Bachelor Thesis Supervisor's Expert Opinion

Student:	Mashoko Tawanda Nduna
Student Number:	E22838
Title of Bachelor Thesis:	Cyber attack detection in IoT networks using deep learning
Aim of the Thesis:	To introduce methods for cyber attack detection in IoT networks, propose a detection system using deep learning, pre-process benchmark datasets, and validate the proposed detection system using the datasets.
Thesis Supervisor:	prof. Ing. Petr Hájek, Ph.D.
Study Programme:	Informatics and System Engineering
Academic Year:	2024/2025

Difficulty of the Topic

	Excellent	Very good	Satisfactory	Unsatisfactory	Cannot be evaluated
Theoretical knowledge	☐	☒	☐	☐	☐
Input data and their processing	☐	☒	☐	☐	☐
Methods used	☒	☐	☐	☐	☐

Thesis Evaluation Criteria

	Excellent	Very good	Satisfactory	Unsatisfactory	Cannot be evaluated
Degree of achievement of the aim of the thesis	☐	☒	☐	☐	☐
Original attitude to the topic processing	☐	☒	☐	☐	☐
Adequacy of the methods used	☐	☒	☐	☐	☐
Depth of analysis (relative to topic)	☐	☒	☐	☐	☐
Logical structure of the thesis and scope	☐	☒	☐	☐	☐
Working with Czech and foreign literature including citations	☐	☒	☐	☐	☐
Formal arrangement of the thesis (text, charts, tables)	☐	☒	☐	☐	☐
Language level (style, grammar, terminology)	☐	☒	☐	☐	☐

Applicability of the Results of the Thesis

	High	Medium	Low	Cannot be evaluated
For theory	☐	☐	☒	☐
For practice	☐	☒	☐	☐

Other Comments on the Thesis

This bachelor thesis is a well-structured work that addresses the timely and relevant problem of cyber-attack detection in IoT networks using deep learning. The student successfully applies Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models to the CICIoT2023 dataset, showing strong classification performance across several attack types. The work is original in combining flow-based and packet-based features to improve detection accuracy, and it compares deep learning approaches against traditional machine learning baselines. The methodological design is appropriate and aligns with the stated objectives. The student demonstrates a solid understanding of both the dataset and the algorithms, providing detailed descriptions of pre-processing steps, model architectures, and evaluation metrics. The comparison with Decision Trees, Logistic Regression, and Naïve Bayes strengthens the argument for using deep learning in IoT intrusion detection. The thesis is logically organized, with a smooth flow between the literature review, methodology, experiments, and discussion. The writing is generally clear, and the use of references is thorough. Figures and tables are used effectively to illustrate results, particularly in highlighting the differences in CNN and LSTM performance. However, there are some limitations that reduce the overall impact of the work. First, while class imbalance is acknowledged, the mitigation strategies could be explored in greater depth. Second, the discussion of model interpretability is limited. The work could also benefit from a more concrete proposal for integrating the IDS into real IoT networks. Finally, a few sections contain repetitive phrasing and minor inconsistencies, and some figures could be more clearly referenced in the text.

Comments on the Outputs from the Theses System

Assessed – not plagiarized, the highest degree of compliance – 5%.

Questions and Suggestions for Defence

1. Deep learning models detect most cyber attacks with high accuracy. However, some attacks have proven to be resistant to detection. Try to explain these results.

2. What are the implications of further IoT expansion for cyber-attack detection?

Final Evaluation

I **recommend** the thesis for the defence.
I propose to grade this Bachelor thesis as follows: **C**

In Pardubice 8.8.2025

Signature .....