# Chapter 7
# Detecting and Analyzing Malware in Android Mobile Devices Through Network Traffic Monitoring

**Khalid Hafiz Mir**
https://orcid.org/0009-0007-2610-3779
*Lovely Professional University, India*

**Anzah Bashir**
*Lovely Professional University, India*

**Isha Batra**
*Lovely Professional University, India*

## ABSTRACT

*Attacks by malevolent software developers have increased in tandem with the growing popularity of cell phones. This study examines several techniques these assailants employ and recommends more effective ones. Android phones are especially susceptible to these attacks since network traffic analysis isn't taken into account sufficiently in today's detection techniques. In this article, a rule-based classifier—a cutting-edge technique—that can reliably identify more than 90% of hazardous traffic is introduced. Malicious apps are becoming more and more prevalent due to the expanding black market and the increasing number of applications that are accessible. To identify questionable activity, the suggested system automatically collects and examines applications from reputable retailers or unofficial marketplaces. The*

DOI: 10.4018/979-8-3693-6925-8.ch007

*research provides a clear picture of how the platform has changed over time and how well various detection techniques work. It also compares several techniques for Android malware detection.*

## 1. INTRODUCTION

Due to their widespread use, cell phones are also a popular target for online criminals. Smartphones are increasingly being utilized for personal data storage and corporate transactions, which makes them susceptible to malware assaults. Because consumers frequently lack the time to carefully consider every program they download from websites or app stores, malicious developers find it simpler to target mobile devices. Malware may take many different forms, such as trojans, spyware, viruses, and phishing programs. Phishing apps imitate genuine apps, but their main goal is to get login passwords and sensitive data for fraudulent financial transactions(Arora et al., 2014). While viruses attach themselves to executable files and proliferate, Trojans pose as trustworthy applications to obtain illegal access to machines. Google's Android has surpassed previous smartphone systems like Symbian to become the most widely used. The proliferation of feature-rich apps in online marketplaces is partly responsible for the exponential increase in Android malware. Although legitimate software stores like Google Play have certain anti-malware features, their main security feature is permissions, which isn't always reliable(Zaheer et al., 2022). The problem is made worse by third-party app marketplaces, which permit software deployment without strict security controls. Attackers use a variety of strategies, such as update assaults, drive-by downloads, and repackaging, to target cellphones. Malware makers, in particular, frequently repackage programs, including dangerous code, into them before redistributing them through official and unofficial shops. Because certain Android viruses can collect personal data and send it to distant locations, they are very harmful. It is critical to address the threat posed by Android malware.

This study presents a system for remotely identifying Android malware that frequently connects to a remote server to transmit sensitive information or is controlled by a server. More reliable methods for identifying Android malware may be created by applying rule-based classifier development and network traffic feature analysis(Wang et al., 2019). App usage is on the rise as a result of the many activities that smartphone users partake in, including messaging, calling, social networking, and online surfing. The unauthorized third-party markets known as Black markets and legitimate app stores like Google Play and the App Store have both experienced explosive development. However, hackers may easily spread dangerous software in these stores because there are no code reviews or security checks in place.