
# Android Hybrid Malware Detection Approaches Using Machine Learning Algorithms

B.K.G.P.N. Weerawardhana
Reg. No: MS20901226
M.Sc. in IT
Specialized in Cyber Security

Supervisor: Dr. Lakmal Rupasinghe

October 2021

**Department of Computing**
**Faculty of Graduate Studies and Research**
**Sri Lanka Institute of Information Technology**

# Table of Contents

# List of Figures

# List of Tables

# Acknowledgements

Before I start, I must dedicate praise and exaltation to few peoples in my research project.

Firstly, I would like to express, my sincerest appreciation, my thanks and gratitude to my research supervisor and co-supervisor Dr. lakmal rupasinghe who is senior lecture in cyber security at Sri Lanka Institute of Information Technology at Sri Lanka. I sincerely thanks for his providing me to more valuable advice, boundaries, directions, assistance, guidance and blessing to complete my research project during each step. He monitors me in every step and gave me to necessary advice and guidance till end of my project. I bottom of my heart thankful to his support, technical advice, and encouragement in this my research area. Sir, as you enabled me to understand and develop of the subject area you guided me to how to build better good experiment project, sir I will always remember you in my every future steps.

Finally, I want to highly be indebted my parents and my family since they stay will me in during entire project. They are assistance, encourage, support and their expectation had guided me to complete my experiment project. They were major part of my life when completing my project. I want to heartily tankful to their since they allow to complete my experiment successfully.

.

# Abstract

Working title: Android Malware analysis using Reverse Engineering, machine learning algorithms and android code analysis, and implement framework detect android malware.

Smart phones are a major part of a life in modern life. Among them android is the most usable mobile operating system. According to IDC corporate report in USA android operating system use 84.5% from market share [3]. currently most mobile attacks [22] happen with android operating system. Most of the attackers use chunks of malware code attached with android application java code to attack devices. The purpose of android malware writes is to get financial benefits; most of the famous type of android malware is ransomware which after executing malicious application on the device The malware will encrypt all the device valuable information of the device. To decrypt all data owners should be pay for decryption key. Due to android openness and free availability of market, android mobile operating system has become major attractive target for Cyber criminals. In this research paper focus issue of mobile application, analyze malware using reverse engineering, static and dynamic malware analysis, Malicious URL analysis and application code analysis of the android application and implement framework using machine learning based on Supervised machine learning approach for detect and classify android malware. static malware analysis based on reverse engineering of application and extracted application features without executing application. This recognizes application information flow, code structure, permissions, network details and static related features. Dynamic analysis examines the dynamic behaviors of the application during run time of the application in a fully controlled virtual environment. comparing both analysis static analysis consists with pattern-based approach; same time dynamic detection approach can be provided additional protecting from malicious application since it consists dynamic behaviors of the application including memory logs, CPU usage, system call logs, etc. Also, used malicious URL analysis to users protect from unawares downloading malware by using untrusted web URLs. Finally, the outcome will be developed platform which will be identified and protected from malware affected functions. Also, this framework will be using both static, dynamic malware analysis and URL analysis technique, and will solution for traditional malware detection tools problems and Final outcome framework called as Hybrid android malware detection [92] [93] system. Application will be based on machine learning algorithms and python programming. This application can protect from both malware codes and functions which functions are previously analyze using reverse engineering [11], machine learning algorithms, android code analysis and traditional malware features. Especially malware functions consisting of both

traditional and newly coming malware features. My experimental result project depicts that based machine learning based android malware classification and my project can be classify unknown applications malware analyzing android application static and dynamic features. In my project primarily based on android applications permissions and all dynamic related features. Also, users can classify their used accessed URLs are malicious or not and can be safe from android attacks.