ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	Sima Sinaei
Nationality	Iranian
Name of the *Host Organisation*	RISE Research Institute of Sweden
First Name / family name of the *Scientific Coordinator*	Dr. Mehrdad Saadatmand
Period of the fellowship	01/03/2021 to 01/03/2022

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

During my fellowship, I worked in the division of Digital System at RISE Research Institutes of Sweden. I got involved in three research projects called IVVES (https://ivves.eu/), Dais (https://dais-project.eu/), and AutoDeep.

IVVES (ITEA3): The purpose of this project is to develop tools and techniques for the verification and validation of evolving industrial systems. Rapid and continuous changes and embedding of Artificial Intelligence services are the key features of the systems targeted by the project. IVVES includes several use cases provided by industrial partners. I had the chance to work on one of the industrial use cases to detect anomalies. For this purpose, DeepAD tool has been developed which is based on combining Autoencoder and LSTM techniques that can detect anomalies in multivariate time-series data. This tool reports subsequence that violates the constraints as anomalies. This approach can model non-linear long-term sequential dependencies among the data records in univariate/multivariate time series, which makes them more practical for real-world applications.

DAIS (ECSEL JU): This project aims at providing solutions for distributed artificial intelligent systems. It focuses on delivering the hardware and software that is needed to run industrial-grade AI on different types of network topologies. It demonstrates how known AI challenges, from different functional areas, are met by this pan-European effort. In this project, my research has been focused on communication frameworks, and in particular on federated learning systems as a promising solution for addressing the issues of communication costs, data privacy, and legalization. Federated learning ensures the privacy of data during the training process. In the Dais project, I've been working on federated learning challenges such as communication, data privacy, and data heterogeneity in two different application domains: 1) Driver fatigue detection systems in the car and 2) smart TV movies recommendation.

AutoDeep (National Vinnova project): The project goal is to design performance-efficient DNNs suitable for deployment on embedded resources-limited computing platforms while enhancing the robustness of DNN models. As a solution, we investigated how to optimize compactness and robustness to adversarial attacks of neural network architectures while maintaining the accuracy using a multi-objective neural architecture search. We proposed the use of previously generated adversarial examples as an objective to evaluate the robustness of our models in addition to the number of floating-point operations to assess model complexity i.e., compactness.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

1. "Artificial Intelligence Enabled Distributed Edge Computing for Internet of Things", published in ERCIM News.
2. "FaCT-LSTM: Fast and Compact Ternary Architecture for LSTM Recurrent Neural Networks", *Accepted in IEEE transaction on Design and Test*.
3. "ELC-ECG: Efficient LSTM Cell for ECG Classification based on Quantized Architecture", *Accepted in ISCAS 2021 (Rank A).*
4. "RoCo-NAS: Robust and Compact Neural Architecture Search", *accepted in IJCNN 2021 (Rank A).*
5. "MONAS: Finding Compressed and Resilient Architectures against Adversarial Examples using Multi-Objective Neural Architecture Search" *submitted to IEEET Transactions on Emerging Topics in Computing.*
6. "Multi-Level Binarized LSTM-Based Classification for Healthcare and Rehabilitation Wearable Devices", *submitted to ACM Transaction on Embedded Computing Systems (TECS).*
7. "Multi-Objective Design Space Exploration of Recurrent Neural Network Architecture" – (Under preparation)
8. "A Survey on Privacy and Security aspects of Federated Learning" - (Under preparation)

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

1. International Joint Conference on Neural Networks (IJCNN) - 18-22 July 2021 – Virtual.
2. International Symposium on Circuits and Systems (ISCAS) - 22-28 May 2021 Virtual.
3. 17th International Summer School on Advanced Computer Architecture and Compilation for High-performance Embedded Systems, 12-18 Sep 2021, Fiuggi, Italy.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

For the research exchange program, I planned to visit NTNU Research Institutes in the winter (2021), but due to the covid-19 situation, the opportunity to do a research exchange program was not as readily available and I was remotely in contact with a few researchers in NTNU. I had virtual discussions with Dr. Magnus Jahre's research team on their ongoing projects. In addition, we had numerous virtual meetings on one of the ongoing projects (Dais) with researchers at Fraunhofer while sharing scientific experiences and ideas.