

I. IDENTIFICATION DATA

Thesis title:	Decentralized Federated Learning for Network Security
Author's name:	Pavel Janata
Type of thesis :	Diploma Thesis
Faculty/Institute:	Faculty of Electrical Engineering
Department:	Department of Computer Science
Thesis reviewer:	Sebastian Garcia
Reviewer's department:	Department of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	A- very demanding
<i>How demanding was the assigned project?</i>	
The assignment was very demanding since federated learning was not widely used for network security, which made it harder to understand the impact. Also since the work was done in a real federated environment in the network, there was a component to make it real that added more complexity.	
Fulfilment of assignment	A - excellent
<i>How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.</i>	
The thesis completely fulfilled the assigned task and the goals have been achieved. There were no incomplete tasks.	
Activity and independence when creating final thesis	A - excellent
<i>Assess whether the student had a positive approach, whether the time limits were met, whether the conception was regularly consulted and whether the student was well prepared for the consultations. Assess the student's ability to work independently.</i>	
The student had a positive approach, when limits were met he consulted regularly and was well prepared for consultations.	
Technical level	A - excellent
<i>Is the thesis technically sound? How well did the student employ expertise in his/her field of study? Does the student explain clearly what he/she has done?</i>	
The technical level was very good, since Pavel implemented and experimented with several machine learning models and neural network architectures to solve the problem, consulting the literature and proposing new ideas. In addition, there was a good evaluation and comparison to understand the limits and constraints of the different approaches.	
Formal level and language level, scope of thesis	A- excellent
<i>Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?</i>	
The language is good, it is organized in a good logical way and sufficiently extensive. It is clear and it can be understood.	
Selection of sources, citation correctness	A - excellent
<i>Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?</i>	
The sources were correctly selected and cited, covering pertinent previous work. The original work of the student was clearly distinguished from previous work.	
Additional commentary and evaluation (optional)	

Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.

The thesis has a high quality of work and research. The student showed his knowledge of the domain, with a strong connection with network security. The solution is highly impactful for the network security research community.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

Summarize your opinion on the thesis and explain your final grading.

The student successfully approached the hard task of researching and implementing a real federated learning system for network detection with many connected clients. He used a novel dataset prepared for federated learning and researched machine learning algorithms that produce competitive results while preserving the privacy of the clients. His work in the novel neural network architectures and comparisons was good and enough to show the promise of federated learning for network cybersecurity.

The grade that I award for the thesis is **A**



Date: **February 3rd, 2023**

Signature: