Privacy-Preserving Edge-AI Framework for Secure EV Battery Data Management and Analysis

Supervisor:

Abdelghani Bekrar: Associate professor, HDR at université Polytechnique de Hauts-de-France and LAMIH laboratory

Co-supervisors:

Youcef Imine : Associate professor at université Polytechnique de Hauts-de-France and LAMIH laboratory

Hamza Ouarnoughi: Associate professor at INSA Hauts-de-France and LAMIH laboratory

IKKEN BENALI Sonia: Teacher-researcher at CESI LINEACT

Introduction and Context

As the electric vehicle (EV) market continues to grow exponentially, managing the lifecycle of EV batteries has become an urgent priority. By 2030, the global demand for EV batteries is expected to increase by 20% annually, reaching a market value of up to $410 billion [1]. However, this rapid growth presents significant challenges in terms of battery longevity, recycling, and traceability. Battery Longevity and Remaining Useful Life (RUL) is a critical factor in the total cost of ownership of an EV. Currently, the average RUL of an EV battery is estimated to be between 8 to 12 years, depending on usage patterns, charging cycles, and environmental conditions. However, studies have shown that poor driving behavior and inefficient charging schedules can reduce this lifespan by up to 20-30% [2]. This results in premature battery failure, increasing costs for both consumers and manufacturers and exacerbating environmental concerns related to battery disposal.

Moreover, recycling of EV batteries in Europe remains limited, with only about 5% of lithium-ion batteries being recycled at the end of their life. This poses a significant challenge, as EV battery production relies heavily on scarce resources such as lithium, cobalt, and nickel. According to the European Environment Agency, demand for these raw materials is expected to increase by 20–25 times by 2030, highlighting the urgent need for efficient recycling practices [1]. The European Union's Battery Directive establishes strict guidelines for ensuring traceability across the entire battery lifecycle. However, current solutions fail to provide adequate traceability, particularly during the recycling and reuse phases. Recognizing this gap, the EU has emphasized the importance of transparent and tamper-proof tracking of battery data to achieve its sustainability goals. The lack of secure traceability consequently increases the risk of non-compliance, reduces recycling efficiency, and limits opportunities for battery reuse due to insufficient information on battery health and performance at the end of their first life.

Edge computing can help address these challenges by enabling the processing of large volumes of data closer to their source of generation, typically at or near the network edge—well-suited to the nature and constraints of EV battery data management. This distributed architecture reduces latency, improves response times, and enhances efficiency in data analysis, making it a promising foundation for EV battery data management and exploitation systems. However, several challenges remain, including the efficient design of resource allocation and model adaptation mechanisms for highly dynamic and heterogeneous edge infrastructures, as well as secure data aggregation across distributed nodes.

Research Hypothesis and Objectives

Given the current state of battery longevity, low recycling rates, and insufficient traceability, this thesis aims to provide an Edge-AI based framework for EV battery data management. This Framework will allow in one hand to enable accurate assessment of battery state and remaining useful life time at the edge level (vehicles) and to securely trace its status all over the network. Moreover, as both data related to batteries and its state prediction may reveal private information on drivers behavior and habits, privacy concerns need to be considered at each step of the proposed approaches. The outcome of this thesis coupled with efficient charging scheduling strategies will potentially extend battery life by 15-20%.

This thesis will be conducted within the framework of the **ANR project BATTL-EU** and hosted at the computer science department of the LAMIH laboratory. The research work will follow the plan outlined below:

- State of the art of existing solutions and tools: This first period will be dedicated to the study of the literature where both the scientific contributions and the technical tools will be analyzed;

- Study of security issues and challenges: In parallel a work of identification and categorization of specific security issues facing the battery data management (aggregation and tracking) and its exploitation by AI-based approaches in heterogeneous Edge computing architecture;

- Proposal and implementation of a secure AI-based framework for battery data management in a large-scale and heterogeneous edge computing architecture. The proposed solution and its security mechanisms have to respond to the scientific problems identified in the literature and allow at the same time to achieve a high performance (efficiency given equipment constraints, optimal communication cost, low overhead, etc..);

- Integration, evaluation, and validation of the proposed solutions: this will involve developing use cases for the integration of the proposed Framework. In addition to that, this step will allow the evaluation of performance and the verification of the expected properties (e.g., robustness against attacks, speed, and energy consumption of all entities involved).

- Dissemination, writing, and defense: the last six months will be dedicated to finalizing the latest scientific and technical contributions and to writing the thesis manuscript which will give a complete view of the scientific questions addressed, the up-to-date state-of-the-art, the proposed solutions, and their evaluation.

Prerequisites

- Master's degree or equivalent in Computer Science
- Good background in computer architecture and design.
- Good background in cyber security.
- Experience in programming languages (Python, C/C++) and scripting (Bash, Shell).
- Experience in GNU/Linux-based operating systems
- Experience in Deep Learning frameworks (Pytorch/Tensorflow/MXNet)
- Experience in embedded systems (Raspberry Pi, Microcontrollers, Edge GPU/ TPU)

Contact:

abdelghani.bekrar@uphf.fr
youcef.imine@uphf.fr
hamza.ouarnoughi@uphf.fr
sikken@cesi.fr

Bibliography:

[1] McKinsey & Company. (2023). Battery 2030: Resilient, Sustainable, and Circular. McKinsey & Company. Retrieved from : Link
[2] Tasnim, M. N., Akter, S., Shahjalal, M., Shams, T., Davari, P., & Iqbal, A. (2023). A critical review of the effect of light duty electric vehicle charging on the power grid. Energy Reports, 10, 4126-4147.
[3] Global Battery Alliance. (2023). Battery Passport. Retrieved from Link m https://www.globalbattery.org/battery-passport/.
[4] Gu, X., Ieromonachou, P., Zhou, L., & Tseng, M. (2018). Developing pricing strategy to optimise total profits in an electric vehicle battery closed loop supply chain. Journal of Cleaner Production, 203, 376-385. https://doi.org/10.1016/j.jclepro.2018.08.209,
*[5] **Imine, Youcef,** Ahmed Lounis, and Abdelmadjid Bouabdallah. "An accountable privacy-preserving scheme for public information sharing systems." Computers & Security 93 (2020): 101786. https://doi.org/10.1016/j.cose.2020.101786*
*[6] Kouicem, D. E., **Imine, Y.**, Bouabdallah, A., & Lakhlef, H. (2020). Decentralized blockchain-based trust management protocol for the Internet of Things. IEEE Transactions on Dependable and Secure Computing, 19(2), 1292-1306. 10.1109/TDSC.2020.3003232*
*[7] **Bekrar** A, Ait El Cadi A, Todosijevic R, Sarkis J. Digitalizing the Closing-of-the-Loop for Supply Chains: A Transportation and Blockchain Perspective. Sustainability. 2021; 13(5):2895.*
*[8] Rath J., **Sentouh** C., Popieul J.-C. (2019). Personalized Lane Keeping Assist Strategy: Adaptation to Driving Style. IET Control Theory & Applications, Volume 13, Issue 1, pp. 106-115, ISSN 1751-8644. [DOI=10.1049/iet-cta.2018.5941].*
*[9] **Ikken, S.**, and Bitaqa, D. (2024, December). "Split-Federated Reinforcement Learning for IoMT Data and Task Management in Edge-Fog-Cloud Infrastructure." 2024 IEEE Conference on Computer Applications (ICCA). https://doi.org/10.1109/ICCA62237.2024.10927980*
*[10] Bouaziz, S., Benmeziane, H., **Imine, Y.**, Hamdad, L., Niar, S., & **Ouarnoughi,** H. (2023, November). FLASH-RL: Federated Learning Addressing System and Static Heterogeneity using Reinforcement Learning. In 2023 IEEE 41st International Conference on Computer Design (ICCD) (pp. 444-447). IEEE. 10.1109/ICCD58817.2023.00074*
*[11] Benmeziane, H., El Maghraoui, K., **Ouarnoughi**, H., & Niar, S. (2024). Grassroots operator search for model edge adaptation using mathematical search space. Future Generation Computer Systems, 157, 29-40. https://doi.org/10.1016/j.future.2024.03.029*