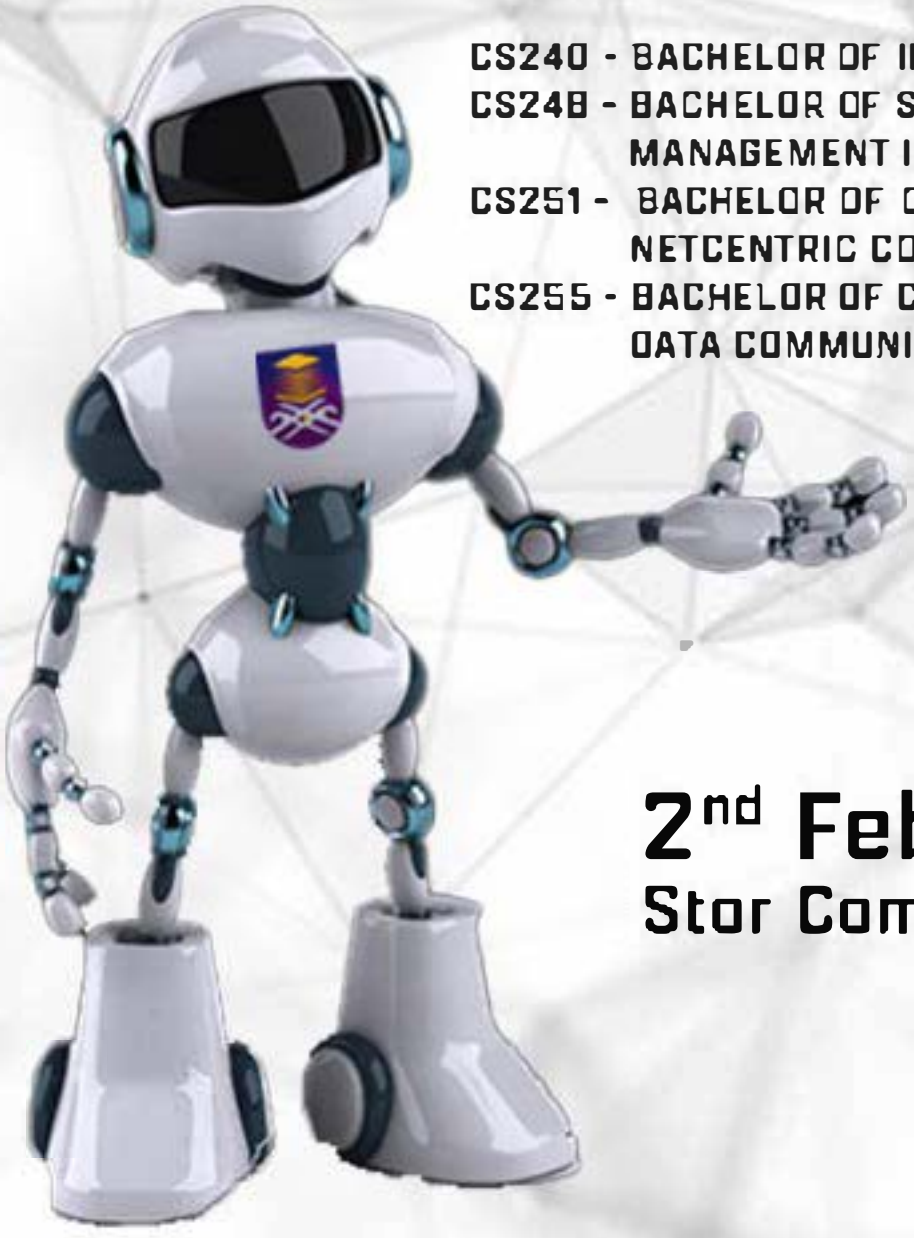
UNIVERSITI TEKNOLOGI MARA
Perlis Branch
Arau Campus

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

ANDROID MALWARE DETECTION USING DEEP LEARNING CLASSIFICATION APPROACH

Nur Amirah Amri and Mohd Faris Mohd Fuzi
College of Computing, Informatics and Media, Universiti Teknologi MARA Perlis Branch, Malaysia

Abstract

Android devices are becoming increasingly popular and there are more threats to Android users because malware writers are shifting their focus to exploiting vulnerabilities of Android devices for malicious behaviour. This paper will study Android malware detection using a deep learning classification approach. Deep learning is a thriving research area with many successful applications in different fields. Recently, these techniques have been applied to detect mobile malware and have once again shown their ability to remedy this type of problem. In this paper, Android software will be analysed by using malware analysis tools like APKTool and 010 Editor. Some selected features will be extracted from this process and compiled into a csv file. The selected features will be trained using the CNN and RNN model approach. The performance of Android malware detection using CNN and RNN model will be analysed by measuring its accuracy based on Metric Formula Definition Accuracy.According to the development process, CNN is performing better by detecting android malware with a 96 percent accuracy, while RNN delivers a 75 percent accuracy.

Keywords*: Android malware detection, malware analysis, deep learning, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN)*

1. Introduction

Android users are growing rapidly as Android devices become more popular. Malware writers are now exploiting Android vulnerabilities for malicious purposes, placing Android users at risk. Malware detection is growing more challenging. Artificial intelligence, machine learning, and deep learning algorithms are used in malware detection. Most of these algorithms have been used for cyberattack mitigation. Particularly feature extraction of malware dataset and hyper parameter optimization play a pivotal role to train a deep neural network. This research focuses on analysing and detecting Android malware families using Convolutional Neural Networks (CNN) and Recurrent Neural Network (RNN) in a deep learning approach. In addition, Android Malware detection development focuses on the accuracy values and network performance of deep learning models. The aims of this project are to construct a deep learning classification model on the extracted features from collected android malware files and evaluate the performance accuracy of the resulting android malware detection model.

2. Methodology

This project will use VirtualBox to secure Windows 10 to prevent viruses from infecting the host system. Malware analysis will be performed on 1,000 Android malware and benign software samples from diverse sources. A malware analysis tool will select and compile Android permissions and hash values into a csv file. The feature is binary-converted to a grayscale image using Python during malware visualisation. This creates the grayscale image dataset. Convolutional Neural Networks will train 75% and validate 25% of the grayscale image dataset and the result will be obtained using a confusion matrix table depending on accuracy and time consuming.

3. Results and Discussion

The accuracy of the performance of a deep learning architecture known as CNN architecture was improved as a direct result of this project. The findings of the experiment, along with the data and observations made during its course, demonstrated that the CNN model has the potential to be utilised in the detection of malicious software designed for use on Android devices. The architecture used by CNN has a 96 percent accuracy rate. This is because CNN layers contain a large number of convolutional filters, which evaluate the entire matrix of features while simultaneously reducing the amount of space they take up in the network. Because of this, CNN is a very convenient and appropriate network for classifying malicious software and harmless data. This demonstrates that CNN's classification of the APK files, determining whether they contain malicious or benign software, is accurate.

4. Novelty of Research / Product

Malware that affects android devices is particularly concerning to experts because of the severity of the damage it can do. Qiu et al. (2021) conducted a literature study on the achievements of deep learning-based Android malware detection and summarised their findings. It delivers a concise yet in-depth review to assist readers in rapidly gaining an understanding of the topic at hand. McLaughlin (2017) suggested a method for the identification of malware that processes the raw Dalvik bytecode of an Android application with the assistance of a convolutional network. The authors Alex V et al. (2020) recommended using a multiple-layer DNN in conjunction with a classifier (DL4J) in order to detect and forecast the presence of Android malware.

5. Conclusion

In conclusion, the data and observations showed that the CNN model may be used to detect Android malware. The constraint can be improved to improve this project. This chapter discusses and recommends the next task. The objectives of this project, which included the model's functionality and performance, were successfully met.

REFERENCE LIST

Alex V, M., Jocelyn, D.-G., & Michelle, L. (2020). Deep Learning in Detection of Mobile Malware. Deep Learning in Detection of Mobile Malware.

McLaughlin, N., Martinez Del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., Safaei, Y., Trickel, E., Zhao, Z., Doupé, A., & Joon Ahn, G. (2017b). Deep Android Malware Detection. Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy. https://doi.org/10.1145/3029806.3029823

Qiu, J., Zhang, J., Luo, W., Pan, L., Nepal, S., & Xiang, Y. (2021). A Survey of Android Malware Detection with Deep Neural Models. ACM Computing Surveys, 53(6), 1–36. https://doi.org/10.1145/3417978

Research Exhibition in Mathematics and Computer Sciences: REMACS 5.0

e ISBN 978-629-97934-0-3