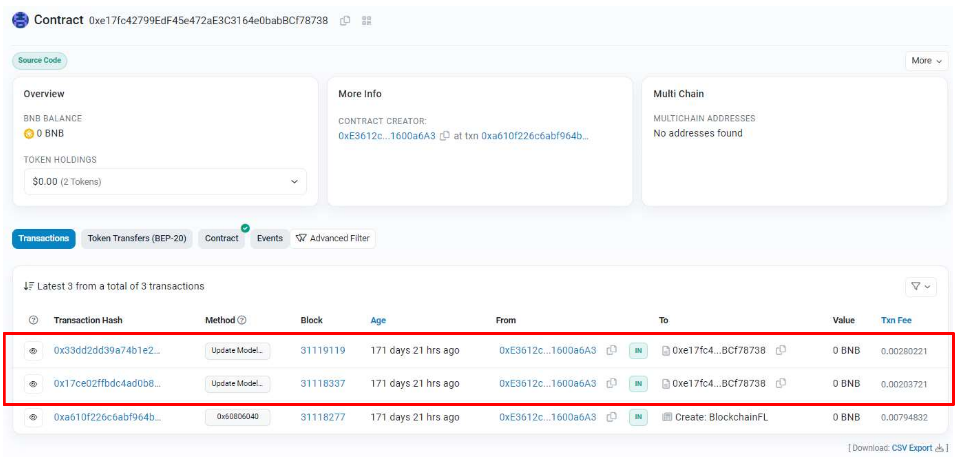


FIGURE 4.15: Transactions recorded permanently within the blockchain.

The red rectangle indicates that a corporation has recently uploaded data to the BC.

This highlights the practical challenges that arise when trust and transparency obstacles hinder effective collaboration among organizations within a federated learning network. Implementing a blockchain-based federated learning architecture may effectively promote trust and openness while safeguarding the security of sensitive data.

Data privacy and security

Safeguarding the privacy and security of sensitive information is essential. The combination of blockchain (BC) with federated learning (FL) presents a viable solution to address these pressing issues by leveraging the immutable and decentralized characteristics of blockchain. Real-world problem, a collaborative initiative with aviation firms from multiple nations focused on developing a federated learning model to predict an aircraft's remaining useful life. The aim is to utilize varied datasets to enhance the precision and generalizability of prediction models. However, the subsequent issues may arise from the process:

- Each aircraft manufacturer and operator maintains exclusive maintenance and performance history data. This data is governed by stringent privacy and confidentiality standards. The dissemination of aircraft-specific information across companies and international boundaries may provoke legal and ethical issues. This method may violate data protection regulations and industry confidentiality agreements, which is a considerable problem in the aviation business.

- Security of Sensitive Aircraft Information: The dissemination of sensitive aircraft data, especially when aggregated, presents security vulnerabilities. Aerospace firms are vigilant about potential data breaches during transmission, which could compromise the security of sensitive information and violate industry laws.

BC solution: The incorporation of BC employs sophisticated cryptographic methods, particularly utilizing the RSA algorithm, to substantially enhance security in the RUL prediction process. Aircraft data is encrypted utilizing RSA keys, a well-recognized cryptographic technique celebrated for its safe data transfer [80]. Access permissions are thoroughly recorded on the blockchain, enhancing data protection with an additional security layer. to substantially augment security in Florida. Patient data is encrypted with RSA keys, a formidable cryptographic technique recognized for its safe data transfer [80]. Access permissions are systematically documented on the BC, enhancing data protection with an extra layer of security. This decentralized security protocol, enhanced by the immutable characteristics of blockchain, directly tackles the ongoing issue of data privacy in federated learning. In the RSA approach, only the federated learning (FL) operator holds the decryption key, therefore guaranteeing the confidentiality and security of critical patient data during the FL process. Figure. Figure 4.16 illustrates the original key, both encrypted and decrypted by the RSA technique. As seen in the figure. The encrypted hash displays a unique string in contrast to the original, thus enhancing its confidentiality. Moreover, upon decryption with the private key, the hash link returns to its original state. Consequently, even if unauthorized individuals obtain the material, unable to decipherof deciphering it without access to the decentralized security strategy, along with the immutable characteristics of the blockchain (BC), which directly addresses the persistent issue of data privacy in RUL prediction via federated learning (FL). Through the use of the RSA technique, only the FL operator retains the decryption key, thus safeguarding the confidentiality and security of critical aircraft data during the FL procedure. Figur, combined with the immutable characteristics of the blockchain (BC), directly addresses the RSA method. The encrypted hash manifests as a unique string, distinct from the original, thereby enhancing its confidentiality and security. Unauthorized parties may access the data; however, they will be unable to decipher it without the requisite private key, thereby safeguarding data confidentiality and privacy in the RUL prediction process.

FIGURE 4.16: Original key encrypted and decrypted using RSA algorithm.

```
Original string: https://
    bafybeibbnrtxrzsanqfgifl4awixxvyr53te3jmlwdaxaeifncsnykhgxe.
    ipfs.nftstorage.link
Encrypted string:  b'\xa5\xb5/\xa77\xfb\xb1\xc5e\xaa\xe6\x7f\xb5
    \x90gj\xc8\xb4\xdd\x08+\xd9\xfb\x91\xbe\xc9\xad\xf5w\x90$uw\
    x91F!\x9f_\xae\xb8\x80\x826L\x992p\xe8\xeaJ\x1bxSYoo\xf9)\
    x1d\xe2\x1d"AM\xf4\xd1\xa1\xcc\xf9\x0el\x9b\xde\xdf\xb4ko\
    xfc\xa8\xdb\x12\x12\x8d \xfagc\xec\xe8\x00`H\xb3\x9b>\xda\
    x0b\xe8\xf5\xbd\xc2Z\x9cB\x914\xcb\x98p\xbej\x9f\x90>\x0cu\
    xc4Q\x07o\x8bo0\x94[\xf8e\xd6'
Decrypted string: https://
    bafybeibbnrtxrzsanqfgifl4awixxvyr53te3jmlwdaxaeifncsnykhgxe.
    ipfs.nftstorage.link
```

Incentives and rewards

Encouraging active involvement and rewarding contributions are essential for establishing a sustainable environment for RUL prediction using FL. This section examines how BC can be utilized to develop unique incentive mechanisms that motivate stakeholders to actively engage in the FL process.

Real world problem statement: Envision a federated learning process designed to optimize predictive maintenance for aircraft. Various aircraft operators and maintenance organizations provide data from multiple sources to improve the accuracy of remaining useful life predictions. However, this context introduces specific incentive and reward challenges:

Establishing Incentives for Data Contributors: Aircraft operators and maintenance organizations that allocate resources and share essential data may be reluctant to engage actively without explicit incentives or rewards. The lack of adequate motivation can result in organizations prioritizing their own interests over collaborative contributions, which could adversely affect the accuracy and effectiveness of Remaining Useful Life predictions. The difficulty is to establish an equitable mechanism for allocating incentives or benefits derived from enhanced RUL predictions. Stakeholders may be conceiving their own interests over collaborative contributions, which could adversely affect the accuracy and effectivenessBC solution:

The BC-based FL framework for predicting aircraft RUL incorporates transparent and automated smart contracts to manage incentive structures. These contracts can programmatically define and execute reward distributions based on each entity's contributions. The decentralized and immutable characteristics of blockchain ensure transparency and trust in the reward allocation process. However, implementation necessitates an automated verification service in the backend, supervised by a monitoring server (as detailed in Subsubsec. 4.3). This service assesses the impact of new model weights on global accuracy. If the updated weights are advantageous, events within the blockchain are triggered to allocate incentives to the respective worker, thereby fostering collaboration and accuracy in RUL predictions.

Figure 4.15 delineates the details of the incentive transaction for the worker after the upload of w_1 to the blockchain via smart contract. As illustrated in the figure's lower portion, upon uploading w_1 as the IPFS hash, the smart contract autonomously initiates the transfer of one BC token to the worker's address. Consequently, the worker is empowered to utilize this token as a coupon or a pertinent reward, as facilitated by the central company managing the federated learning process. This mechanism incentivizes active participation and enhances the precision of remaining useful life predictions.

Scalability and efficiency

In the rapidly evolving domain of federated learning, achieving scalability and operational efficiency presents a crucial challenge. The incorporation of blockchain presents a transformative framework that tackles these essential issues. By leveraging the intrinsic advantages of blockchain, federated learning can scale efficiently to manage diverse and dynamic datasets through optimized resource allocation and enhanced computational efficiency within blockchain infrastructure.

The joint effort among several aircraft operators and maintenance groups may lead to scalability and efficiency issues. Consider a federated learning initiative aimed at optimizing energy consumption within a decentralized smart grid system. Various energy providers and grid operators collaborate to enhance the efficiency of energy distribution and consumption patterns. However, the following challenges may arise from this process:

Scalability in predicting Remaining Useful Life (RUL) in aircraft presents challenges, especially with the involvement of various aircraft operators and maintenance organizations. As the number of participating entities increases, managing the scalability of the federated learning (FL) system becomes complex. Coordinating disparate datasets and computational resources becomes increasingly difficult, obstructing efficient model updates across a broad and heterogeneous corporate network. In the realm of aircraft predictive maintenance, attaining computational efficiency in the federated learning process is crucial for real-time decision-making. Suboptimal model training or communication protocols may lead to delays in addressing dynamic changes in aircraft maintenance requirements and operational demands.

BC solution: Leveraging the intrinsic advantages of blockchain, federated learning can scale efficiently to manage diverse and dynamic datasets through optimized resource allocation and enhanced updates, facilitating efficient collaboration among numerous participants. The blockchain's decentralized structure aids in distributlead to scalability and efficiency issuesng overall efficiency.

This section clarifies that the framework is currently in its conceptual stage and has not been empirically validated. Consequently, the results of its implementation are not presented here. We encourage the research community and industry experts to offer constructive feedback on this proposed infrastructin predictingtiative seeks to enhance the integration of BC and FL, thereby promoting more accessible and impactful applications, especially within the aircraft industry.

The four challenges outlined illustrate the proposed blockchain-enabled federated learning infrastructure, which signifies a promising advancement in collaborative federated learning. As it becomes increasingly difficult, which obstructs the advantages of blockchain and federated learning, we foresee a transformative effect on industries, helping distribute and scalable solutions.

4.4 Conclusion

This chapter introduces a novel methodology for transforming multivariate CoDa into real vectors using the Dirichlet density transformation, effectively eliminating constraints and reducing dimensionality. It also presents two monitoring and Anomaly detection approaches that integrate SVDD control charts and MEWMA techniques with Dirichlet density and ilr transformations, with the S_{ilr} control chart demonstrating superior performance in most scenarios. Additionally, the chapter explores an innovative framework that combines federated learning (FL) with blockchain (BC) for predictive maintenance, particularly in predicting remaining useful life (RUL). This approach enhances data security, trust, and efficiency, with applications in aerospace and Industry 5.0. Key contributions include integrating BC into FL for RUL prediction, open-source software availability, and demonstrating the framework's effectiveness using the CMAPSS dataset.

In addition to the studies provided, we have conducted research on machine learning methodologies and AI-driven monitoring strategies to optimize predictive maintenance, enhance reliability, and ensure safety in industrial systems. The research conducted by Saghir et al. (2023) presents a hybrid model that integrates an Autoencoder with Transformer and utilizes Explainable AI (XAI) to enhance anomaly detection in IoT systems, hence tackling security concernanticipate a transformative impact on industries seekingguyen et al. (2024) investigate the integration of physics-based models with machine learning, focusing on Physics-Informed Neural Networks (PINNs) to enhance the reliability and safety of industrial systems, thus improving the precision in forecasting system states and executing predictive maintenance [146]. Nguyen et al. (2024) present a solution that integrates Edge AI with Federated Learning to enhance performance and security, while maximizing predictive maintenance for intelligent systems, minimizing latency, and ensuring real-time responses in smart factories. [151]. This research significantly advances the development of intelligent and safe industpredicting remaining useful life (RUL)es progressively use automation and artificial intelligence. Furthermore, the study conducted by Vu et al. (2024) on enhancing predictive maintenance through Genetic Algorithms (GA) in Future Industrial Systems (FIS) illustrates the effectiveness of GA in optimizing maintenance within dynamic aIn addition to the studies provided, we have conducted research on machine learning methodologies and AI-driven monitoring strategies to optimize predictive maintenance, enhance reliability, and ensurepredictability and system reconfiguration in contemporary industrial settings. Future directions focus on optimizing transformation models, leveraging advanced AI techniques for anomaly detection, and incorporating explainable AI (XAI) to enhance transparency and trust in decentralized industrial environments.

Chapter 5

Adaptive Anomaly Detection, Classification, and Explanations with Federated Learning for Smart Healthcare Applications

The content of this chapter is based on the following publications, in which I am a co-author:

- A. Raza, S. Li, K.P. Tran, L. Köehl, K.D. Tran* (2024). "Using Anomaly Detection to Detect Poisoning Attacks in Federated Learning Applications" *Engineering Applications of Artificial Intelligence*. Elsevier. Submitted.
- A. Raza, K.P. Tran, L. Köehl, X. Zeng, K. Benzaidi, S. Li, S. Hotham, K.D. Tran*(2024). "Lightweight Transformer in Federated Setting for Human Activity Recognition in Home Care" *Pattern Recognition*. Elsevier. Under Review.
- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System" Book: *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

- T. Nguyen, Q.T. Nguyen, K.D. Tran*, L. Köehl, K.P. Tran, (2024), "Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, G. Tartare, K.P. Tran (2024), "Explainable Transformer-based Approach for ECG Anomaly Detection," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam* .

- T. Banfalvi, D.H. Nguyen, K.D. Tran, G. Tartare, P. Bruniaux, L.H. Le, X. Zeng, K.P. Tran (2024), "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T. Banfalvi, K.D. Tran, G. Tartare, P. Bruniaux, K.P. Tran (2024), "Unsupervised classification of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings: A survey and perspective," in *International Conference on Responsible Artificial Intelligence and Data Science, DaNang, Vietnam*.

- T.T.V. Nguyen, C. Heuchenne, K.D. Tran, K.P. Tran (2024). "A Novel Transformer-Based Anomaly Detection Approach for ECG Monitoring Healthcare System" Proceedings of the *International Conference on Safety and Security in IoT*, Springer Nature Switzerland Publishing, pp. 111-129. http://dx.doi.org/10.1007/978-3-031-53028-9_7

5.1 Introduction

Diabetes has become a major global public health issue, with its prevalence projected to increase by 59.7% from 2021 to 2050, affecting over 1.31 billion people worldwide [206]. This growing epidemic underscores the urgent need for advanced medical data processing techniques, particularly machine learning models, to enable more accurate and efficient diagnoses. Similarly, Human Activity Recognition (HAR) has gained prominence in healthcare applications such as disease prevention, rehabilitation, and health monitoring [238]. As mobile computing, smart sensing, and IoT technologies advance, the volume of health-related data has surged, necessitating the application of sophisticated machine learning algorithms for effective processing. Recent breakthroughs in deep learning, including convolutional neural networks

(CNNs) and recurrent neural networks (RNNs), have significantly enhanced the accuracy of HAR classifiers [1]. However, challenges such as privacy concerns, large dataset requirements, and data communication overhead persist. Federated learning presents a promising solution by allowing collaborative model training across decentralized data sources while safeguarding privacy [121]. Despite these advancements, challenges such as adversarial attacks and the integration of complex models like transformers into HAR systems remain, warranting further research into robust defense strategies and efficient data-handling methodologies [200].

In the medical domain, compression therapy plays a vital role in managing conditions like Chronic Venous Insufficiency (CVI) and Lymphoedema [42]. However, determining the optimal compression level for individual patients remains a complex challenge due to the wide variations in leg shapes and sizes [130]. Recent advancements in 3D scanning and deep learning techniques have opened new avenues for representing and analyzing human leg morphology [241]. Point cloud data, a 3D representation of the human body, offers a promising solution for this purpose. By utilizing deep learning models to process point cloud data, researchers aim to develop accurate shape descriptors and adaptive models for medical compression stockings (MCSs) that can be customized to individual leg shapes, improving therapeutic outcomes and overcoming the limitations of traditional sizing approaches [50].

Next, Human Activity Recognition (HAR) is a critical machine learning task with significant applications in healthcare, particularly in home-based care for patients and older adults [249]. By leveraging data from smart sensors embedded in Internet of Things (IoT) devices such as smartphones, wearables, and other body-worn sensors, HAR systems enable continuous health monitoring, disease prevention, and rehabilitation support. The advancement of deep learning techniques—such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs)—has enhanced HAR performance in both centralized and federated learning settings [161]. However, these methods come with notable challenges: RNNs suffer from limited parallelizability, CNNs are constrained by fixed sequence lengths, and both require high computational resources. Additionally, the centralized approach raises significant privacy concerns, as HAR classifiers rely on highly sensitive personal data collected within home environments [52].

To address these limitations, we propose a novel lightweight (one-patch) transformer architecture that combines the strengths of RNNs and CNNs while mitigating their drawbacks [259]. Furthermore, we introduce TransFed, a privacy-preserving, federated learning-based HAR classifier that leverages this transformer architecture [266]. Our approach strikes a balance between model efficiency, privacy, and classification accuracy. We constructed a new HAR dataset by collecting activity data from five human participants using a custom-built testbed and evaluated our classifier in both federated and centralized learning settings [118]. Additionally, we assessed the classifier's performance on a publicly available dataset to benchmark it against existing HAR classifiers. Experimental results demonstrate that our approach achieves superior accuracy and efficiency compared to traditional models.

Beyond performance optimization, federated learning-based HAR systems are vulnerable to adversarial threats, particularly data poisoning attacks [19]. In traditional machine learning, poisoning attacks manipulate training data to degrade model performance. In federated learning, these attacks extend to model poisoning, where adversaries introduce malicious updates that evade conventional detection techniques due to their limited access to local training data. Existing poisoning attack detection methods in FL suffer from limitations such as reliance on assumptions about the number of attackers, dependence on independent and identically distributed (i.i.d.) data, and excessive computational complexity.

To counter these threats, we propose a novel framework for detecting poisoning attacks in federated learning, which leverages a reference model trained on a public dataset alongside an auditor model for identifying malicious updates [40]. Our framework employs a one-class support vector machine (OC-SVM) for efficient attack detection, achieving a computational complexity of O(K), where K is the number of clients. We evaluated our detector against state-of-the-art (SOTA) poisoning attacks in two key FL applications: electrocardiograph (ECG) classification and HAR [57]. Our results demonstrate the superiority of our detection framework over existing methods, reinforcing its applicability in safeguarding federated learning-based HAR systems [168].

- Objective 3.1: Design adaptive anomaly detection frameworks leveraging federated learning to enable privacy-preserving analysis across distributed healthcare data sources.

- Objective 3.2: Integrate explainable AI techniques into the anomaly detection models to enhance transparency and interpretability in decision-making, supporting better patient monitoring and improved clinical outcomes.

- Objective 3.3: Assess the impact of AI-driven methods on healthcare by testing the models on relevant datasets and evaluating improvements in early diagnosis and patient management.

5.2 Contributions about Diabetes Classification with ML

Diabetes is a substantial global public health concern, exerting considerable strain on healthcare systems and socio-economic advancement. The anticipated effect is predicted to escalate, with prevalence forecast to climb by 59.7% from 2021 to 2050, affecting more than 1.31 billion individuals [56]. There is an increasing focus on the processing of medical data and the assessment of machine learning models to fully use artificial intelligence in diabetes diagnosis [47]. The FT-Transformer demonstrated commendable classification efficacy, achieving an accuracy of 98.07%, precision of 95.76%, and recall of 98.26%, compared to models such as Random Forest, XGBoost, and LGBM [206]. While it is somewhat behind these models, it has potential for future applications in more intricate database systems [38]. The data processing methodology, including KNN imputation, ICA, and Isolation Forest, efficiently streamlines and enhances the model [46]. These findings represent a substantial advancement in data processing optimization and provide future researchers with valuable insights for discovering ideal models for application, especially in medical databases related to diabetes diagnosis [206].

5.2.1 Proposed methodology

The study methodology was conducted sequentially as outlined in Figure 5.1. This study processed the data using three powerful techniques: KNN imputation to address missing values in the data, ICA to optimize the data for easier anomaly detection, and Isolation Forest to remove those anomalies from the dataset. After preprocessing, the data were split into two sets: training (80%) and testing (20%) for model training and analysis, comparing the FT-Transformer model with five other models. After fine-tuning and achieving good results, the models were evaluated on the test dataset to compare their performance. Additionally, the study utilized SHAP values to evaluate the impact of features on the classification process in the FT-Transformer model.

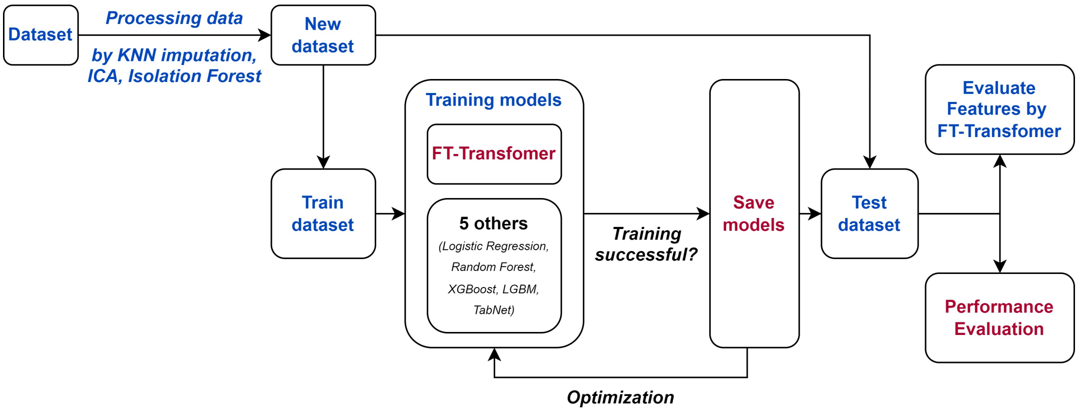


FIGURE 5.1: Research flowchart

To investigate the performance of the proposed method, we use a diabetes dataset amassed from a cohort of 2000 individuals at the Frankfurt Hospital situated in Germany [1] [180]. The dataset encompasses eight distinct attributes. From the total of 2000 samples, 684 individuals are classified as diabetes patients, while the remaining participants exhibit normal glucose metabolism. The dataset comprises eight features, namely: Pregnancy, Glucose, Blood Pressure, Skin Thickness, Insulin, BMI, Diabetes Pedigree Function, and Age (Table 5.1).

[1]https://ieee-dataport.org/documents/type-2-diabetes-dataset

TABLE 5.1: The attributes of the Frankfurt dataset

Attribute	Description	Type	Mean ± SD
Pregnancies	Number of Times Pregnant	Categorial	3.7 ± 3.3
Glucose	Plasma glucose concentration 2h in an oral glucose tolerance test.	Numeric	121.18 ± 32.07
Blood pressure	Diastolic blood pressure (mm Hg).	Numeric	69.14 ± 19.18
Skin Thickness	Triceps Skinfold Thickness (mm).	Numeric	20.93 ±16.1
Insulin	2-hour serum insulin (μ IU/mL).	Numeric	80.25 ± 111.18
BMI	Body mass index (kg/m^2).	Numeric	32.19 ±8.15
DPF	Diabetes pedigree function.	Numeric	0.47 ± 0.32
Age	Age (years).	Numeric	33.09 ± 11.79
Outcome	Diabetes diagnose results (tested_positive: 1, tested_negative: 0)	Nominal	–

The Frankfurt dataset has a considerable volume of missing data across five attributes, particularly Glucose, Blood Pressure, Skin Thickness, Insulin, and BMI (Table 5.2). There is a total of 1,660 missing values. The study processed missing data using the KNN imputation.
Thereby, the data addressed outliers using the Isolation Forest method combined with ICA. The results showed that 190 subjects were excluded, leaving a final dataset of 1,810 subjects (Figure 5.2). This dataset was then split proportionally to train and evaluate the models. The training dataset included 1448 (80%) samples, and the testing dataset had 362 (20%) samples.

TABLE 5.2: Missing values in the Frankfurt dataset

Attributes	No. of missing values
Glucose	13
Blood Pressure	90
Skin Thickness	573
Insulin	956
BMI	28
Total	1660

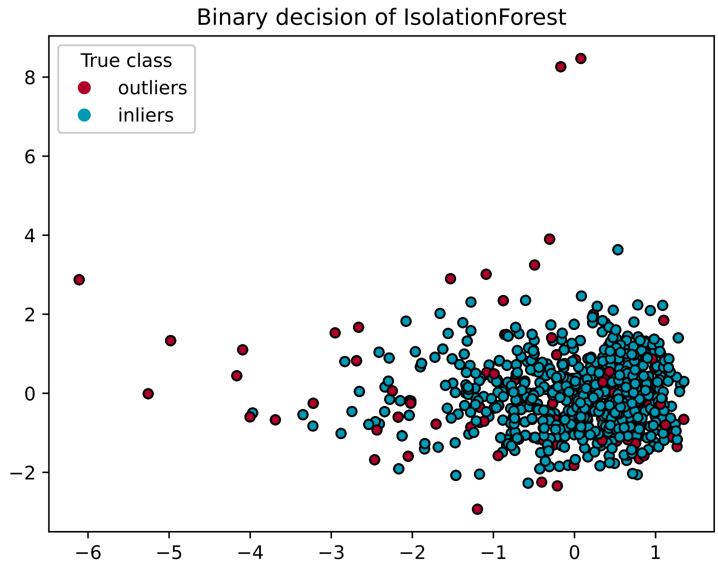


FIGURE 5.2: Decision to exclude outliers of Isolation Forest

Table 5.3 discusses the best learning rate for training under the same settings using the FT-Transformer on this dataset. The results indicated that, with a consistent setup of 1,000 epochs and a batch size of 128, a learning rate of 0.001 yielded the best performance, achieving an accuracy of 0.9834 along with the lowest loss (0.0001).

TABLE 5.3: Impact of learning rate by accuracy measurement of FT-Transformer with 1000 epochs and batch size = 128

Learning rate	Loss	Accuracy
0.001	0.0001	0.9834
0.0001	0.0008	0.9834
0.00001	0.0970	0.8809

Outlines the training process of the FT-Transformer model, which was trained on a dataset derived from the Frankfurt dataset with a learning rate of 0.001.

To reduce overfitting, the model was halted at the 99th epoch using a validation method based on the performances of AUC and Root Mean Square Error (RMSE). The final AUC and RMSE stopped at 0.9951 and 0.1350, respectively. The classification performance of the FT-Transformer model after training is evaluated using a confusion matrix in Figure 5.3. The classification results are great, with a total misclassification rate of approximately 1.93% (7 out of 362 instances). The correct classification rates for each class are 98.26% (113/115) for Diabetes and 97.98% (242/247) for No Diabetes.

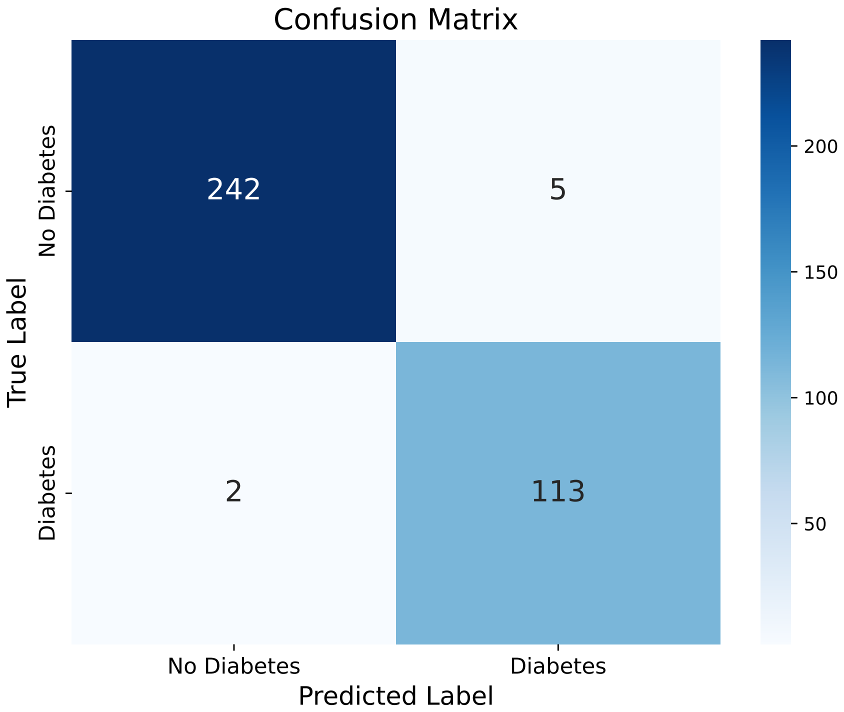


FIGURE 5.3: Confusion matrix of FT-Transformer model in test dataset

Figure 5.4 represents the impact of features on the binary classification capability of the FT-Transformer model using SHAP values. Glucose and diabetes pedigree function were the two most influential features in classification, while pregnancies, blood pressure, and BMI showed the least influence.

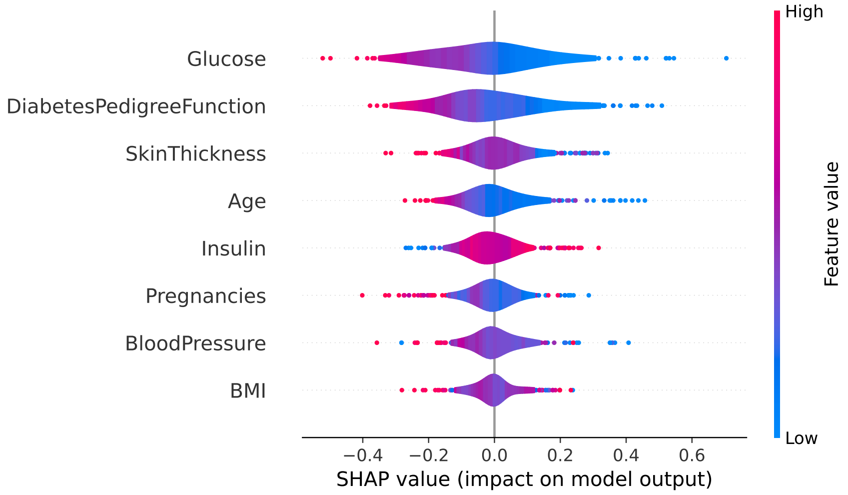


FIGURE 5.4: SHAP summary plot for the FT-Transformer model

5.2.2 Model Performances

Table 5.4 introduces the binary classification performances of 6 models in the test dataset. The Random Forest model achieved the best classification performance with an accuracy of 0.9945 and an F1-score of 0.9914. It was followed by LGBM, XGBoost, and FT-Transformer, all with accuracies above 0.98. TabNet also performed relatively well, with an accuracy of 0.9751. In contrast, Logistic Regression had poor classification performance, with an accuracy of only 0.7818 and a very low F1-score of 0.6070.

TABLE 5.4: Performance measure of all classification algorithms

Model	Accuracy	Precision	Recall	F1-score
Logistic Regression	0.7818	0.7093	0.5304	0.6070
Random Forest	0.9945	0.9829	1.0000	0.9914
XGBoost	0.9834	0.9658	0.9826	0.9741
TabNet	0.9751	0.9417	0.9826	0.9617
LGBM	0.9890	0.9826	0.9826	0.9826
FT-Transformer	0.9807	0.9576	0.9826	0.9700

The figure 5.5 shows the AUC performances by 6 classification models in the test dataset. All models demonstrated very good classification results as measured by AUC, with scores above 0.98 (except for Logistic Regression). The Random Forest model continued to yield the best performance with an AUC of 0.9999. The FT-Transformer model also performed relatively well, achieving an AUC of 0.9812.

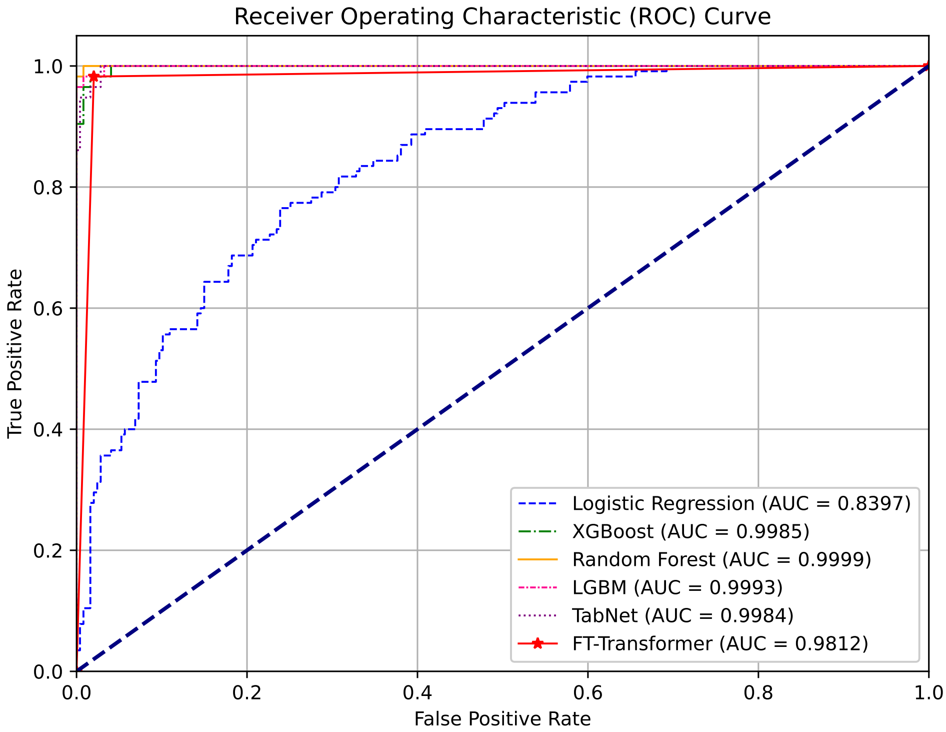


FIGURE 5.5: AUC classification models

This study applied KNN imputation, ICA, and Isolation Forest to preprocess the dataset, evaluated the performance of the FT-Transformer model in diabetes classification compared to other models, and analyzed the influence of features on the FT-Transformer's decision-making in diagnosis.
The evaluation results showed that while the FT-Transformer achieved relatively good performance, it did not surpass the three models: LGBM, XGBoost, and Random Forest [56, 13, 38]. These three models remained the best classifiers, consistent with previous studies, despite the dataset being processed differently. This suggests that even with varying preprocessing techniques, these three models consistently excel in classification tasks for tabular data.
This data preprocessing approach once again underscores the crucial role of data handling in improving model predictive performance [47, 46]. The classification results are very promising, demonstrating that this approach will help eliminate redundant data from the dataset, thus saving resources during model training. Notably, executing tasks sequentially and automatically, rather than manually, significantly reduces the time required for data processing. It also demonstrates that addressing outliers enhances model accuracy more effectively than knowledge-based processing methods [206].
Besides, Glucose remains the most decisive feature influencing diabetes diagnosis.

The findings suggest that the Transformer model may not be the optimal approach for tabular data [219]. This can be attributed to the heterogeneous nature of tabular data in the medical field, which often includes a mix of continuous, categorical, and ordinal features. Additionally, Transformer models are primarily designed for text and image data, where tokens (such as characters and pixels) are arranged in meaningful semantic and correlated structures. This highlights the need for future improvements to Transformer models to optimize their performance on such datasets, ensuring they can compete with simpler yet highly effective models, such as XGBoost [190].
Although the FT-Transformer incurs higher computational costs, these results suggest that in practical applications, such as in medical clinical decision support systems, large datasets from electronic medical records, and more complex systems, it remains a superior choice. This is particularly true for large-scale systems requiring more flexible models. Overall, the Transformer-based architecture shows promising potential advantages in the healthcare domain. This transformer model is also promising for implementing a Federated setting framework, which protects data privacy and security for the system [118], increases collaboration in training AI models [200], and reduces training cost [266].
In the context of advancing electronic diagnostic systems and smart healthcare, this study provides compelling evidence for selecting appropriate models to integrate into such systems. This application could assist physicians in remotely monitoring and managing patients, particularly in controlling the progression of diabetes in postpartum women. This study has highlighted the power of combining data processing techniques (KNN imputation, ICA, and Isolation Forest) to enhance model performance and evaluate the FT-Transformer model's classification performance on tabular data. Additionally, the application of SHAP values revealed the key factors that critically influence classification and diagnosis decisions.

5.3 Contributions about Efficient Lightweight Transformer Architecture for Federated Human Activity Recognition for Smart Healthcare

Human Activity Recognition (HAR) is a classification task that aims to identify specific human activities (e.g., sitting, walking, running) within a given timeframe, typically using supervised machine learning methods. Advances in mobile computing, smart sensing, and IoT have generated extensive health-related data useful for HAR classifiers [1]. The recent integration of graph neural networks and recurrent neural networks has improved HAR accuracy by effectively capturing spatiotemporal dependencies [172]. However, the increasing use in critical areas, such as autonomous vehicles and healthcare, raises concerns about the vulnerability of HAR systems, especially skeleton-based methods, which are susceptible to adversarial attacks [54]. Approaches such as spatiotemporal Hard Attention with Deep Reinforcement Learning (STH-DRL) offer enhanced accuracy but highlight the critical need for robust defenses against adversarial threats [156]. HAR supports numerous healthcare applications, including disease prevention, rehabilitation monitoring, fall detection, and real-time health feedback, promoting effective health management [238]. It also underpins safety features like the iOS "Do not disturb while driving" function [10]. Integrating deep learning models like Deep Capsule Networks (DCapsNet) further enhances HAR performance by leveraging advanced feature extraction from convolutional layers and capsule networks [188]. Deep learning significantly improved HAR accuracy [161, 61]. Hybrid CNN-RNN models, such as those by Yao et al. [249], have achieved notable results but face challenges related to data requirements, communication overhead, and privacy concerns [249, 52, 39]. Federated learning addresses these by collaboratively training global models without sharing local data, thus preserving privacy and reducing communication overhead [121, 246, 126, 22, 196].

Despite their strengths, CNNs and RNNs have limitations: CNNs excel in parallelization, but RNNs struggle with long-term dependencies [44]. Transformers, initially developed for sequence modeling without recurrent structures [219], have shown promise in fields like NLP and healthcare [236, 248]. Although hybrid CNN-transformer models exist [259], they retain CNN limitations. Thus, the integration of transformers specifically tailored for HAR, particularly within federated learning contexts, remains largely unexplored. We proposed a novel lightweight (in terms of the number of trainable parameters required) transformer for HAR classification. We demonstrate that the proposed transformer outperforms other state-of-the-art HAR classification methods based on CNNs and RNNs when trained and tested on both a public dataset and a dataset we constructed. Given the challenges of privacy and computation cost, we introduce TransFed, the first framework for HAR classification based on federated learning and transformers. We designed a prototype to collect human activity data using three different types of body sensors: an accelerometer, a gyroscope, and a magnetometer. We also tested different sensor types on the human body to identify the points of maximum impulse (PMIs). We evaluated the performance of the data for each location. We then constructed a new dataset for evaluating HAR classifiers, which will be released publicly as a new research dataset. We evaluated the performance of TransFed using non-identically independent distributed (non-IID) data. Based on the data distribution, we analyze how non-iid data from clients can affect TransFed's performance.

5.3.1 Proposed Methods

Figure 5.7 shows the basic flowchart of the proposed transfer. In our method, the federated setting is adopted to facilitate collaborative learning while preserving the privacy of the underlying data. In the federated setting, a central (global) server sends the compiled architecture of the model (which is a transformer in our case) to all edge or client[2] devices. Each device trains its transformer locally using its local data. After all the local transformers are trained, each edge device sends the trained parameters of its transformer to the global server, which then aggregates these parameters to construct the global model without a training process. After the global model is available, each edge device downloads the aggregated parameters of the global model and updates its local model according to its local needs. There are two expected key advantages of the federated setting: (i) it increases the overall accuracy and the generalization of the model, and (ii) it provides better privacy protection to the data owners. Algorithm 5.1 defines the workflow of the proposed TransFed framework.

[2]In this paper, we use the terms 'edge' and 'client' interchangeably.

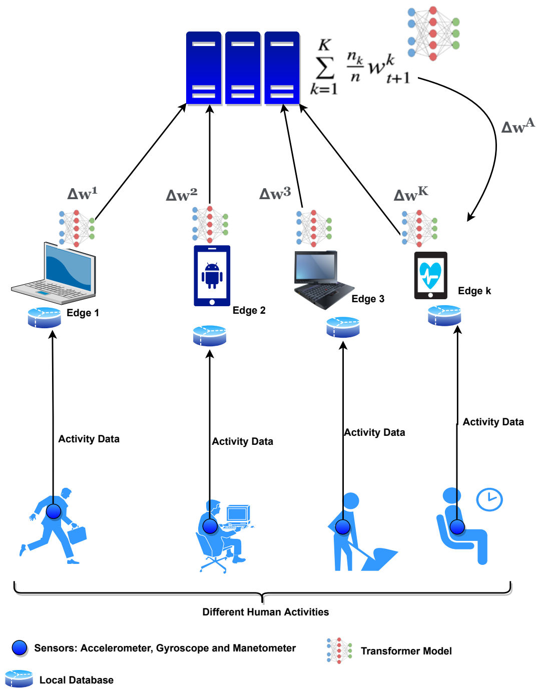


FIGURE 5.6: An illustrative diagram of the proposed framework.

5.3.2 Comparison with State-of-the-Art Methods

In this subsection, we compare the proposed transformer with existing state-of-the-art methods. Table 5.5 compares two key features of our proposed transformers with methods based on RNNs and CNNs. RNN-based models do not allow for parallelization during training due to their sequential nature, which makes the model computationally slow and expensive. CNN-based methods can perform parallel computation, but they are computationally expensive because the input and output representations on the proposed transformer eliminate recurrence and convolution, replacing them with a self-attention mechanism to establish dependencies between the input and output. It is the first type of architecture to rely entirely on attention to calculate input and output representations. In addition, transformers leave more room for parallelization. RNNs and CNNs utilize many parameters (typically hundreds of thousands or even more), whereas the proposed transformer employs only 14,697 parameters, making it more suitable for mobile computing devices. Moreover, unlike traditional transformers, the proposed transformer uses a single patch instead of multiple patches. Therefore, the proposed transformer is also much more computationally efficient.

We also compared the performance of the TransFed global model and

TABLE 5.5: Comparison of our transformer-based approach with those based on RNNs and CNNs, regarding computation costs.

Method	Parallelization	Computationally Expensive
RNNs	No	Yes
CNNs	Yes	Yes
Transformers	Yes	No

the centralized classifier based on the proposed transform with that of selected state-of-the-art HAR methods in the literature [196, 90, 144], including five methods that operate in a centralized setting and one in a federated setting. These three state-of-the-art methods were chosen because their performance results were reported using the WISDM dataset, which allows a direct comparison of the performance results. Table 5.6 shows the comparison results with the six selected state-of-the-art methods. Our proposed methods achieved a substantial improvement in terms of accuracy when trained and tested using our new dataset and the WISDM dataset. Specifically, our method achieved an accuracy of 98.74% and 99.14% in the federated and centralized settings, respectively, using our collected dataset. Furthermore, using the WISDM dataset in the centralized setting, it achieved an overall accuracy of 98.89%. Hence, from Table 5.6 it can be seen that the proposed transformer outperforms existing state-of-the-art methods, in both centralized and federated settings.

TABLE 5.6: Comparison with selected state-of-the-art methods for HAR classification.

Scheme	Centralized or Federated	Number of Activities	Accuracy
[196][a]	Federated	6	89.00%
[90][a]	Centralized	6	97.63%
[144][a]	Centralized	6	96.70%
Proposed[a]	Centralized	6	98.89%
Proposed[b]	Federated	15	98.74%
Proposed[b]	Centralized	15	99.14%

[a] Using the WISDM dataset.
[b] Using our new dataset.

5.4 Contributions about Detection of poisoning attacks with anomaly detection in federated learning for healthcare applications: A machine learning approach

Adversarial attacks, such as poisoning attacks, have garnered the attention of many machine learning researchers. Traditionally, poisoning attacks attempt to inject adversarial training data to manipulate the trained model. In federated learning (FL), data poisoning attacks can be generalized to model poisoning attacks, which cannot be detected by simpler methods due to the detector's lack of access to local training data. State-of-the-art poisoning attack detection methods for FL have various weaknesses, including the requirement for the number of attackers to be known or not sufficiently high, reliance on i.i.d. data only, and high computational complexity. To overcome the above weaknesses, we propose a novel framework for detecting poisoning attacks in FL, which employs a reference model based on a public dataset and an auditor model to detect malicious updates. We implemented a detector based on the proposed framework, utilizing a one-class support vector machine (OC-SVM), which achieves the lowest possible computational complexity of O(K), where K is the number of clients.

5.4.1 Proposed Framework

Attacker's goal: Similar to many other studies [19, 40, 189], we consider an attacker whose goal is to manipulate the global model in such a way that it has low performance (i.e., high error rates) and/or misbehaves in a particular way. Such attacks make the global model underperform. For example, an attacker can attack competitor FL systems. We consider both targeted and untargeted [197] attacks, as discussed previously.

Assumptions: We consider the following assumptions about the threat model:

1. There are one or more malicious edge devices that try to launch a model poisoning attack against the global model, possibly in a collaborative manner (i.e., launching a colluding attack).

2. All the attackers follow the FL algorithm, i.e., they train their local model using their local data and share the parameters with the global model.

3. All the attackers have two strategies: manipulating their local training data and training the local model using the manipulated data, and manipulating the model parameters after training it on benign data.

4. All the attackers have the full knowledge about the aggregation rules, the global model architecture, the auditor model (see Section **??** for more details about the auditor model proposed in our method), and the detection results, i.e., the whole detection framework is a white box and can be used as an oracle to adapt the attackers' strategy.

5. The global server can trust a third party or an isolated component, which maintains a public dataset that has data representing all classes of the underlying application for training the auditor model, and the attackers cannot poison this public dataset or the auditor model.

An overview of the proposed method is shown in Figure 5.7. Let us assume K edged devices (hospitals, organizations, etc.) collaborate to train a joint global model **GM**. An edge $\mathbf{E}_k$ trains a local model $\mathbf{LM}_k$ using its local data $\mathbf{D}_k$, where $k = 1, 2, \ldots, K$. The global server **GS** is responsible for receiving the updates from edge devices and aggregation. We assume that a trusted third party or **GS** (we consider a trusted third party to be a different entity from **GS**) also has an open-source dataset, which is referred to as public data, and we represent it as **DP**. **DP** is intended to be a representative dataset of all classes in a classification problem, i.e., it contains samples from each candidate class. The training for a global round is given as follows.

1. Trusted third party creates an audit model **AM** and a reference model **RM**. Where **RM** has the same architecture as the global model **GM**.

2. Trusted third party splits **DP** into train $\mathbf{DP}_{\text{train}}$ and test $\mathbf{DP}_{\text{test}}$ datasets and trains the **RM** using $\mathbf{DP}_{\text{train}}$.

3. After training, trusted third party makes predictions with **RM** using $\mathbf{DP}_{\text{train}}$ and $\mathbf{DP}_{\text{test}}$. During the predictions for each dataset, a trusted third party taps the activations of the last hidden layer for each input sample using Algorithm 5.1 to create a dataset $\mathbf{DA}_{\text{train}}$, and $\mathbf{DA}_{\text{test}}$ for each $\mathbf{DP}_{\text{train}}$ and $\mathbf{DP}_{\text{test}}$, respectively.

4. Trusted third-party trains the audit model (a one-class classifier) using $\mathbf{DA}_{\text{train}}$. Here, we treat all the samples of $\mathbf{DA}_{\text{train}}$ as a single class.

Trusted third party sends the trained **AM**, **RM**, $\mathbf{DP}_{\text{test}}$ and a value P to **GS**. We define P later in the section.

5. Each $\mathbf{E}_i$ trains $\mathbf{LM}_i$ using $\mathbf{D}_i$.

6. Each $\mathbf{E}_i$ sends updates W_i of trained $\mathbf{LM}_i$ to **GS**.

7. **GS** sets W_i as the parameters of **RM** and makes predictions using $\mathbf{DP}_{\text{test}}$. During the predictions, **GS** taps the activations of **RM** for each input sample using Algorithm 5.1 to create a dataset $\mathbf{DA}_i$.

8. **GS** makes predictions using **AM** and $\mathbf{DA}_i$ as input data. For every input sample $X \in \mathbf{DA}_i$, **AM** outputs $y_i \in \{1, -1\}$ and creates a set $Y = \{y_1, y_2, \ldots, y_z\}$, where z is the total number of samples in $\mathbf{DA}_i$.

9. **GS** computes poisoned rate $h_i = \frac{o \times 100}{z}$, where o is the total number of $-1's$ in Y.

10. **GS** includes W_i in global aggregation if $h_i \leq P$, otherwise discards W_i. Here, $P = h_{\text{test}} + \alpha\sigma$, and it is the percentage of poison that we want to tolerate. σ is called deviation tolerance and it is given as $\sigma = |h_{\text{test}} - h_{\text{train}}|$. h_{test} and h_{train} are calculated using $\mathbf{DP}_{\text{train}}$ and $\mathbf{DP}_{\text{test}}$, respectively. α is a parameter to make the threshold flexible. In our experiments, we set $\alpha = 1$.

Algorithm 5.1: Creation of Audit Dataset(s) $\mathbf{DA}_i$

Input: A dataset $\mathbf{D}_i$ and a trained model **M**
Output: a new dataset $\mathbf{DA}_i$

for $X \in \boldsymbol{D}_i$ **do**
  Transform X into batch size
  Make Prediction using X as a test sample in **M**
  Get activation maps $A^k_{l,w}$ of the last convolutional layer. where k is the number of activation maps with length l and width w each.
  Get probability score y^c, where c is the class label of X.
  Reshape A^k as an array of $1 \times j$, where $j = l \times w \times k$.
  Reshape X as an array of $1 \times l$, where l is the product of the height and width of X
  Compute $s = X \parallel A^k \parallel y^c$
  Append s in $\mathbf{DA}_i$ as a new data sample
Output $\mathbf{DA}_i$

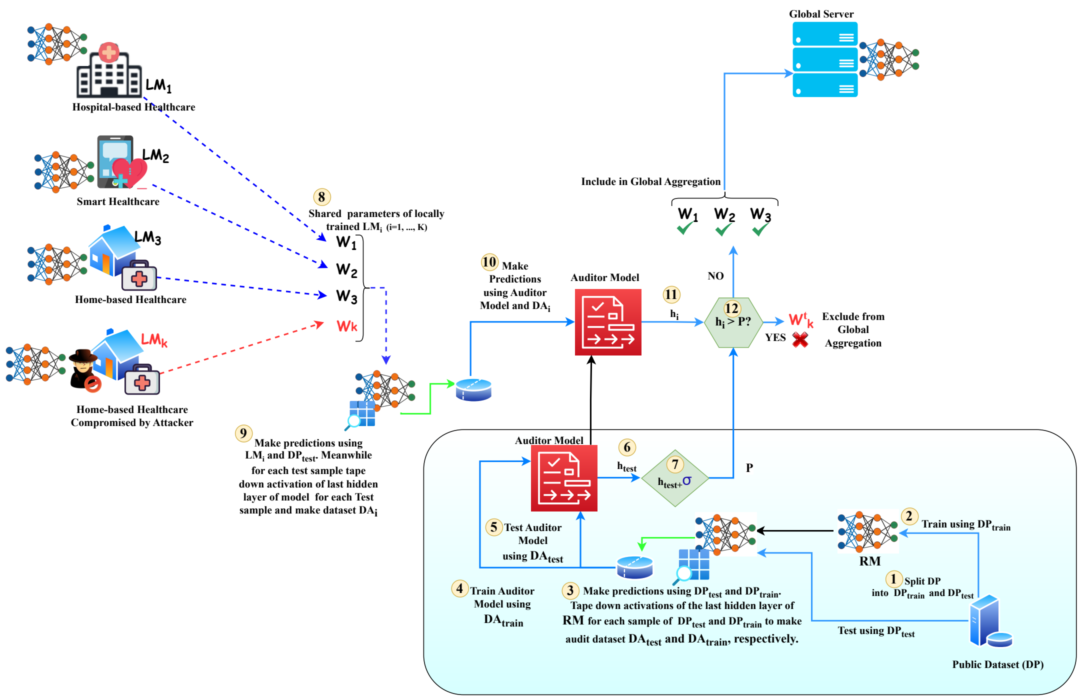


FIGURE 5.7: Overview of the proposed framework

Models trained on similar datasets should exhibit similar behavior, so we utilize the last hidden layer's activations to capture relevant features for detecting poisoning attacks. While other higher-level layers could be used, they increase computational costs without significantly improving detection performance. We train an auxiliary model (AM) to learn the behavior of a benign model (RM), ensuring that models behaving similarly are likely free from poisoning.

5.4.2 Performance Evaluation

We evaluated the proposed framework using two healthcare applications, i.e., ECG classification and HAR. Table 5.6 shows a comparison of our proposed framework with some of the SOTA methods for detecting poisoning attacks in FL [240, 29, 57, 21, 66, 120, 242, 30, 143, 119, 168, 261], where the *Category* column presents the type of detection mechanism, attack type presents a type of attack, the *Model Accuracy* column presents the accuracy of global model under attack compared with the accuracy of the global model without any attack, the *Data Distribution* column presents the type of data distribution among clients: independent identically distributed (IID), non identically distributed (Non-IID), d represents model size (depth) of each client and K is the total number of edge devices/clients. It can be seen that our proposed framework provides more desirable features than all other SOTA methods.

Our proposed framework does not need knowledge about the number of attackers. It can detect both types of attacks, i.e., model and data poisoning attacks. Moreover, its time complexity is the lowest compared to others. Additionally, the proposed method can be used in both IID and non-IID data distributions with high accuracy.

5.5 Contributions about Anomaly Detection in Morphologies of Human Legs for the Implementation of Adaptive Leg Morphotypes and Medical Compression Stockings

Compression therapy is widely used to improve blood circulation and reduce tissue inflammation and lymphatic fluid accumulation[42]. Determining the optimal compression level for treating Chronic Venous Insufficiency (CVI) and Lymphoedema remains a challenge due to variations in leg shape and size[130], making it difficult for the industry to design Medical Compression Stockings that match real anatomy[50]. Deep learning-based methods for 3D shape representation have advanced significantly since 2015, enabling geometric learning from both Euclidean and non-Euclidean 3D data[241, 3]. In our study, we obtained a database of scanned human legs represented as point clouds, later transformed into polygonal meshes through smoothing, hole-filling, and noise removal. Rather than converting these into Euclidean formats, such as 2D projections or voxel grids, we aim to preserve their simplified information. We opt for deep learning techniques that process point clouds directly, as they offer a simple yet effective structure for learning [241].

5.5.1 Anomaly Detection in Morphologies of Human Legs

In this study, we propose a novel approach to anomaly detection by leveraging the Deep Convolutional K-Means (DCKM) [72] and the Elliptic Envelope method [40]. This integrated method is particularly useful in applications such as analyzing the 3D morphologies of human legs, where identifying anomalies is crucial for medical purposes, including designing custom compression stockings. By combining the power of deep learning-based clustering with statistical methods for anomaly detection, we provide an efficient pipeline for analyzing complex morphological data.

DCKM integrates convolutional neural networks (CNNs) with K-means clustering into a unified learning framework. This method leverages the feature extraction power of CNNs while embedding clustering within the learning process. It eliminates the decoder typically seen in encoder-decoder architectures, thereby reducing the risks of overfitting and computational complexity, particularly in data-limited scenarios. DCKM is a notable advancement over traditional deep clustering techniques as it introduces Deep Convolutional Transform Learning (DCTL) [134] to learn compact representations for clustering directly.

The DCTL framework extends convolutional transform learning (CTL) [133] by jointly optimizing the convolutional filters and representations. The key innovation of DCTL is the extension to multiple layers of convolutional transforms, enabling the model to capture hierarchical representations of data and solve unsupervised learning tasks. The DCTL model learns a set of convolutional kernels at each layer by minimizing the following:

$$\min_{T_1,T_2,T_3,Z} \|T_3 * (T_2 * (T_1 * X)) - Z\|_F^2 + \psi(Z) + \lambda \sum_{i=1}^{3} \left(\|T_i\|_F^2 - \log\det(T_i) \right),$$

Where T_1, T_2, T_3 are the convolutional filters applied at different layers, X represents the input data, and Z is the learned representation. The penalty terms $\|T_i\|_F^2$ and $\log\det(T_i)$ are used to prevent trivial or degenerate solutions, thus ensuring that the learned filters are meaningful.

K-means clustering, traditionally used for partitioning data into distinct groups based on feature similarity, is seamlessly embedded into the DCKM model to enable both feature learning and clustering within a single framework. DCKM incorporates K-means clustering by embedding the clustering loss directly into the DCTL framework. The final optimization jointly trains both the convolutional filters and the clustering parameters. Specifically, the clustering loss function is integrated as follows:

$$\text{Loss}_{\text{DCKM}} = \text{Loss}_{\text{DCTL}} + \mu \left\| Z - ZH^T(HH^T)^{-1}H \right\|_F^2,$$

Where H represents the binary cluster indicator matrix, where $h_{ij} = 1$ if the j-th data point belongs to cluster i, and 0 otherwise. This combination allows the DCKM model to improve clustering performance by jointly learning features and cluster assignments.

Given the feature representations of DCKM, we apply the Elliptic Envelope, which is designed to model the shape of the dataset in a lower-dimensional space by assuming that the data follows a multivariate Gaussian distribution. Mathematically, the Elliptic Envelope minimizes the Mahalanobis distance between the data points and the center of the Gaussian distribution:

$$d_M(x) = \sqrt{(x-\mu)^T \Sigma^{-1} (x-\mu)},$$

Where x is a data point, μ is the mean of the data, and Σ is the covariance matrix. Points with a Mahalanobis distance greater than a threshold are considered anomalies. The diagram is shown in Figure 5.8.

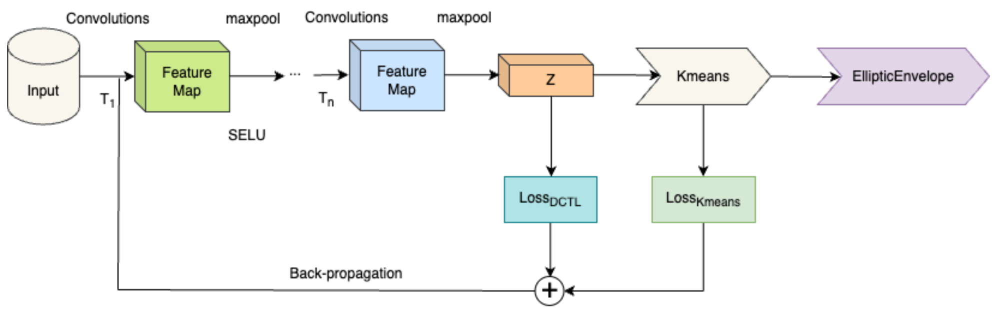


FIGURE 5.8: Diagram of Anomaly Detection with DCKM and Elliptic Envelope

5.5.2 Performance Analysis

The experimental results presented in this section demonstrate the effectiveness of the proposed anomaly detection approach applied to human leg morphologies. The dataset comprised 131 3D scans, constituting 73 from women (63 younger than 30 and 10 older than 30) and 58 from men (49 younger than 30 and 9 older than 30). Additionally, each scan was preprocessed to address geometric inconsistencies and remove noise. The left leg of every subject was then defined in a CAD environment using the anthropometric markers that define a single standard for the entire dataset, illustrated in Figure 5.9.

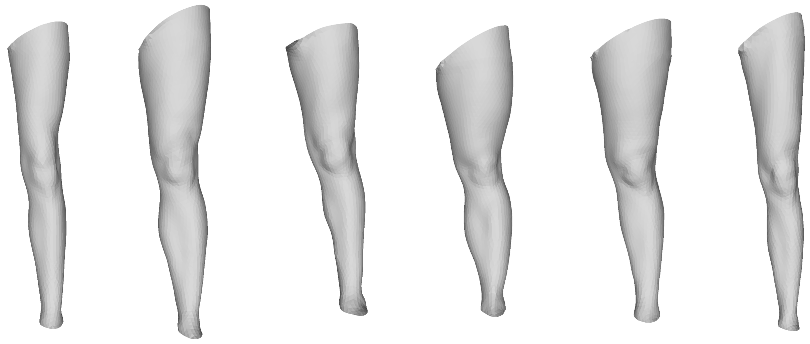


FIGURE 5.9: 3D Mesh Representation of Human Leg Morphology from the dataset

The Deep Convolutional K-Means (DCKM) model is configured with two 3D convolutional layers, each using 8 filters with a 3x3x3 kernel, followed by SELU activations and max-pooling operations. The model is designed to extract features and perform K-Means clustering, using 4 clusters for unsupervised learning on 3D point cloud data. The loss function combines K-Means clustering loss with a regularization term, controlled by $\lambda_{\text{reg}} = 0.001$, to ensure the stability of the convolutional filters. Training is conducted using the Adam optimizer with a learning rate of 0.001 for 2000 epochs on a machine running Python 3.11 and PyTorch, equipped with an Intel i5-13500 CPU @ 3.50GHz, 32GB RAM, 512GB SSD, Nvidia RTX 3060 12GB GPU and the system operates on the Windows Subsystem for Linux (WSL) platform. To input the data into our model, we need to convert the dataset from a mesh to a 3D point cloud, as illustrated in Figure 5.10. The output of the trained Deep Convolutional K-Means (DCKM) model, specifically the flattened feature representations from the final layer, is passed through an Elliptic Envelope (EE) algorithm to detect anomalies. The EE model is initialized with a contamination factor of 0.05, indicating that 5% of the data is expected to be outliers, and trained using the support fraction of 1 to fit the robust covariance estimate. We archived 7 outlier points that were detected. With the help of geodesic paths at 16 anatomical sites, we have visualized certain zones that could explain the outlier characteristics of these 7 subjects. In Figure 5.11, we can visualize the 16 geodesic paths mentioned, which run along the leg from the medial side, circling from front to back, and conform to the shape of the outer soft tissue on every side. For example, Figure 5.11 a., e., i., m. are the side silhouettes of each leg, representing the medial, anterior, lateral, and posterior contours. From these 2D contours, we can easily identify the problematic zones that might have ruled out the identified outliers. While some of the subjects could be excluded because our database has limited obese subjects and subject numbers 20183, 20187 and 20148 are representative of these groups, we can also observe that the anomaly detection observed surface defaults like the folds of the boxer shorts, that could be visualized on the upper segment of Figure 5.11 g., h., i., j. for subject number 10195 and 10159 and folds of the socks that are visible on the lower segment of Figure 5.11 i. and j., for subject 10195 and n. for subject 20148. There could be other observable reasons for the exclusion, such as extreme postural differences between the legs, this tendency is observed in the case of subjects 20183 and 20206, both subjects presenting knock-knee characteristics, meaning that the alignment of their leg is in the shape of an "X". Other observations we made were related to certain soft tissue surface areas that were largely deviated from the other subjects, subject 10195 having a visible bump on Figure 5.11 c., which is a geodesic path that passes over the vastus medialis muscle, which is the medial part of the quadriceps group, and in case of this subject, this muscle is very well developed, creating a visible bump in the upper section of this path. Similarly, we observed a convex indentation in the middle segment of the lower leg in the case of subject 20246, visible in Figure K. In Figure 5.12, the same identified outliers can be visualized, where we highlighted the above-described anomalous regions.

Detecting anomalies in data plays a vital role in enhancing data quality, thereby enabling the training of more robust models. In particular, detecting anomalies in leg morphology data may reveal pathological markers that can classify the anomalies, further fine-tuning the model's training to help attain better results that can eventually contribute to personalized medical applications.

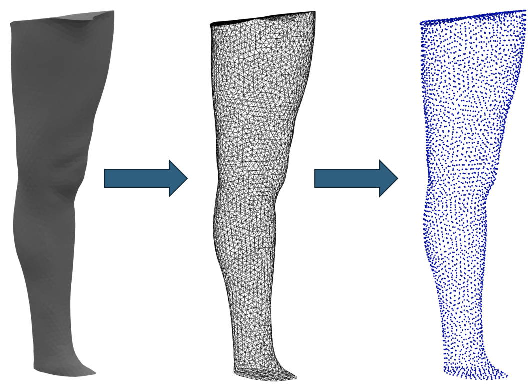


FIGURE 5.10: Meshes convert to 3D point clouds to input into the model

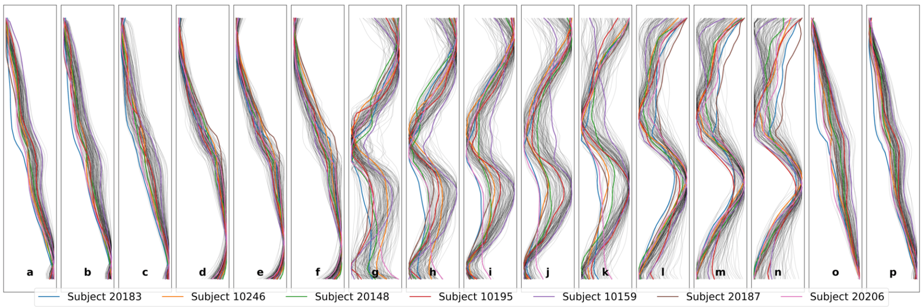


FIGURE 5.11: 2D representation of 16 geodesic paths that run over anatomical sites on the length of the leg

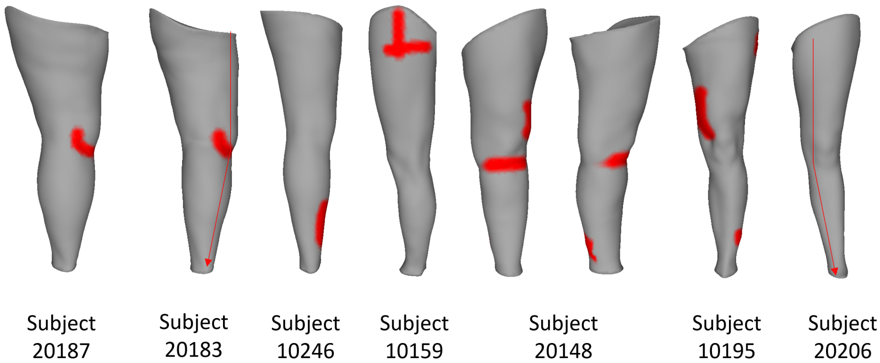


FIGURE 5.12: Highlighted anomalous regions on the 7 identified outliers

The proposed method, combining Deep Convolutional K-Means (DCKM) and Elliptic Envelope for anomaly detection in human leg morphologies, has demonstrated its effectiveness in identifying morphological deviations. By leveraging the power of convolutional neural networks and integrating K-Means to learn latent features, applying the Elliptic Envelope algorithm enables the precise identification of 7 outliers, representing leg shape abnormalities critical in medical contexts, specifically custom medical compression stockings. Our approach's key advantage is its ability to learn features and perform clustering. The K-means loss drives the network to organize similar representations into distinct clusters, while the DCTL framework extracts meaningful features using convolutional operations. The Elliptic Envelope method also enhances the process by identifying potential outliers within the clusters, boosting anomaly detection accuracy. Notwithstanding the success, there are many possibilities for future research to be undertaken. While the study yields promising results, its limitations lie in the "black-box" issue: the lack of transparency in identifying anomalies, which will be addressed by enhancing the method's interpretability in future work. We also plan to apply advanced techniques that can handle mesh data directly rather than being dependent only on point clouds, which may yield even more accurate results in detecting anomalies. In summary, this study highlights the potential of combining Deep Convolutional K-means and Elliptic Envelope techniques to automatically extract key features from 3D point cloud data and accurately detect anomalies in human leg shapes. These results show great promise for the medical compression stocking industry, laying a strong foundation for creating more precise and customized sizing systems tailored to individual needs.

5.6 Conclusions

In this section, we present a novel framework addressing three key areas: Diabetes Classification with ML, an Efficient Lightweight Transformer Architecture for Federated Human Activity Recognition in Smart Healthcare, and Anomaly Detection in Human Leg Morphologies for Adaptive Medical Compression Stockings. Our study highlights the importance of selecting suitable models for electronic diagnostic systems, which enable remote patient monitoring and diabetes management, particularly in postpartum women. We demonstrate the effectiveness of combining data processing techniques such as KNN imputation, ICA, and Isolation Forest to enhance classification performance. The application of SHAP values reveals crucial factors that influence diagnostic decisions. Future research will focus on expanding datasets, particularly from Vietnam, to improve real-time applicability in hospitals. For human activity recognition (HAR), our transformer-based approach outperforms CNN and RNN methods on public and custom datasets. To address privacy and computational challenges, we introduce TransFed, a federated learning framework for HAR classification. We developed a prototype for collecting sensor data from accelerometers, gyroscopes, and magnetometers, optimizing sensor placement for maximum impulse points (PMIs). Our results demonstrate the impact of non-IID data on TransFed's performance, contributing to privacy-preserving HAR applications. In the domain of adaptive medical compression stockings, we propose a novel anomaly detection method using Deep Convolutional K-means (DCKM) and Elliptic Envelope techniques. This approach effectively identifies morphological deviations in human legs, which are crucial for the customization of compression stockings. While our method successfully detects outliers, future work will enhance interpretability and explore advanced techniques for analyzing mesh data directly. To address adversarial attacks in federated learning, we introduce a framework leveraging a reference model and an auditor model to detect poisoning attacks without requiring knowledge of the number of attackers. Our one-class support vector machine (OC-SVM)-based detector achieves optimal computational efficiency (O(K), where K is the number of clients), overcoming the limitations of existing methods. These advancements contribute to improving security, privacy, and performance in FL applications.

Additionally, our recent studies focus on the application of artificial intelligence in the medical field using various advanced methods. The study by Banfalvi et al. proposes the Deep Convolutional K-Means (DCKM) method for clustering human leg morphologies, supporting the improvement of medical compression stocking design and leg morphology classification [17]. Meanwhile, Nguyen et al. have developed an ECG anomaly detection method based on a Transformer-based Variational Autoencoder (VAE) combined with MEWMA-SVDD, which helps reduce the false alarm rate and improve accuracy [155]. Furthermore, Tho et al. applied FT-Transformer to predict diabetes risk in women while also comparing its performance with models such as Tabnet, XGBoost, Random Forest, and Logistic Regression, thereby evaluating the potential of Transformer in processing tabular medical data [206].

Chapter 6

Conclusions, Limitations and Future Work

6.1 Conclusions

In this thesis, we developed frameworks that integrate advanced statistical computing and machine learning techniques to enhance monitoring, anomaly detection, and classification in both smart manufacturing and smart healthcare. These frameworks address key challenges, including the limitations of traditional methods, scalability, real-time processing, privacy concerns, and the need for explainable AI. In smart manufacturing, we introduced machine learning models that effectively handle high-dimensional, non-linear data, enabling real-time fault detection and predictive maintenance. In healthcare, we leveraged federated learning to preserve patient privacy while enabling collaborative anomaly detection across distributed data sources alongside explainable AI models to ensure transparency and interpretability for clinical decision-making. The developed frameworks offer a unified solution, optimizing performance in both domains and ensuring timely interventions, improved system reliability, and greater trust in anomaly detection systems. The integration of these approaches marks a significant step toward enhancing monitoring systems and addressing the complexities inherent in modern industrial and healthcare environments.

6.2 Limitations and Future Work

6.2.1 Limitations

This section discusses some limitations and perspectives of the proposed frameworks.

1. **Dependency on Quality and Availability of Data:** The performance of the proposed frameworks relies heavily on the availability and quality of data from both smart manufacturing and healthcare systems. In smart healthcare, patient data must be accurate, comprehensive, and representative of the target population for effective anomaly detection and classification. Similarly, in manufacturing, the system's success hinges on the availability of high-quality operational data. Data quality can be inconsistent, sparse, or biased in real-world settings, which may impact the framework's robustness and generalizability.

2. **Scalability Challenges:** While the framework addresses the scalability issue in smart manufacturing and healthcare, large-scale deployments (e.g., across multiple manufacturing plants or healthcare institutions) may still face significant challenges. The increase in data volume, complexity, and the number of devices can overwhelm the system's ability to process data in real time, particularly in federated learning environments where decentralized data from multiple sources must be aggregated.

3. **Real-Time Processing and Latency:** Achieving real-time anomaly detection and decision-making can be difficult, especially when dealing with large and high-dimensional datasets. The proposed framework must balance the need for fast processing with the accuracy of the predictions, which may not always be achievable due to limitations in computational resources or the complexity of the data.

4. **Privacy Concerns and Security Risks:** Despite the use of federated learning to preserve patient privacy in healthcare, there are still potential security risks. Adversarial attacks on federated learning systems, such as model poisoning or gradient leakage, could compromise data privacy and system integrity. The proposed framework assumes that federated learning protocols are sufficiently secure; however, the evolving nature of cyber threats may necessitate additional protection measures, which have not been fully addressed in this thesis.

5. **Interpretability and Trust in AI Models:** Although the thesis highlights the importance of explainable AI (XAI) in healthcare and manufacturing, achieving full interpretability of complex machine learning models remains a challenge. Even with the inclusion of XAI techniques, there may still be limitations in providing explanations that are sufficiently transparent for non-expert users, especially in high-stakes environments such as healthcare. This could hinder trust in AI-based decision-making systems by clinicians or operators.

6. **Limited Domain-Specific Validation:** The frameworks proposed in the thesis may work well under controlled conditions or in theoretical scenarios, but real-world validation in diverse environments is necessary for robust performance. For example, while the models are designed for smart manufacturing and healthcare, they may need further refinement or adaptation to specific industry standards, clinical practices, or operational constraints to be effectively deployed in these domains.

7. **Adaptation to Evolving Systems:** In both smart manufacturing and healthcare, systems and environments evolve—whether it's a change in the underlying hardware, new diseases emerging in healthcare, or evolving production processes. The proposed frameworks may face challenges in adapting to such changes, requiring ongoing updates to the models or methodologies, as well as continuous learning mechanisms to handle new, unseen data.

8. **Energy Efficiency:** While real-time processing is emphasized, the energy consumption of complex machine learning models, especially in federated learning scenarios with numerous edge devices, could become a limitation. Smart devices in healthcare or manufacturing environments often have limited computational and energy resources. Without efficient models or low-power techniques, energy consumption can become a bottleneck.

9. **Generalization Across Domains:** The frameworks developed in the thesis aim to optimize performance across both smart manufacturing and healthcare domains, but the specific needs of each domain may require domain-specific adjustments. For example, the anomaly detection models suited for detecting faults in machines may not directly translate to detecting medical anomalies in patient data. Future work may need to address how to better generalize models for various use cases without compromising accuracy or performance.

6.2.2 Future directions

To address the limitations of the proposed framework, some future directions are as follows:

1. **Postdoctoral Research Direction**: My postdoctoral research project on integrating physics-guided deep learning with textile mechanics and biomedical material modeling. Building upon the promising results of the PGNN framework developed in this work—where a Laplacian-based physical prior significantly improved convergence, stability, and mechanical consistency—the next phase of my postdoctoral agenda aims to advance this hybrid modeling approach toward a more comprehensive physics-enabled ecosystem. Specifically, my future work will focus on enriching the physical priors with constitutive laws of elastic yarns, developing multi-scale architectures that bridge yarn-level mechanics with fabric behavior and limb geometry, and coupling the PGNN surrogate models with high-fidelity FEM simulations to enable real-time digital twins of compression garments. Beyond technical development, this project also targets translational impact: designing personalized medical compression systems, optimizing material structures through AI-assisted inverse design, and extending the methodology to broader classes of smart textiles and wearable biomedical systems. As a postdoctoral program, this research represents a strategic pathway toward unifying physics-based modeling and modern AI for next-generation textile engineering and medical device innovation.

2. **Enhancing Data Quality and Availability:** Future work will focus on improving data quality by exploring advanced data preprocessing techniques, such as data augmentation, noise reduction, and anomaly detection during data collection. Additionally, we will explore methods for handling missing data and addressing data imbalances that may impact the performance of anomaly detection models. Collaborations with healthcare institutions and manufacturing industries will help in obtaining more diverse, real-world datasets that are representative of the target environments.

3. **Improving Scalability:** To better handle large-scale deployments, we will explore techniques for distributed computing and parallel processing in federated learning systems. Optimization strategies, such as model pruning and quantization, will also be studied to reduce model

size and computational overhead. Furthermore, a dynamic model architecture that adapts to available resources and data size will be developed to ensure scalability while maintaining real-time processing capabilities.

4. **Latency and Real-Time Processing Optimization:** Addressing the challenge of real-time processing, we will investigate more efficient algorithms that reduce latency without compromising on accuracy. Techniques such as edge computing and model compression will be explored to enable faster processing on edge devices, minimizing delays and ensuring timely anomaly detection in both healthcare and manufacturing applications.

5. **Enhancing Privacy and Security:** To further enhance privacy and security, we will integrate more robust federated learning protocols, such as differential privacy and secure multi-party computation, to mitigate the risks of data leakage and malicious attacks. We will also investigate adversarial training techniques to enhance the resilience of models against poisoning attacks and improve the security of federated learning systems.

6. **Advancing Interpretability and Trust in AI Models:** To improve the interpretability and trustworthiness of AI models, we will focus on developing novel methods for explainability that are tightly coupled with model design rather than relying solely on post-hoc explanation techniques. Techniques like feature importance, saliency maps, and decision trees will be explored to ensure transparency in the decision-making process. We will also work on designing user-friendly interfaces for non-expert users to facilitate understanding and trust in the system's predictions.

7. **Designing Explainable-by-Design Models:** As part of future work, we will focus on developing AI models that are inherently explainable by design. This will involve creating machine learning models that integrate explainability features into their architecture, ensuring transparency and interpretability at every level of the decision-making process. These models will be designed to provide clear, concise explanations to clinicians and manufacturing operators during real-time anomaly detection.

8. **Expanding Real-World Validation:** The proposed framework will be tested in more diverse and real-world settings, involving a wider range of participants in healthcare and manufacturing. This will help ensure

that the models are generalizable and can perform effectively across different industries and patient demographics. Collaborative studies with healthcare professionals, engineers, and end-users will also be conducted to evaluate the practicality and effectiveness of the framework.

9. **Adapting to Evolving Systems:** We will explore techniques for continuous learning to ensure that the system can adapt to evolving data and environments. This will involve implementing mechanisms to update models in real time as new data becomes available, without requiring complete retraining. We will also investigate how to incorporate emerging technologies, such as IoT devices and wearable sensors, to enhance system adaptability.

10. **Improving Energy Efficiency:** To address the energy consumption challenges, we will focus on optimizing the federated learning process for energy efficiency by incorporating techniques like model quantization, low-power model inference, and hardware acceleration. Research will be conducted on energy-efficient edge devices and optimized algorithms that minimize the energy cost while maintaining performance.

11. **Domain-Specific Customization:** Future work will include developing domain-specific models that tailor the anomaly detection framework to the unique requirements of different industries, such as healthcare, manufacturing, or even automotive. This will ensure that the models are more relevant and capable of detecting subtle anomalies that may be specific to a particular domain.

References

[1] Kiran Adnan et al. "Role and Challenges of Unstructured Big Data in Healthcare". In: *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1*. Springer, 2020, pp. 301–323. DOI: 10.1007/978-981-32-9949-8_22.

[2] B Shamreen Ahamed, Meenakshi S Arya, and Auxilia Osvin V Nancy. "Diabetes mellitus disease prediction using machine learning classifiers with oversampling and feature augmentation". In: *Advances in Human-Computer Interaction* 2022.1 (2022), p. 9220560.

[3] E Ahmed et al. "A survey on deep learning advances on different 3D data representations. arXiv 2018". In: *arXiv preprint arXiv:1808.01462* (2019).

[4] Shamim Ahmed et al. "A Comparative Analysis of LIME and SHAP Interpreters with Explainable ML-Based Diabetes Predictions". In: *IEEE Access* (2024).

[5] M. Ahsan et al. "Support vector data description with kernel density estimation (SVDD-KDE) control chart for network intrusion monitoring". In: *Scientific Reports* 13.1 (2023), p. 19149.

[6] J. Aitchison. *The Statistical Analysis of Compositional Data (Monographs on Statistics and Applied Probability)*. Chapman & Hall Ltd., London, (Reprinted in 2003 with additional material by The Blackburn Press), 1986.

[7] John Aitchison. "The statistical analysis of compositional data". In: *Journal of the Royal Statistical Society: Series B (Methodological)* 44.2 (1982), pp. 139–160.

[8] Mohammed Aledhari et al. "Federated learning: A survey on enabling technologies, protocols, and applications". In: *IEEE Access* 8 (2020), pp. 140699–140725.

[9] Layth C Alwan and Harry V Roberts. "Time-series modeling for statistical process control". In: *Journal of business & economic statistics* 6.1 (1988), pp. 87–95.

[10] Apple Inc. *Use Driving Focus on your iPhone to concentrate on the road*. Online document. 2021. URL: https://support.apple.com/en-gb/HT208090.

[11] Sercan Ö Arik and Tomas Pfister. "Tabnet: Attentive interpretable tabular learning". In: *Proceedings of the AAAI conference on artificial intelligence*. Vol. 35. 8. 2021, pp. 6679–6687.

[12] Leo A Aroian and Howard Levene. "The effectiveness of quality control charts". In: *Journal of the American Statistical Association* 45.252 (1950), pp. 520–529.

[13] Kebira Azbeg et al. "Diabetes emergency cases identification based on a statistical predictive model". In: *Journal of Big Data* 9.1 (2022), p. 31.

[14] Jean-Louis Auget Balakrishnan. "Statistics for Industry and Technology". In: (2007).

[15] Uditha Balasooriya and N Balakrishnan. "Reliability sampling plans for lognormal distribution, based on progressively-censored samples". In: *IEEE Transactions on Reliability* 49.2 (2000), pp. 199–203.

[16] A. Banerjee, P. Burlina, and R. Meth. "Fast Hyperspectral Anomaly Detection via SVDD". In: *2007 IEEE International Conference on Image Processing*. Vol. 4. 2007, pp. IV-101 - IV–104.

[17] T. Banfalvi et al. "Deep Convolutional K-Means of 3D morphologies of human legs for the implementation of adaptive leg morphotypes and Medical Compression Stockings". In: *International Conference on Responsible Artificial Intelligence and Data Science*. Springer. 2024, pp. 83–109.

[18] Xianglin Bao et al. "Flchain: A blockchain for auditable federated learning with trust and incentive". In: *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*. IEEE. 2019, pp. 151–159.

[19] Battista Biggio, Blaine Nelson, and Pavel Laskov. "Poisoning Attacks against Support Vector Machines". In: *Proceedings of the 29th International Conference on Machine Learning*. ICML, 2012, pp. 1467–1474. URL: https://icml.cc/2012/papers/880.pdf.

[20] Ermiyas Birihanu and Imre Lendák. "Explainable correlation-based anomaly detection for Industrial Control Systems". In: *Frontiers in Artificial Intelligence* 7 (2025), p. 1508821.

[21] Peva Blanchard et al. "Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent". In: *Advances in Neural Information Processing Systems*. Vol. 30. Curran Associates, Inc., 2017, pp. 119–129. URL: https://papers.nips.cc/paper/2017/hash/f4b9ec30ad9f68f89b29639786cb62ef-Abstract.html.

[22] Keith Bonawitz et al. "Towards Federated Learning at Scale: System Design". In: *Proceedings of Machine Learning and Systems*. Ed. by A. Talwalkar, V. Smith, and M. Zaharia. Vol. 1. 2019, pp. 374–388. URL: https://proceedings.mlsys.org/paper_files/paper/2019/file/7b770da633baf74895be22a8807f1a8f-Paper.pdf.

[23] R. A. Boyles. "Using the chi-square statistic to monitor compositional process data". In: *Journal of Applied Statistics* 24.5 (1997), pp. 589–602. eprint: http://dx.doi.org/10.1080/02664769723567.

[24] H Brian Hwarng and Yu Wang. "Shift detection and source identification in multivariate autocorrelated processes". In: *International Journal of Production Research* 48.3 (2010), pp. 835–859.

[25] Lucas C. Brito et al. "An explainable artificial intelligence approach for unsupervised fault detection and diagnosis in rotating machinery". In: *Mechanical Systems and Signal Processing* 163 (2022), p. 108105. ISSN: 0888-3270. DOI: https://doi.org/10.1016/j.ymssp.2021.108105. URL: https://www.sciencedirect.com/science/article/pii/S0888327021004891.

[26] DAED Brook and DA Evans. "An approach to the probability distribution of CUSUM run length". In: *Biometrika* 59.3 (1972), pp. 539–549.

[27] Sonal Budhiraja and Biswabrata Pradhan. "Computing optimum design parameters of a progressive type I interval censored life test from a cost model". In: *Applied Stochastic Models in Business and Industry* 33.5 (2017), pp. 494–506.

[28] Vitalik Buterin et al. "A next-generation smart contract and decentralized application platform". In: *white paper* 3.37 (2014), pp. 2–1.

[29] Di Cao et al. "Understanding Distributed Poisoning Attack in Federated Learning". In: *Proceedings of the 25th International Conference on Parallel and Distributed Systems*. 2019, pp. 233–239. DOI: 10.1109/ICPADS47876.2019.00042.

[30] Xinyang Cao and Lifeng Lai. "Distributed Gradient Descent Algorithm Robust to an Arbitrary Number of Byzantine Attackers". In: *IEEE Transactions on Signal Processing* 67.22 (2019), pp. 5850–5864. DOI: 10.1109/TSP.2019.2946020.

[31] Philippe Castagliola, Giovanni Celano, and Stelios Psarakis. "Monitoring the coefficient of variation using EWMA charts". In: *Journal of Quality Technology* 43.3 (2011), pp. 249–265.

[32] G. Celano and P. Castagliola. "Design of a Phase II Control Chart for Monitoring the Ratio of two Normal Variables". In: *Quality and Reliability Engineering International* 32 (2014).

[33] Giovanni Celano and Philippe Castagliola. "Design of a phase II control chart for monitoring the ratio of two normal variables". In: *Quality and Reliability Engineering International* 32.1 (2016), pp. 291–308.

[34] Giovanni Celano et al. "Statistical performance of a control chart for individual observations monitoring the ratio of two normal variables". In: *Quality and Reliability Engineering International* 30.8 (2014), pp. 1361–1377.

[35] Ahmad Chaddad et al. "Explainable, domain-adaptive, and federated artificial intelligence in medicine". In: *IEEE/CAA Journal of Automatica Sinica* 10.4 (2023), pp. 859–876.

[36] V. Chandola, A. Banerjee, and V. Kumar. "Anomaly detection: A survey". In: *ACM computing surveys (CSUR)* 41.3 (2009), pp. 1–58.

[37] Chih-Chung Chang and Chih-Jen Lin. "Training v-support vector classifiers: theory and algorithms". In: *Neural computation* 13.9 (2001), pp. 2119–2147.

[38] Victor Chang et al. "Pima Indians diabetes mellitus classification based on machine learning (ML) algorithms". In: *Neural Computing and Applications* 35.22 (2023), pp. 16157–16173.

[39] Danton S. Char, Nigam H. Shah, and David Magnus. "Implementing Machine Learning in Health Care – Addressing Ethical Challenges". In: *New England Journal of Medicine* 378.11 (2018), pp. 981–983. DOI: 10.1056/NEJMp1714229. URL: https://doi.org/10.1056/NEJMp1714229.

[40] Jinyin Chen et al. "DeepPoison: Feature Transfer Based Stealthy Poisoning Attack for DNNs". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 68.7 (2021), pp. 2618–2622. URL: https://doi.org/10.1109/TCSII.2021.3060896.

[41] S. Chen, J. Yu, and S. Wang. "Monitoring of complex profiles based on deep stacked denoising autoencoders". In: *Computers & Industrial Engineering* 143 (2020), p. 106402.

[42] A Cornu-Thénard et al. "Bas de contention ou bas de compression? Une question de définition". In: *Phlébologie* 60.2 (2007), pp. 179–86.

[43] Nahuel Costa and Luciano Sánchez. “Variational encoding approach for interpretable assessment of remaining useful life estimation”. In: *Reliability Engineering & System Safety* 222 (2022), p. 108353.

[44] Jianjing Cui et al. “Comparative study of CNN and RNN for deep learning based intrusion detection system”. In: *Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part V 4*. Springer. 2018, pp. 159–170.

[45] Pinchen Cui et al. “A blockchain-based framework for supply chain provenance”. In: *Ieee Access* 7 (2019), pp. 157113–157125.

[46] Othmane Daanouni, Bouchaib Cherradi, and Amal Tmiri. “Predicting diabetes diseases using mixed data and supervised machine learning algorithms”. In: *Proceedings of the 4th International Conference on Smart City Applications*. 2019, pp. 1–6.

[47] Othmane Daanouni, Bouchaib Cherradi, and Amal Tmiri. “Type 2 diabetes mellitus prediction model based on machine learning approach”. In: *Innovations in Smart Cities Applications Edition 3: The Proceedings of the 4th International Conference on Smart City Applications 4*. Springer. 2020, pp. 454–469.

[48] Erik Daniel and Florian Tschorsch. “IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks”. In: *IEEE Communications Surveys & Tutorials* 24.1 (2022), pp. 31–52.

[49] S Abedin Daryabari, Behnam Malmir, and Amirhossein Amiri. “Monitoring Bernoulli processes considering measurement errors and learning effect”. In: *Quality and Reliability Engineering International* 35.4 (2019), pp. 1129–1143.

[50] Alun H Davies. “The seriousness of chronic venous disease: a review of real-world evidence”. In: *Advances in therapy* 36.Suppl 1 (2019), pp. 5–12.

[51] Ittai Dayan et al. “Federated learning for predicting clinical outcomes in patients with COVID-19”. In: *Nature medicine* 27.10 (2021), pp. 1735–1743.

[52] Emiliano De Cristofaro. “A Critical Overview of Privacy in Machine Learning”. In: *IEEE Security & Privacy* 19.4 (2021), pp. 19–27. DOI: 10.1109/MSEC.2021.3076443.

[53] Massimo Di Pierro. “What is the blockchain?” In: *Computing in Science & Engineering* 19.5 (2017), pp. 92–95.

[54] Yunfeng Diao et al. "Understanding the vulnerability of skeleton-based Human Activity Recognition via black-box attack". In: *Pattern Recognition* 153 (2024), p. 110564.

[55] Kim Duc Tran et al. "Design of a variable sampling interval exponentially weighted moving average median control chart in presence of measurement errors". In: *Quality and Reliability Engineering International* 37.1 (2021), pp. 374–390.

[56] Houda El Bouhissi et al. "Towards diabetes mellitus prediction based on machine-learning". In: *2023 International Conference on Smart Computing and Application (ICSCA)*. IEEE. 2023, pp. 1–6.

[57] El Mahdi El Mhamdi, Rachid Guerraoui, and Sébastien Rouault. "The Hidden Vulnerability of Distributed Learning in Byzantium". In: *Proceedings of the 35th International Conference on Machine Learning*. Vol. 80. Proceedings of Machine Learning Research. PMLR, 2018, pp. 3521–3530. URL: https://proceedings.mlr.press/v80/mhamdi18a.html.

[58] Hatem M Elattar, Hamdy K Elminir, and AM Riad. "Towards online data-driven prognostics system". In: *Complex & Intelligent Systems* 4 (2018), pp. 271–282.

[59] Iñaki Elía and Miguel Pagola. "Anomaly detection in Smart-manufacturing era: A review". In: *Engineering Applications of Artificial Intelligence* 139 (2025), p. 109578.

[60] André Listou Ellefsen et al. "Remaining useful life predictions for turbofan engine degradation using semi-supervised deep architecture". In: *Reliability Engineering & System Safety* 183 (2019), pp. 240–251.

[61] Çağatay Berke Erdaş and Selda Güney. "Human activity recognition by using different deep learning approaches for wearable sensors". In: *Neural Processing Letters* 53.3 (2021), pp. 1795–1809.

[62] Absalom E Ezugwu et al. "A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects". In: *Engineering Applications of Artificial Intelligence* 110 (2022), p. 104743.

[63] Carlos Ferreira and Gil Gonçalves. "Remaining Useful Life prediction and challenges: A literature review on the use of Machine Learning Methods". In: *Journal of Manufacturing Systems* 63 (2022), pp. 550–562.

[64] John Fields, Kevin Chovanec, and Praveen Madiraju. "A survey of text classification with transformers: How wide? how large? how long? how accurate? how expensive? how safe?" In: *IEEE Access* 12 (2024), pp. 6518–6531.

[65] Tim RL Fry, Simon Broadbent, and Janine M Dixon. "Estimating advertising half-life and the data interval bias". In: (1999).

[66] Clement Fung, Chris JM Yoon, and Ivan Beschastnikh. *Mitigating sybils in federated learning poisoning*. 2018. DOI: 10.48550/arXiv.1808.04866.

[67] Kuofeng Gao et al. "Backdoor attack on hash-based image retrieval via clean-label data poisoning". In: *arXiv preprint arXiv:2109.08868* (2021).

[68] Robert X Gao et al. "Artificial Intelligence in manufacturing: State of the art, perspectives, and future directions". In: *CIRP Annals* (2024).

[69] Mohammadhossein Ghahramani et al. "AI-based modeling and data-driven evaluation for smart manufacturing processes". In: *IEEE/CAA Journal of Automatica Sinica* 7.4 (2020), pp. 1026–1037.

[70] Sunil Ghane et al. "Diabetes Prediction using Feature Extraction and Machine Learning Models". In: *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE. 2021, pp. 1652–1657.

[71] Anurag Goel et al. "Deep Convolutional K-Means Clustering". In: *2022 IEEE International Conference on Image Processing (ICIP)*. 2022, pp. 211–215. DOI: 10.1109/ICIP46576.2022.9897742.

[72] Anurag Goel et al. "Deep Convolutional K-Means Clustering". In: *2022 IEEE International Conference on Image Processing (ICIP)*. 2022, pp. 211–215. DOI: 10.1109/ICIP46576.2022.9897742.

[73] Ian Goodfellow et al. "Generative adversarial nets". In: *Advances in neural information processing systems* 27 (2014).

[74] Alex Graves, Abdel-rahman Mohamed, and Geoffrey Hinton. "Speech recognition with deep recurrent neural networks". In: *2013 IEEE international conference on acoustics, speech and signal processing*. Ieee. 2013, pp. 6645–6649.

[75] R. Guevara, J. Vargas, and D. Linero Segrera. "Profile Monitoring for Compositional Data". In: *Revista Colombiana de Estadística* 37 (July 2014), p. 159.

[76] Serdar Gündoğdu. "Efficient prediction of early-stage diabetes using XGBoost classifier with random forest feature selection technique". In: *Multimedia Tools and Applications* 82.22 (2023), pp. 34163–34181.

[77] David Gunning et al. "XAI—Explainable artificial intelligence". In: *Science robotics* 4.37 (2019), eaay7120.

[78] Ashish Gupta et al. *Long-Short History of Gradients is All You Need: Detecting Malicious and Unreliable Clients in Federated Learning*. arXiv preprint arXiv:2208.10273. 2022. DOI: 10.48550/arXiv.2208.10273.

[79] Firoozeh Haghighi, Francis Pascual, and Philippe Castagliola. "Conditional control charts for Weibull quantiles under type II censoring". In: *Quality and Reliability Engineering International* 31.8 (2015), pp. 1649–1664.

[80] Aljaafari Hamza and Basant Kumar. "A review paper on DES, AES, RSA encryption standards". In: *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*. IEEE. 2020, pp. 333–338.

[81] Shahid A Hasib et al. "A comprehensive review of available battery datasets, RUL prediction approaches, and advanced battery management". In: *Ieee Access* 9 (2021), pp. 86166–86193.

[82] Zeynab Hassani, Amirhossein Amiri, and Philippe Castagliola. "Variable Sample Size EWMA Chart With Measurement Errors". In: *Scientia Iranica* (2019).

[83] Sepp Hochreiter and Jürgen Schmidhuber. "Long short-term memory". In: *Neural computation* 9.8 (1997), pp. 1735–1780.

[84] Dongkun Hou et al. "A systematic literature review of blockchain-based federated learning: Architectures, applications and issues". In: *2021 2nd Information communication technologies conference (ICTC)*. IEEE. 2021, pp. 302–307.

[85] Shengshan Hu et al. *Challenges and approaches for mitigating byzantine attacks in federated learning*. arXiv:2112.14468 [cs.CR]. 2022. URL: https://doi.org/10.48550/arXiv.2112.14468.

[86] Xin Huang et al. "Tabtransformer: Tabular data modeling using contextual embeddings". In: *arXiv preprint arXiv:2012.06678* (2020).

[87] Xuan Huang, Søren Bisgaard, and Nuo Xu. "Model-based multivariate monitoring charts for autocorrelated processes". In: *Quality and Reliability Engineering International* 30.4 (2014), pp. 527–543.

[88] Truong Thu Huong et al. "Anomaly Detection Enables Cybersecurity with Machine Learning Techniques". In: *Machine Learning and Probabilistic Graphical Models for Decision Support Systems*. CRC Press, 2023, pp. 124–183.

[89] Adedoyin A Hussain and Fadi Al-Turjman. "Artificial intelligence and blockchain: A review". In: *Transactions on emerging telecommunications technologies* 32.9 (2021), e4268.

[90] Andrey Ignatov. “Real-time human activity recognition from accelerometer data using Convolutional Neural Networks”. In: *Applied Soft Computing* 62 (2018), pp. 915–922. DOI: 10.1016/j.asoc.2017.09.027.

[91] M. Imran et al. “Analyzing out-of-control signals of T2 control chart for compositional data using artificial neural networks”. In: *Expert Systems with Applications* 238 (2024), p. 122165.

[92] M. Imran et al. “Effect of measurement errors on the multivariate CUSUM CoDa control chart for the manufacturing process”. In: *arXiv preprint arXiv:2201.12318* (2022).

[93] M. Imran et al. “Evaluating the performance of variable sampling interval Hotelling T2 charting scheme for compositional data in the presence of measurement error”. In: *Quality and Reliability Engineering International* (2023).

[94] M. Imran et al. “Incorporating principal component analysis into Hotelling T2 control chart for compositional data monitoring”. In: *Computers & Industrial Engineering* 186 (2023), p. 109755.

[95] M. Imran et al. “Investigating zero-state and steady-state performance of MEWMA-CoDa control chart using variable sampling interval”. In: *Journal of Applied Statistics* (2023), pp. 1–22.

[96] M. Imran et al. “On designing efficient multivariate exponentially weighted moving average control chart for compositional data using variable sample size”. In: *Journal of Statistical Computation and Simulation* 93.10 (2023), pp. 1622–1643.

[97] Kürşat İnce, Uğur Ceylan, and Yakup Genç. “Remaining Useful Life Prediction on C-MAPSS Dataset via Joint Autoencoder-Regression Architecture”. In: *2022 30th Signal Processing and Communications Applications Conference (SIU)*. IEEE. 2022, pp. 1–4.

[98] Md Rashedul Islam and Fahmid Al Farid. “Advancements in AI-Based Anomaly Detection for Smart Manufacturing”. In: *Artificial Intelligence for Smart Manufacturing and Industry X. 0* (2025), pp. 37–68.

[99] Hyejun Jeong et al. “FedCC: Robust Federated Learning against Model Poisoning Attacks”. In: *arXiv preprint arXiv:2212.01976* (2022). DOI: 10.48550/arXiv.2212.01976.

[100] Arlind Kadra et al. “Well-tuned simple nets excel on tabular datasets”. In: *Advances in neural information processing systems* 34 (2021), pp. 23928–23941.

[101] Peter Kairouz et al. “Advances and open problems in federated learning”. In: *Foundations and Trends® in Machine Learning* 14.1–2 (2021), pp. 1–210.

[102] AA Kalgonda and SR Kulkarni. “Multivariate quality control chart for autocorrelated processes”. In: *Journal of Applied Statistics* 31.3 (2004), pp. 317–327.

[103] Anwer Khurshid and Ashit B Chakraborty. “Power of Control Chart for the Ratio of Two Poisson Distributions Under Misclassification Error”. In: *Yugoslav Journal of Operations Research* 430(2) (2020), pp. 199–208.

[104] Hafsa Binte Kibria et al. “An ensemble approach for the prediction of diabetes mellitus using a soft voting classifier with an explainable AI”. In: *Sensors* 22.19 (2022), p. 7268.

[105] Diederik P Kingma, Max Welling, et al. *Auto-encoding variational bayes*. 2013.

[106] Sven Knoth and Wolfgang Schmid. “Control charts for time series: A review”. In: *Frontiers in statistical quality control 7* (2004), pp. 210–236.

[107] Anusuya Krishnan. “Exploring Machine Learning and Transformer-based Approaches for Deceptive Text Classification: A Comparative Analysis”. In: *arXiv preprint arXiv:2308.05476* (2023).

[108] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. “Imagenet classification with deep convolutional neural networks”. In: *Advances in neural information processing systems* 25 (2012).

[109] S. Kumar et al. “Kernel distance-based robust support vector methods and its application in developing a robust K-chart”. In: *International Journal of Production Research* 44.1 (2006), pp. 77–96.

[110] Andrew Kusiak. “Smart manufacturing”. In: *International journal of production Research* 56.1-2 (2018), pp. 508–517.

[111] Saeb Ragani Lamooki et al. “A data analytic end-to-end framework for the automated quantification of ergonomic risk factors across multiple tasks using a single wearable sensor”. In: *Applied Ergonomics* 102 (2022), p. 103732.

[112] Jerry F Lawless. “Confidence interval estimation for the Weibull and extreme value distributions”. In: *Technometrics* 20.4 (1978), pp. 355–364.

[113] Jay Lee, Behrad Bagheri, and Hung-An Kao. "A cyber-physical systems architecture for industry 4.0-based manufacturing systems". In: *Manufacturing letters* 3 (2015), pp. 18–23.

[114] Yaguo Lei et al. "Machinery health prognostics: A systematic review from data acquisition to RUL prediction". In: *Mechanical systems and signal processing* 104 (2018), pp. 799–834.

[115] Roberto Campos Leoni et al. "The skipping strategy to reduce the effect of the autocorrelation on the T 2 chart's performance". In: *The International Journal of Advanced Manufacturing Technology* 80 (2015), pp. 1547–1559.

[116] Bing Li et al. "Two-Stream Convolution Augmented Transformer for Human Activity Recognition". In: *Proceedings of the 2021 AAAI Conference on Artificial Intelligence*. Vol. 35. AAAI, 2021, pp. 286–293. URL: https://ojs.aaai.org/index.php/AAAI/article/view/16103.

[117] Dong Li, Zai Luo, and Bo Cao. "Blockchain-based federated learning methodologies in smart environments". In: *Cluster Computing* 25.4 (2022), pp. 2585–2599.

[118] Hongxia Li et al. "Fedtp: Federated learning by transformer personalization". In: *IEEE transactions on neural networks and learning systems* (2023).

[119] Liping Li et al. "RSA: Byzantine-robust stochastic aggregation methods for distributed learning from heterogeneous datasets". In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 33. 01. 2019, pp. 1544–1551. DOI: 10.1609/aaai.v33i01.33011544.

[120] Suyi Li et al. *Abnormal client behavior detection in federated learning*. arXiv preprint arXiv:1910.09933. 2019. DOI: 10.48550/arXiv.1910.09933.

[121] Tian Li et al. "Federated Learning: Challenges, Methods, and Future Directions". In: *IEEE Signal Processing Magazine* 37.3 (2020), pp. 50–60. DOI: 10.1109/MSP.2020.2975749.

[122] Xiang Li et al. "On the convergence of fedavg on non-iid data". In: *arXiv preprint arXiv:1907.02189* (2019).

[123] Yuzheng Li et al. "A blockchain-based decentralized federated learning framework with committee consensus". In: *IEEE Network* 35.1 (2020), pp. 234–241.

[124] JiGuan G Lin. "On min-norm and min-max methods of multi-objective optimization". In: *Mathematical programming* 103.1 (2005), pp. 1–33.

[125] K.W. Linna, W.H. Woodall, and K.L. Busby. “The performance of multivariate control charts in the presence of measurement error”. In: *Journal of Quality Technology* 33.3 (2001), p. 349.

[126] Ruixuan Liu et al. “FedSel: Federated SGD Under Local Differential Privacy with Top-k Dimension Selection”. In: *Database Systems for Advanced Applications: 25th International Conference, DASFAA 2020, Jeju, South Korea, September 24–27, 2020, Proceedings, Part I*. Springer, 2020, pp. 485–501. DOI: 10.1007/978-3-030-59410-7_33.

[127] Cynthia A Lowry and Douglas C Montgomery. “A review of multivariate control charts”. In: *IIE transactions* 27.6 (1995), pp. 800–810.

[128] Yunlong Lu et al. “Blockchain and federated learning for privacy-preserved data sharing in industrial IoT”. In: *IEEE Transactions on Industrial Informatics* 16.6 (2019), pp. 4177–4186.

[129] James M Lucas and Michael S Saccucci. “Exponentially weighted moving average control schemes: properties and enhancements”. In: *Technometrics* 32.1 (1990), pp. 1–12.

[130] KA Lurie and Andrej V Cherkaev. “" Effective Characteristics of Composite Materials and the Optimal Design of Structural Elements”. In: *Topics in the mathematical modelling of composite materials* (2018), pp. 175–271.

[131] Chuan Ma et al. “When federated learning meets blockchain: A new distributed learning paradigm”. In: *IEEE Computational Intelligence Magazine* 17.3 (2022), pp. 26–33.

[132] E.M. Maboudou-Tchao, I. R. Silva, and N. Diawara. “Monitoring the mean vector with Mahalanobis kernels”. In: *Quality Technology & Quantitative Management* 15.4 (2018), pp. 459–474.

[133] Jyoti Maggu et al. “Convolutional Transform Learning”. In: *Neural Information Processing*. Ed. by Long Cheng, Andrew Chi Sing Leung, and Seiichi Ozawa. Cham: Springer International Publishing, 2018, pp. 162–174. ISBN: 978-3-030-04182-3.

[134] Jyoti Maggu et al. “Deep Convolutional Transform Learning”. In: *Neural Information Processing*. Ed. by Haiqin Yang et al. Cham: Springer International Publishing, 2020, pp. 300–307. ISBN: 978-3-030-63823-8.

[135] Priyanka Mary Mammen. “Federated learning: Opportunities and challenges”. In: *arXiv preprint arXiv:2101.05428* (2021).

[136] Roshan Joy Martis, U Rajendra Acharya, and Lim Choo Min. "ECG beat classification using PCA, LDA, ICA and discrete wavelet transform". In: *Biomedical Signal Processing and Control* 8.5 (2013), pp. 437–448.

[137] Brendan McMahan et al. "Communication-Efficient Learning of Deep Networks from Decentralized Data". In: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*. Vol. 54. Proceedings of Machine Learning Research. PMLR, 2017, pp. 1273–1282. URL: https://proceedings.mlr.press/v54/mcmahan17a.html.

[138] Brendan McMahan et al. "Communication-efficient learning of deep networks from decentralized data". In: *Artificial intelligence and statistics*. PMLR. 2017, pp. 1273–1282.

[139] H. Brendan McMahan et al. *Federated learning of deep networks using model averaging*. arXiv:1602.05629 [cs.LG]. 2016. DOI: 10.48550/arXiv.1602.05629.

[140] Tom M Mitchell and Tom M Mitchell. *Machine learning*. Vol. 1. 9. McGraw-hill New York, 1997.

[141] Douglas C Montgomery. *Introduction to statistical quality control*. John wiley & sons, 2019.

[142] Douglas C Montgomery. *Introduction to statistical quality control*. John wiley & sons, 2019.

[143] Luis Muñoz-González, Kenneth T Co, and Emil C Lupu. *Byzantine-robust federated machine learning through adaptive model averaging*. arXiv preprint arXiv:1909.05125. 2019. DOI: 10.48550/arXiv.1909.05125.

[144] Abdulmajid Murad and Jae-Young Pyun. "Deep Recurrent Neural Networks for Human Activity Recognition". In: *Sensors* 17.11 (2017), 2556:1–2556:17. DOI: 10.3390/s17112556.

[145] H. K. T. Ng, P. S. Chan, and N. Balakrishnan. "Optimal progressive censoring plans for the Weibull distribution". In: *Technometrics* 46.4 (2004), pp. 470–481.

[146] Dac Hieu Nguyen et al. "Physics-Informed Machine Learning for Industrial Reliability and Safety Engineering: A Review and Perspective". In: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges* (2024), pp. 5–23.

[147] Dinh C Nguyen et al. "Federated learning meets blockchain in edge computing: Opportunities and challenges". In: *IEEE Internet of Things Journal* 8.16 (2021), pp. 12806–12825.

[148] H.D. Nguyen et al. “The Shewhart-type RZ control chart for monitoring the ratio of autocorrelated variables”. In: *International Journal of Production Research* 61.20 (2023), pp. 6746–6771.

[149] HD Nguyen, Kim Phuc Tran, and Kim Duc Tran. “The effect of measurement errors on the performance of the exponentially weighted moving average control charts for the ratio of two normally distributed variables”. In: *European Journal of Operational Research* 293.1 (2021), pp. 203–218.

[150] Huu Du Nguyen and Kim Phuc Tran. “Effect of the measurement errors on two one-sided Shewhart control charts for monitoring the ratio of two normal variables”. In: *Quality and Reliability Engineering International* (2020).

[151] Le Hoang Nguyen et al. “Human-Centered Edge Artificial Intelligence for Smart Factory Applications in Industry 5.0: A Review and Perspective”. In: *Artificial Intelligence for Safety and Reliability Engineering: Methods, Applications, and Challenges* (2024), pp. 79–100.

[152] Quoc Thong Nguyen et al. “One-sided synthetic control charts for monitoring the multivariate coefficient of variation”. In: *Journal of Statistical Computation and Simulation* 89.10 (2019), pp. 1841–1862.

[153] Quoc-Thông Nguyen et al. “One-sided variable sampling interval EWMA control charts for monitoring the multivariate coefficient of variation in the presence of measurement errors”. In: *The International Journal of Advanced Manufacturing Technology* 115 (2021), pp. 1821–1851.

[154] T.T.V. Nguyen, C. Heuchenne, and K.P. Tran. “Anomaly Detection for Compositional Data using VSI MEWMA control chart”. In: *IFAC-PapersOnLine* 55.10 (2022). 10th IFAC Conference on Manufacturing Modelling, Management and Control MIM 2022, pp. 1533–1538. ISSN: 2405-8963.

[155] Thi Thuy Van Nguyen et al. “A novel transformer-based anomaly detection approach for ecg monitoring healthcare system”. In: *International Conference on Safety and Security in IoT*. Springer. 2023, pp. 111–129.

[156] Bahareh Nikpour and Narges Armanfard. “Spatio-temporal hard attention learning for skeleton-based activity recognition”. In: *Pattern Recognition* 139 (2023), p. 109428.

[157] William S Noble. “What is a support vector machine?” In: *Nature biotechnology* 24.12 (2006), pp. 1565–1567.

[158] Michael Nofer et al. "Blockchain". In: *Business & Information Systems Engineering* 59 (2017), pp. 183–187.

[159] Keiron O'shea and Ryan Nash. "An introduction to convolutional neural networks". In: *arXiv preprint arXiv:1511.08458* (2015).

[160] Aleksandr Ometov et al. "A survey on wearable technology: History, state-of-the-art and current challenges". In: *Computer Networks* 193 (2021), p. 108074.

[161] Francisco Javier Ordóñez and Daniel Roggen. "Deep Convolutional and LSTM Recurrent Neural Networks for Multimodal Wearable Activity Recognition". In: *Sensors* 16.1 (2016), 115:1–115:25. DOI: 10.3390/s16010115.

[162] Alexandros Pantelopoulos and Nikolaos G Bourbakis. "A survey on wearable sensor-based systems for health monitoring and prognosis". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 40.1 (2009), pp. 1–12.

[163] Francis Pascual, Sansi Yang, and Min Ye. "Monitoring Weibull quantiles by EWMA charts based on a pivotal quantity conditioned on ancillary statistics". In: *Quality and Reliability Engineering International* 33.1 (2017), pp. 103–119.

[164] E. J. Pauwels and O. Ambekar. "One Class Classification for Anomaly Detection: Support Vector Data Description Revisited". In: *Advances in Data Mining. Applications and Theoretical Aspects*. Ed. by Petra Perner. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 25–39.

[165] Vera Pawlowsky-Glahn, Juan José Egozcue, and Raimon Tolosana-Delgado. *Modeling and analysis of compositional data*. John Wiley & Sons, 2015.

[166] Ricardo Silva Peres et al. "Industrial artificial intelligence in industry 4.0-systematic review, challenges and outlook". In: *IEEE access* 8 (2020), pp. 220121–220139.

[167] Thinh Quy Duc Pham et al. "Fast and accurate prediction of temperature evolutions in additive manufacturing process using deep learning". In: *Journal of Intelligent Manufacturing* 34.4 (2023), pp. 1701–1719.

[168] Krishna Pillutla, Sham M Kakade, and Zaid Harchaoui. *Robust aggregation for federated learning*. arXiv preprint arXiv:1912.13445. 2019. DOI: 10.48550/arXiv.1912.13445.

[169] Utomo Pujianto, Aji Prasetya Wibawa, Muhammad Iqbal Akbar, et al. "K-nearest neighbor (k-NN) based missing data imputation". In: *2019 5th International Conference on Science in Information Technology (ICSITech)*. IEEE. 2019, pp. 83–88.

[170] P. Qiu and X. Xie. "Transparent Sequential Learning for Statistical Process Control of Serially Correlated Data". In: *Technometrics* just-accepted (2021), pp. 1–29.

[171] Anushree Raj. "Artificial Intelligence and Machine Learning applications in Smart Production". In: *Artificial Intelligence* 9.6 (2021).

[172] MS Subodh Raj, Sudhish N George, and Kiran Raja. "Leveraging spatio-temporal features using graph neural networks for human activity recognition". In: *Pattern Recognition* 150 (2024), p. 110301.

[173] Priyanka Rajendra and Shahram Latifi. "Prediction of diabetes using logistic regression and ensemble techniques". In: *Computer Methods and Programs in Biomedicine Update* 1 (2021), p. 100032.

[174] Hiba Ramadan et al. "Medical image registration in the era of Transformers: a recent review". In: *Informatics in Medicine Unlocked* (2024), p. 101540.

[175] Emmanuel Ramasso and Abhinav Saxena. "Performance Benchmarking and Analysis of Prognostic Methods for CMAPSS Datasets." In: *International Journal of Prognostics and Health Management* 5.2 (2014), pp. 1–15.

[176] Ali Raza et al. "Designing ecg monitoring healthcare system with federated transfer learning and explainable ai". In: *Knowledge-Based Systems* 236 (2022), p. 107763.

[177] Gregory C Reinsel. *Elements of multivariate time series analysis*. Springer Science & Business Media, 2003.

[178] Marion R Reynolds et al. "Charts with variable sampling intervals". In: *Technometrics* 30.2 (1988), pp. 181–192.

[179] Nicola Rieke et al. "The future of digital health with federated learning". In: *NPJ digital medicine* 3.1 (2020), p. 119.

[180] Kabrambam Rupabanta Singh. *Type 2 Diabetes Dataset*. 2024. DOI: 10.21227/xm4p-nx87. URL: https://dx.doi.org/10.21227/xm4p-nx87.

[181] Michael Rüßmann et al. "Industry 4.0: The future of productivity and growth in manufacturing industries". In: *Boston consulting group* 9.1 (2015), pp. 54–89.

[182] Hamed Sabahno, Amirhossein Amiri, and Philippe Castagliola. "Performance of the variable parameters t control chart in presence of measurement errors". In: *Journal of Testing and Evaluation* 47.1 (2018), pp. 480–497.

[183] Hamed Sabahno, Philippe Castagliola, and Amirhossein Amiri. "A variable parameters multivariate control chart for simultaneous monitoring of the process mean and variability with measurement errors". In: *Quality and Reliability Engineering International* 36.4 (2020), pp. 1161–1196.

[184] Michael S Saccucci, Raid W Amin, and James M Lucas. "Exponentially weighted moving average control schemes with variable sampling intervals". In: *Communications in Statistics-simulation and Computation* 21.3 (1992), pp. 627–657.

[185] Stephan R Sain. *The nature of statistical learning theory*. 1996.

[186] Mark Schwabacher. "A survey of data-driven prognostics". In: *Infotech@ Aerospace* (2005), p. 7002.

[187] Dhruv R Seshadri et al. "Wearable devices for sports: new integrated technologies allow coaches, physicians, and trainers to better understand the physical demands of athletes in real time". In: *IEEE pulse* 8.1 (2017), pp. 38–43.

[188] Ahmadreza Sezavar, Randa Atta, and Mohammed Ghanbari. "DCapsNet: Deep capsule network for human activity and gait recognition with smartphone sensors". In: *Pattern Recognition* 147 (2024), p. 110054.

[189] Ali Shafahi et al. "Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks". In: *Advances in neural information processing systems*. Vol. 31. Curran Associates, Inc., 2018, pp. 6103–6113. URL: https://proceedings.neurips.cc/paper/2018/hash/22722a343513ed45f14905eb07621686-Abstract.html.

[190] Ravid Shwartz-Ziv and Amitai Armon. "Tabular data: Deep learning is not all you need". In: *Information Fusion* 81 (2022), pp. 84–90.

[191] Deepti Sisodia and Dilip Singh Sisodia. "Prediction of diabetes using classification algorithms". In: *Procedia computer science* 132 (2018), pp. 1578–1585.

[192] A. Smola, B. Scholkopf, and K. Muller. "The connection between regularization operators and support vector kernels". In: *Neural Networks* (1998), pp. 637–649.

[193] Gowthami Somepalli et al. "Saint: Improved neural networks for tabular data via row attention and contrastive pre-training". In: *arXiv preprint arXiv:2106.01342* (2021).

[194] Zhi Song, Amitava Mukherjee, and Jiujun Zhang. "Some robust approaches based on copula for monitoring bivariate processes and component-wise assessment". In: *European Journal of Operational Research* 289.1 (2021), pp. 177–196.

[195] Zhi Song et al. "Optimizing joint location-scale monitoring–An adaptive distribution-free approach with minimal loss of information". In: *European Journal of Operational Research* 274.3 (2019), pp. 1019–1036.

[196] Konstantin Sozinov, Vladimir Vlassov, and Sarunas Girdzijauskas. "Human Activity Recognition Using Federated Learning". In: *Proceedings of the 8th IEEE International Conference on Big Data and Cloud Computing*. IEEE, 2018, pp. 1103–1111. DOI: 10.1109/BDCloud.2018.00164.

[197] Octavian Suciu et al. "When Does Machine Learning FAIL? Generalized Transferability for Evasion and Poisoning Attacks". In: *Proceedings of the 27th USENIX Security Symposium*. USENIX Association, 2018, pp. 1299–1316. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/suciu.

[198] R. Sun and F. Tsung. "A kernel-distance-based multivariate control chart using support vector methods". In: *International Journal of Production Research* 41.13 (2003), pp. 2975–2989.

[199] Tao Sun, Dongsheng Li, and Bao Wang. *Decentralized Federated Averaging*. arXiv:2104.11375 [cs.DC]. 2021. URL: https://doi.org/10.48550/arXiv.2104.11375.

[200] Kahou Tam et al. "FedCoop: Cooperative Federated Learning for Noisy Labels". In: *ECAI 2023*. IOS Press, 2023, pp. 2298–2306.

[201] A. Tang et al. "An assessment for the conditional performance of an support vector data description (SVDD)-based chart". In: *Quality and Reliability Engineering International* (2022), pp. 1–17.

[202] Fei Tao et al. "Data-driven smart manufacturing". In: *Journal of Manufacturing Systems* 48 (2018), pp. 157–169.

[203] Isfafuzzaman Tasin et al. "Diabetes prediction using machine learning and explainable AI techniques". In: *Healthcare Technology Letters* 10.1-2 (2023), pp. 1–10.

[204] D. M. J. Tax and R. P. W. Duin. "Support Vector Data Description". In: *Machine Learning* 54.1 (2004), pp. 45–66.

[205] David MJ Tax and Robert PW Duin. "Support vector data description". In: *Machine learning* 54 (2004), pp. 45–66.

[206] N Tho et al. "Transformer-Based Models for Predicting High-Risk Diabetes in Women using Tabular Data". In: *International Conference on Responsible Artificial Intelligence and Data Science*. Springer. 2024, pp. 83–109.

[207] K. P. Tran et al. "Monitoring compositional data using multivariate exponentially weighted moving average scheme". In: *Quality and Reliability Engineering International* 34.3 (2017), pp. 391–402.

[208] K.P. Tran, P. Castagliola, and G. Celano. "Monitoring the ratio of two normal variables using Run Rules type control charts". In: *International Journal of Production Research* ahead-of-print (2015), pp. 1–19.

[209] Kim Duc Tran et al. "One-sided Shewhart control charts for monitoring the ratio of two normal variables in short production runs". In: *Journal of Manufacturing Processes* 69 (2021), pp. 273–289.

[210] Kim Phuc Tran, Philippe Castagliola, and Giovanni Celano. "Monitoring the ratio of two normal variables using EWMA type control charts". In: *Quality and Reliability Engineering International* 32.5 (2016), pp. 1853–1869.

[211] Kim Phuc Tran, Philippe Castagliola, and Giovanni Celano. "The performance of the Shewhart-RZ control chart in the presence of measurement error". In: *International Journal of Production Research* 54.24 (2016), pp. 7504–7522.

[212] Kim Phuc Tran, Huu Du Nguyen, and Sébastien Thomassey. "Anomaly detection using long short term memory networks and its applications in supply chain management". In: *IFAC-PapersOnLine* 52.13 (2019), pp. 2408–2412. DOI: 10.1016/j.ifacol.2019.11.567.

[213] Phuong Hanh Tran et al. "Application of machine learning in statistical process control charts: A survey and perspective". In: *Control Charts and Machine Learning for Anomaly Detection in Manufacturing*. Springer, 2022, pp. 7–42.

[214] Ruey S Tsay. *An introduction to analysis of financial data with R*. John Wiley & Sons, 2014.

[215] Kwok L Tsui et al. "Prognostics and health management: A review on data driven approaches". In: *Mathematical Problems in Engineering* 2015 (2015).

[216] Dennis Ulmer, Lotta Meijerink, and Giovanni Cinà. "Trust issues: Uncertainty estimation does not enable reliable ood detection on medical tabular data". In: *Machine Learning for Health*. PMLR. 2020, pp. 341–354.

[217] Thi Thuy Van Nguyen et al. "SVDD control charts based on MEWMA technique for monitoring compositional data". In: *Computers & Industrial Engineering* 201 (2025), p. 110865.

[218] V. N. Vapnik. *Statistical Learning Theory*. John Wiley & Sons, 1998.

[219] Ashish Vaswani et al. "Attention Is All You Need". In: *Advances in Neural Information Processing Systems 30 (NIPS 2017)*. NeurIPS, 2017, pp. 5998–6008. URL: https://papers.nips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html.

[220] E. Verna et al. "Defects-per-unit control chart for assembled products based on defect prediction models". In: *The International Journal of Advanced Manufacturing Technology* (2022), pp. 1–12.

[221] Friedhelm Victor and Bianca Katharina Lüders. "Measuring ethereum-based erc20 token networks". In: *Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*. Springer. 2019, pp. 113–129.

[222] K VijiyaKumar et al. "Random forest algorithm for the prediction of diabetes". In: *2019 IEEE international conference on system, computation, automation and networking (ICSCAN)*. IEEE. 2019, pp. 1–5.

[223] Román Viveros and N Balakrishnan. "Interval estimation of parameters of life from progressively censored data". In: *Technometrics* 36.1 (1994), pp. 84–91.

[224] M. Vives-Mestres, J. Daunis-i-Estadella, and J. A. Martin-Fernandez. "Signal interpretation in Hotelling's T 2 control chart for compositional data". In: *IIE Transactions* 48.7 (2016), pp. 661–672.

[225] M. Vives-Mestres, J. Daunis-I-Estadella, and J.A. Martin-Fernandez. "Individual T^2 Control Chart for Compositional Data". In: *Journal of Quality Technology* 46.2 (2014), pp. 127–139.

[226] M. Vives-Mestres, J. Daunis-I-Estadella, and J.A. Martin-Fernandez. "Out-of-Control Signals in Three-Part Compositional T^2 Control Chart". In: *Quality and Reliability Engineering International* 30.3 (2014), pp. 337–346.

[227] Simon Vollert and Andreas Theissler. "Challenges of machine learning-based RUL prognosis: A review on NASA's C-MAPSS data set". In: *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE. 2021, pp. 1–8.

[228] Jing Wang, Mohammad Tabrez Quasim, and Bo Yi. "Privacy-Preserving Heterogeneous Multi-Modal Sensor Data Fusion via Federated Learning for Smart Healthcare". In: *Information Fusion* (2025), p. 103084.

[229] Jiujian Wang et al. "Remaining useful life estimation in prognostics using deep bidirectional LSTM neural network". In: *2018 Prognostics and System Health Management Conference (PHM-Chongqing)*. IEEE. 2018, pp. 1037–1042.

[230] Kunfeng Wang et al. "Generative adversarial networks: introduction and outlook". In: *IEEE/CAA Journal of Automatica Sinica* 4.4 (2017), pp. 588–598.

[231] Fu-Kwun Wang, Berihun Bizuneh, and Xiao-Bin Cheng. "EWMA chart based on Bayes-conditional pivotal quantity for Weibull percentiles under complete data and type-II censoring". In: *Quality and Reliability Engineering International* 34.5 (2018), pp. 707–717.

[232] Maonan Wang et al. "An Explainable Machine Learning Framework for Intrusion Detection Systems". In: *IEEE Access* 8 (2020), pp. 73127–73141. DOI: 10.1109/ACCESS.2020.2988359.

[233] Qin Wang et al. *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*. 2021. arXiv: 2105.07447 [cs.CR].

[234] Sanford Weisberg. *Applied linear regression*. Vol. 528. John Wiley & Sons, 2005.

[235] XUCFANXL Wencui. "Research of tool wear based on radical basic function network". In: *Proceedings of the International MultiConference of Engineers and Computer Scientists*. Vol. 1. Citeseer. 2009.

[236] Thomas Wolf et al. "Transformers: State-of-the-Art Natural Language Processing". In: *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations*. ACL, 2020, pp. 38–45. DOI: 10.18653/v1/2020.emnlp-demos.6.

[237] William H Woodall and Douglas C Montgomery. "Some current directions in the theory and application of statistical process monitoring". In: *Journal of Quality Technology* 46.1 (2014), pp. 78–94.

[238] Min Wu and Jake Luo. "Wearable Technology Applications in Healthcare: A Literature Review". In: *Online Journal of Nursing Informatics* 23.3 (2019). URL: https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review.

[239] Geming Xia et al. "Poisoning Attacks in Federated Learning: A Survey". In: *IEEE Access* 11 (2023), pp. 10708–10722. DOI: 10.1109/ACCESS.2023.3238823.

[240] Qi Xia et al. "FABA: An Algorithm for Fast Aggregation against Byzantine Attacks in Distributed Neural Networks". In: *IJCAI* (2019). DOI: 10.24963/ijcai.2019/670.

[241] Yun-Peng Xiao et al. "A survey on deep geometry learning: From a representation perspective". In: *Computational Visual Media* 6 (2020), pp. 113–133.

[242] Cong Xie, Sanmi Koyejo, and Indranil Gupta. "Zeno: Distributed stochastic gradient descent with suspicion-based fault-tolerance". In: *Proceedings of the 36th International Conference on Machine Learning*. PMLR. 2019, pp. 6893–6901.

[243] Junfeng Xie et al. "A survey of blockchain technology applied to smart cities: Research issues and challenges". In: *IEEE communications surveys & tutorials* 21.3 (2019), pp. 2794–2830.

[244] Chang Xu et al. "TDFL: Truth Discovery Based Byzantine Robust Federated Learning". In: *IEEE Transactions on Parallel and Distributed Systems* 33.12 (2022), pp. 4835–4848. DOI: 10.1109/TPDS.2022.3205714.

[245] Dong Xu et al. "An improved data anomaly detection method based on isolation forest". In: *2017 10th international symposium on computational intelligence and design (ISCID)*. Vol. 2. IEEE. 2017, pp. 287–291.

[246] Jie Xu et al. "Federated Learning for Healthcare Informatics". In: *Journal of Healthcare Informatics Research* 5.1 (2021), pp. 1–19. DOI: 10.1007/s41666-020-00082-4.

[247] H. Yan, K. Paynabar, and J. Shi. "Real-time monitoring of high-dimensional functional data streams via spatio-temporal smooth sparse decomposition". In: *Technometrics* 60.2 (2018), pp. 181–197.

[248] Xi Yang et al. "Clinical concept extraction using transformers". In: *Journal of the American Medical Informatics Association* 27.12 (2020), pp. 1935–1942. DOI: 10.1093/jamia/ocaa189.

[249] Shuochao Yao et al. "DeepSense: a Unified Deep Learning Framework for Time-Series Mobile Sensing Data Processing". In: *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conference Committee (IW3), 2017, pp. 351–360. DOI: 10.1145/3038912.3052577.

[250] A. Yeganeh and A. Shadman. "Using evolutionary artificial neural networks in monitoring binary and polytomous logistic profiles". In: *Journal of Manufacturing Systems* 61 (2021), pp. 546–561.

[251] Hongxu Yin et al. "Smart healthcare". In: *Foundations and Trends® in Electronic Design Automation* 12.4 (2018), pp. 401–466.

[252] F.S. Zaidi et al. "Analyzing abnormal pattern of hotelling T2 control chart for compositional data using artificial neural networks". In: *Computers & Industrial Engineering* 180 (2023), p. 109254.

[253] F.S. Zaidi et al. "Monitoring autocorrelated compositional data vectors using an enhanced residuals Hotelling T2 control chart". In: *Computers & Industrial Engineering* 181 (2023), p. 109280.

[254] F.S. Zaidi et al. "Performance of the MEWMA-CoDa control chart in the presence of measurement errors". In: *Quality and Reliability Engineering International* 36.7 (2020), pp. 2411–2440.

[255] FS Zaidi et al. "Performance of the hotelling T 2 control chart for compositional data in the presence of measurement errors". In: *Journal of Applied Statistics* 46.14 (2019), pp. 2583–2602.

[256] Chen Zhang et al. "A survey on federated learning". In: *Knowledge-Based Systems* 216 (2021), 106775:1–106775:11. URL: https://doi.org/10.1016/j.knosys.2021.106775.

[257] Chen Zhang et al. "A survey on federated learning". In: *Knowledge-Based Systems* 216 (2021), p. 106775.

[258] Shichao Zhang. "Nearest neighbor selection for iteratively kNN imputation". In: *Journal of Systems and Software* 85.11 (2012), pp. 2541–2552.

[259] Ye Zhang et al. "IF-ConvTransformer: A framework for human activity recognition using IMU fusion and ConvTransformer". In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6.2 (2022), pp. 1–26. DOI: 10.1145/3534584.

[260] Z. Zhang and X. Deng. "Anomaly detection using improved deep SVDD model with data structure preservation". In: *Pattern Recognition Letters* 148 (2021), pp. 1–6.

[261] Bo Zhao et al. "FedInv: Byzantine-robust Federated Learning by Inversing Local Model Updates". In: *Proceedings of the AAAI Conference on Artificial Intelligence* 36.8 (2022), pp. 9171–9179. URL: https://doi.org/10.1609/aaai.v36i8.20903.

[262] Shuai Zheng et al. "Long short-term memory network for remaining useful life estimation". In: *2017 IEEE international conference on prognostics and health management (ICPHM)*. IEEE. 2017, pp. 88–95.

[263] Ray Y Zhong et al. "Intelligent manufacturing in the context of industry 4.0: a review". In: *Engineering* 3.5 (2017), pp. 616–630.

[264] Keliang Zhou, Taigang Liu, and Lifeng Zhou. "Industry 4.0: Towards future industrial opportunities and challenges". In: *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)*. IEEE. 2015, pp. 2147–2152.

[265] ZX Zhou et al. "Applying deep learning and wearable devices for educational data analytics". In: *2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI)*. IEEE. 2019, pp. 871–878.

[266] Yuxuan Zhu et al. "FedTrans: Efficient Federated Learning via Multi-Model Transformation". In: *Proceedings of Machine Learning and Systems* 6 (2024), pp. 395–407.

[267] VINCENT et al. "Stacked denoising autoencoders: learning useful representations in a deep network with a local denoising criterion". In: *Journal of machine learning research* 11.12 (2010), pp. 3371–3408.