Master's Thesis Supervisor's Expert Opinion

Student:	Kebede Zeru Kifle
Student Number:	E21821
Title of Master's Thesis:	Detection of IoT Cyberattacks in Smart Cities using Deep Neural Networks
Aim of the Thesis:	To summarize existing approaches to detecting IoT cyber attacks, propose a DNN-based model for detecting IoT cyber attacks, validate the model using datasets relevant to smart cities, and discuss implications of the results for smart cities.
Thesis Supervisor:	prof. Ing. Petr Hájek, Ph.D.
Study Programme:	Informatics and System Engineering
Academic Year:	2022/2023

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

Detecting IoT cyber attacks in smart cities has become increasingly important with the rapid adoption of smart city technologies. Accurate detection of IoT cyber attacks is important not only to protect critical infrastructure, but also to ensure public safety and privacy. Therefore, the detection of IoT cyber attacks has become a hot topic in current cybersecurity research. The author provides sufficient theoretical background by introducing the smart city architecture and presenting the problems related to IoT cyber attacks. There are several challenging problems in this area. First, the IoT environment is highly dynamic and new attack techniques are constantly emerging. Second, scalable detection systems are required due to the large amount of data. Deep neural networks are particularly effective in learning from such data, while automatically capturing higher order features from the data. Therefore, the proposed methodology is well chosen and the author elaborates the deep learning models in sufficient detail. Similarly, the datasets are large enough and, unlike most existing approaches, the author uses the whole datasets to improve the detection performance. All experiments are well documented and therefore easy to validate. Obviously, the author has done a lot of experiments, but their settings should be better justified. The results are presented clearly. In particular, the results of this thesis outperform those reported in previous research, and the author also shows the performance for different types of attacks, which increases the credibility of the proposed system. Overall, the thesis is well developed, but its theoretical and practical implications should be better highlighted.

Comments on the Outputs from the Theses System

Highest degree of compliance: 6%, similarity assessment: the thesis is not plagiarized

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 Master's thesis as follows: **B**

In Pardubice 15.5.2023

Signature .....