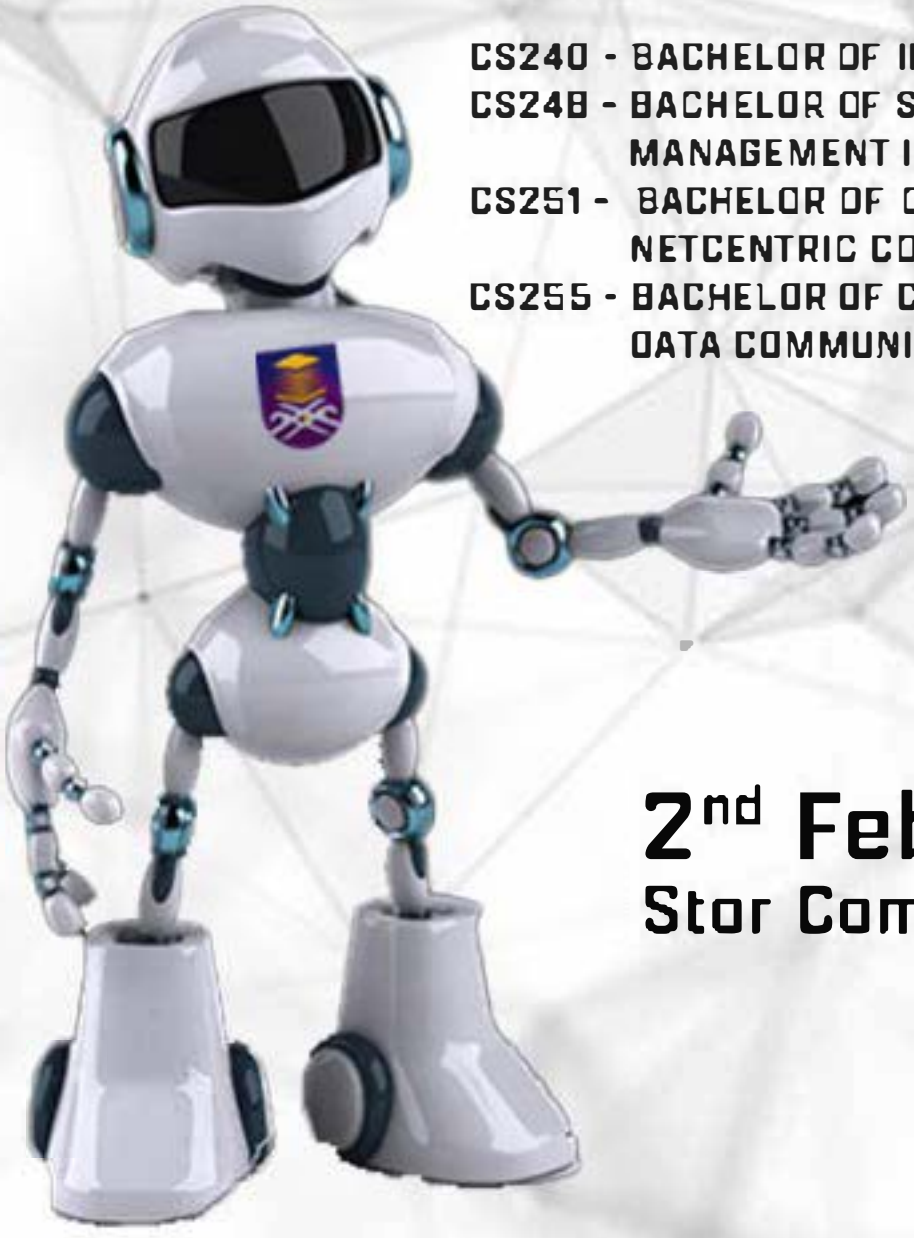
UNIVERSITI TEKNOLOGI MARA
Perlis Branch
Arau Campus

RESEARCH EXHIBITION IN MATHEMATICS & COMPUTER SCIENCES

REMACS 5.0



CS240 - BACHELOR OF INFORMATION TECHNOLOGY (HONS.)
CS248 - BACHELOR OF SCIENCES (HONS.)
MANAGEMENT IN MATHEMATICS
CS251 - BACHELOR OF COMPUTER SCIENCE (HONS)
NETCENTRIC COMPUTING
CS255 - BACHELOR OF COMPUTER SCIENCE (HONS)
DATA COMMUNICATION & NETWORKING

2nd Februory 2023

Stor Complex, UiTM Perlis

Organized by:
College of Computing, Informatics and Media
Universiti Teknologi MARA Perlis Branch

Research Exhibition in Mathematics and Computer Sciences (REMACS 5.0)

Research Exhibition in Mathematics and Computer Sciences (REMACS 5.0)

Editors
Rafiza Ruslan, Mohamad Najib Mohamad Fadzil, Noorfaizalfaird Mohd Nor, Mohammad Hafiz bin Ismail

e ISBN: 978-629-97934-0-3

Perpustakaan Negara Malaysia

Published by

MOHAMMAD HAFIZ BIN ISMAIL
Universiti Teknologi MARA
02600 Arau, Perlis
Tel: +604 988 2028

https://fskmperlis.uitm.edu.my/remacs50/

CONTENTS

Preface

It is with great pleasure that we present this extended abstract book, titled "The 5th Research Exhibition in Mathematics and Computer Sciences (REMACS 5.0)". This book is a collection of research work in the fields of Computer Science and Mathematics, contributed by the final year students from Universiti Teknologi MARA, Perlis Branch. The aim of this book is to showcase the diversity and depth of research in these two interrelated fields.

Mathematics and Computer Science are two fields that have seen tremendous growth and advancement in recent years. With the rise of new technologies and the increasing demand for data-driven solutions, researchers in these fields have been working hard to develop new theories, algorithms, and models that can help solve some of the most pressing problems of our time. This book is a testament to their hard work and dedication.

The abstracts in this book cover a wide range of topics, including algebra, analysis, logic, computer architecture, algorithms, artificial intelligence, machine learning, computer network, netcentric computing and many more. The work presented here is both theoretical and practical, and has the potential to impact many areas of society, from finance and healthcare to education and security.

We hope that this book will serve as a valuable resource for future students in the fields of Mathematics and Computer Science. We also hope that it will inspire more students to pursue innovative and groundbreaking research in these two fields. Finally, we would like to express our gratitude to all the contributors for their hard work and dedication, without which this book would not have been possible.

COMMITTEE

PATRON

- PROF. MADYA Ts. DR SHUKOR SANIM MOHD FAUZI

ADVISORS

- Ts. DR SITI ZULAIHA AHMAD
- PN SUZANAWATI ABU HASAN
- PN NORA YANTI CHE JAN

PROGRAMME DIRECTOR

- EN MUHAMAD ARIF HASHIM

PROGRAMME DEPUTY DIRECTOR

- DR NURIZATUL SYARFINAS AHMAD BAKHTIAR

SECRETARY

- PN SITI SARAH RASELI
- CIK SITI SARAH MD ILYAS

TRESURER

- PN NORPAH MAHAT

PROMOTION

- PROF. MADYA DR RIZAUDDIN SAIAN
- DR RUZITA AHMAD
- PN NORWAZIAH MAHMUD

EXHIBITION

- DR AZNOORA OSMAN
- EN MOHAMAD HAFIZ ISMAIL
- EN ROS SYAMSUL HAMID
- PN RAIHANA ZAINORDIN
- DR HUDA ZUHRAH AB.HALIM

REGISTRATION COORDINATORS

- Ts. DR ABIDAH HJ MAT TAIB
- DR NUR FATIHAH FAUZI
- PN NOR HAYATI SHAFII
- PN WAN NURSHAZELIN WAN SHAHIDAN

TECHNICAL & LOGISTIC

- EN MOHD FARIS MOHD FUZI
- EN IMAN HAZWAM ABD HALIM
- EN MOHD FAZRIL IZHAR MOHD IDRIS
- EN MOHD HASBULLAH MOHD RAZALI

EVENT MGT & PROTOCOL

- PN ROMIZA MD NOR
- EN ABDUL HAPES MOHAMMED
- PN DIANA SIRMAYUNIE MOHD NASIR

CERTIFICATE

- EN ALIF FAISAL IBRAHIM
- EN HALIMI AB HALIM

PROGRAMME BOOK

- PN RAFIZA RUSLAN
- EN MOHAMAD NAJIB MOHAMAD FADZIL
- Ts. NOORFAIZALFARID MOHD NOOR

BANQUET

- CIK KU AZLINA KU AKIL
- DR NUR IZZATI KHAIRUDIN

RESEARCH EXHIBITION IN MATHEMATICS & COMPUTER SCIENCES
REMACS 5.0

EVENT SCHEDULE

8:00 – 8:30 am
•Registration

8:00 am – 12:00 pm
•FYP Project Presentation

12:00 - 2:00pm
•Lunch Break

2:15 – 2:35 pm
•National & Wawasan Setia Anthems
•Doa Recitation

2:35 – 2:45 pm
•Welcoming Address by Director of REMACS 5.0

2:45 – 2:55 pm
•Officiating & Closing Remarks from Rector of UiTM Perlis

2:55 – 3:00 pm
•REMACS 5.0 Montage

3:00 – 4:00 pm
•Awarding of Winners:
•Best Poster
•Best Project Award

•Photo Session

•End of Ceremony

Dress Code: Formal / Corporate

List of Papers

RESEARCH EXHIBITION IN MATHEMATICS & COMPUTER SCIENCES

REMACS 5.0

EXTENDED ABSTRACTS

MALWARE DETECTION IN WINDOWS USING DEEP LEARNING CLASSIFICATION APPROACH

Aishah Anuar and Mohd Faris Mohd Fuzi
College of Computing, Informatics and Media, Universiti Teknologi MARA Perlis Branch, Malaysia

Abstract

Cybercrime has become a major threat to every individual, business, and national security system in the modern world. Deep learning has been implemented in numerous safety-focused environments for the purpose of protecting applications as a result of its rapid evolution and notable success in a wide range of applications. Due to the precision of the data and the capacity to train a huge number of data, deep learning has become popular in response to the current high demand. In terms of accomplishing the project's objective, the project's success was determined by its outputs. Using the Metric Formula Definition Accuracy, the performance of CNN and RNN malware detection models in Windows has been tested. According to the afore mentioned models, CNN is doing better, providing an accuracy of 97.5 percent in detecting malware, whereas RNN provides an accuracy of 88.5 percent and respectively. This study evaluated the performance accuracy between the CNN and RNN architecture models.

***Keywords**: Deep learning, CNN, RNN, accuracy,*

1. Introduction

According to recent statistics by the AV-Test Institute, over 17 million new malware variants are registered each month. This shows cyber-attacks increase greatly from time to time. Windows malware families was chosen to doing malware detection using deep learning by applying the Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN). This malware detection will construct deep learning classification model on the extracted features from sampled malware families. This study wants to evaluate the performance accuracy of the resulting malware detection model in Windows architecture.

2. Methodology

Malware and benign software will be collected from various repositories. It will be analysed using static analysis to know the behaviour of the software files. This static analysis will be run in a secure environment without infecting the host system. The analysis data will be collected in csv files. Then it will convert the binaries of the malware and benign software to grayscale image datasets. This image will be used in the CNN architecture model. This dataset will be randomly split into 80 percent for training and 20 percent for validation sets of both the malicious and benign grayscale image datasets. The RNN architecture will use the features that were extracted from the software files using static analysis to run the model. Both deep learning architectures will use Anaconda environments to run the Spyder IDE, the scikit-learn tool, Keras, and TensorFlow.

3. Results and Discussion

The result of this project is the performance accuracy of two deep leaning architecture which is CNN and RNN architecture. The accuracy of CNN architecture is 97.5 percent meanwhile the RNN architecture is 88.5 percent. Since CNN has improved its ability to determine whether a file is malicious or benign. This is due to the fact that CNN layers contain many convolutional filters that evaluate the complete matrix of features and minimize spatial size. This makes CNN a very convenient and suitable network for categorizing malware and benign data. RNN are less accurate than CNN due to memory-

bandwidth-restricted computations that minimize the utilization of neural network implementation. This prove that CNN more accurate in classifying the files is malicious or benign.

4. Novelty of Research / Product

A number of studies have been conducted on the topic of malware detection via deep learning classifications. Previous studies have made use of CNN to identify malicious software by using grayscale image (Choi et al., 2017; S.L. and C.D., 2021). Additionally, a number of experiments on RNN architecture that employs long short-term memory (LSTM) to differentiate between malicious and benign files have been carried out (Hossain et al., 2021; Agrawal et al., 2019). An RNN architecture is used by Jha et al. (2020) for the classification of malware using a variety of feature vectors that are controlled by hyperparameters.

5. Conclusion

In conclusion, this project achieving the objectives. The CNN architecture has higher accuracy which is 97.5 percent meanwhile RNN architecture is 88.5 percent. The indicates CNN architecture more accurate to differentiate it is malicious or benign files. RNN are less accurate than CNN due to memory-bandwidth-restricted computations that minimize the utilization of neural network implementation.

REFERENCE LIST

Agrawal, R., Stokes, J. W., Selvaraj, K., & Marinescu, M. (2019). Attention in recurrent neural networks for ransomware detection. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). https://doi.org/10.1109/icassp.2019.8682899

Choi, S., Jang, S., Kim, Y., & Kim, J. (2017). Malware detection using malware image and Deep Learning. 2017 International Conference on Information and Communication Technology Convergence (ICTC). https://doi.org/10.1109/ictc.2017.8190895

Hossain, H., Kayum, S. I., Paul, A., Rohan, A. A., Tasnim, N., & Hossain, M. I. (2021). Malware detection using Neural Networks. 2021 5th International Conference on Electrical Information and Communication Technology (EICT). https://doi.org/10.1109/eict54103.2021.9733457

Jha, S., Prashar, D., Long, H. V., & Taniar, D. (2020). Recurrent neural network for detecting malware. Computers & Security, 99, 102037. https://doi.org/10.1016/j.cose.2020.102037

Malware statistics & trends report: AV-TEST. AV. (n.d.). Retrieved April 18, 2022, from https://www.av-test.org/en/statistics/malware/

S.L, S. D., & C.D, J. (2021). Windows malware detector using convolutional neural network based on visualization images. IEEE Transactions on Emerging Topics in Computing, 9(2), 1057–1069. https://doi.org/10.1109/tetc.2019.2910086

Research Exhibition in Mathematics and Computer Sciences: REMACS 5.0

e ISBN 978-629-97934-0-3