

A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices

A PROJECT REPORT

Submitted by

E.ARUNKUMAR	421818104001
R.BABU	421818104002
S.HARIHARAN	421818104007
K.KESAVAN	421818104014

in partial fulfilment for the award of degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

**SARASWATHY COLLEGE OF ENGINEERING AND TECHNOLOGY
OLAKKUR, TINDIVANAM - 604 305.**



ANNA UNIVERSITY :: CHENNAI 600 025

MONTH 2022

ANNA UNIVERSITY : CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report “**A Performance-Sensitive Malware Detection System Using Deep Learning on Mobile Devices**” is the bonafide work of “**E.ARUNKUMAR, R.BABU, S.HARIHARAN, K.KESAVAN**” who carried out the project work under my supervision.

SIGNATURE

**Mr.P.T.SIVASHANKAR,M.E.,
ASSISTANT PROFESSOR,
HEAD OF THE DEPARTMENT,**
Computer Science and Engineering,
Saraswathy College of Engineering
and Technology.

SIGNATURE

**Mrs.S.SANTHANA PRIYA,M.E.,
ASSISTANT PROFESSOR,
SUPERVISOR,**
Computer Science and Engineering,
Saraswathy College of Engineering
and Technology.

Submitted for the university Examination held on

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We express our deepest gratitude to our Management of Saraswathy College of Engineering and Technology, **Dr.S.Ramadoss, Chairman & Correspondent**, who provides us with the entire infrastructure to proceed with our project.

We heart fully thank **Dr.C.Elanchezhian.M.E, M.B.A, Ph.D., Principal**, for giving us the opportunity to do the project successful

We would like to express our heart full gratitude to **Mr.P.T.SIVASHANKAR,M.E., Assistant Professor, Head of Department** of Computer Science and Engineering, Saraswathy College of Engineering and Technology, Tindivanam. He has been a motivating force and we keenly admire her for the support rendered throughout our project.

We express sincere thanks to our guide **Mrs.S.SANTHANA PRIYA,M.E., Assistant Professor**, Department of Computer science and Engineering, Saraswathy College of Engineering and Technology, Olakkur, Tindivanam. for her invaluable and generously given support and encouragement to us throughout our project.

We thank the other **Staff Members** and our friends for their generous support in making our project a successfully one.

Also we take this opportunity to extend our deep appreciation to our **family members** for all that they meant to us during crucial time of the completion of our project.

Finally we thank god almighty for his abundant blessings that enabled us to complete our project.

ABSTRACT

Android has become the most standard smartphone operating system. The rapidly growing acceptance of android has resulted in significant increase in the number of malwares when compared with earlier years. There exists plenty of antimalware programs which are designed to efficiently protect the user's sensitive data in mobile systems from such attacks. Here, I have examined the different android malwares and their methods based on deep learning that are used for attacking the devices and antivirus programs that act against malwares to care for Android systems. Then, we have discuss on different deep learning based android malware detection techniques such as, Maldozer, Droid Detector, DroidDeepLearner, Deep Flow, Droid Delver and Droid Deep. We aim to implement a model based on deep learning that can automatically identify whether an android application is malware infected or not without installation.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	iii
	LIST OF FIGURES	vi
	LIST OF ABBREVIATION	vii
1.	INTRODUCTION	1
	1.1 AIM OF THE PROJECT	2
	1.2 SCOPE OF THE PROJECT	2
2.	LITERATURE SURVEY	3
3.	SYSTEM ANALYSIS	7
	3.1 EXISTING SYSTEM	7
	3.1.1 Drawback Of Existing System	7
	3.2 PROPOSED SYSTEM	8
	3.2.1 Advantage Of Proposed System	9
4.	SYSTEM REQUIREMENTS	10
	4.1 HARDWARE REQUIREMENTS	10
	4.2 SOFTWARE REQUIREMENTS	10
5.	SYSTEM DESIGN	11
	5.1 SYSTEM ARCHITECTURE	11
	5.2 DATA FLOW DIAGRAM	12
	5.3 UML DIAGRAM	13
	5.3.1 Class Diagram	13
	5.3.2 Activity Diagram	14
	5.3.3 Use Case Diagram	15
	5.3.4 Sequence Diagram	16
	5.3.5 Collaboration Diagram	17

6.	METHODOLOGY	18
6.1	ALGORITHM	18
6.2	TECHNIQUE	19
6.2.1	K-Nearest Neighbors	20
6.2.2	Support Vector Machines	20
6.2.3	Artificial Neural Network (ANN)	20
6.2.4	Generative Adversarial Network (GAN)	21
7.	MODULE DESCRIPTION	22
7.1	FEATURE EXTRACTION	22
7.2	MALWARE DETECTION TECHNIQUE	23
7.3	DEEP LEARNING BASED MALWARE DETECTION	24
8.	SYSTEM IMPLEMENTATION	25
8.1	INTRODUCTION TO PYTHON	25
8.2	Spyder IDE	26
8.2.1	Features of Spyder	26
8.3	ANACONDA PROMPT	27
9.	CONCLUSION	28
	APPENDIX 1 SAMPLE CODE	29
	APPENDIX 2 SCREENSHOTS	50
	REFERENCES	52

LIST OF FIGURES

FIGURE NO	FIGURE	PAGE NO
5.1	SYSTEM ARCHITECTURE	11
5.2	DATA FLOW DIAGRAM	12
5.3.1	CLASS DIAGRAM	13
5.3.2	ACTIVITY DIAGRAM	14
5.3.3	USE CASE DIAGRAM	15
5.3.4	SEQUENCE DIAGRAM	16
5.3.5	COLLABORATION DIAGRAM	17

LIST OF ABBREVIATION

DNN	-	Deep Neural Network
ANN	-	Artificial Neural Networks
GAN	-	Generative Adversarial Network
SVM	-	Support Vector Machines
KNN	-	K-Nearest Neighbors
DL	-	Deep Learning
ML	-	Machine Learning
DBN	-	Deep Belief Network
IDE	-	Integrated Development Environment
APK	-	Android Application Package
XML	-	Extensible Markup Language
CLI	-	Command-Line Interface
API	-	Application Programming Interface
DFD	-	Data Flow Diagram
UML	-	Unified Modelling Language
OMG	-	Object Management Group