A Deep Learning Approach to Malware Detection in Android Platform

Abdulrazak Yahya Saleh, Corrine Francis

Abstract*: Throughout the years, mobile devices such as tablets, smartphones and computers are extremely widespread because of the development of modern technology. By using these devices, users all over the globe can easily access a huge range of applications from both commercial and private use. Malware detection is an important aspect of software protection. As a matter of fact, the development of malware had begun soaring as more and more unknown malware are discovered. Malware is a common term used to describe malicious software that can induce security threats to any device and also to the Internet network. In this paper, malware detection based Deep Learning approach utilizing the Long-Short Term Memory Networks (LSTM) algorithm is conducted by the researchers. The chosen approach learns and trains itself using the features that are needed for malware detection. Then, large data sets are used for evaluating the trained algorithm.

***Index Terms*: Android Platform, Deep Learning, Long-Short Term Memory, Malware, Malware Detection.**

I. INTRODUCTION

According to [1], Android malware is uncommon but they occur. Android malware were created to quietly command a gadget, embezzle credential data or money from the gadget's holder, and steal security passwords together with bank account numbers [2]. Portable gadgets such as tablets and smartphones have spread via modern civilization at an exponential tempo and as a matter of fact the usage of the gadgets have blossom for a while. According to [3], the quantity of movable gadgets in use will expand from over 11 billion within 2016 to over 5 billion addition by 2020. Within the gadget platforms, Android has become one of the most notable Gaia of all the gadget platforms. In hock to the open-door nature of applications (apps) amelioration as against to the "confined oasis" kind of workflow tailed by its rivals, it has achieved idolization at a tremendous stride. Since there is much crucial private information being kept on these computing gadgets, it is easy for the malware creators and hackers to gain that information. It is because Android is an open fountainhead with ground-level barricades to break in and thus may avail to become the target for malware invasion. Malware is malevolent software that acts to creep into the concealment and integrity of a system [4] such as, in [5] it guise grave dangers to the smartphone users. The malware will steal classified data, and also can dispatching memo and ad without the user permission [6]. As stated by the mobile warning report liberated by F-Secure in 2014 [7], estimated 95% of bad-natured apps were released on the Android platform. All the malware creators have turned their concentration from Windows of the PC generation to Android of the gadget aeon [8- 9].

Based on a study conducted in 2015 that advised over 6.3 million apps, nearly 1 million were discover to be malware dropping in greater than 250 classifications as stated by Symantec [9]. Addition to that, in 2015 there are nearly 750,000 fresh Android malware models were discovered, a 32% thrive from 2014 [9] and this flow is anticipated to get atrocious. Furthermore, according to [10], the Android gadgets are being contemplated by a huge part of malware.

The threat that malware hold is bringing a negative effects in both emotional and financial as stated by a newest report by Kaspersky Lab [11] that there are almost 1 billion dollars that being stole within approximate two years from the entire monetary establishment all around the globe as the aftereffect of malware invasions. Because of that, the immediate obligation for capable safeguard techniques to shield all the Android-enabled gadgets that have the functions of identification and prevention with the malware are needed.

In January 2017, the detection of malware infection was at 43% and since then there was a soaring activity of malware infection where there is approximately 56% of new and unknown malware being detected in April 2017 [12]. Smartphones possessed a huge pile of classified information that includes financial security and personal details. That quantity of valuable information can be retrieved illegally from the smartphones had made it the main mark for cyber law-breaker from all stripes [13]. Therefore, the malware detection is important as it can prevent illegal hackers from stealing user's credential information [13]. Deep Learning (DL) is the software that tried to imitate the activity in layers of neurons in the human brain, specifically in the neocortex segment that consists of 80% wrinkly part where the process of thinking happens [14]. DL's main function is to learn how to represent data [15]. There are numerous researches that incorporate the utilization of DL technique in the malware detection for Android platform [16-18]. The method of using DL in malware detection has inspired a large quantity of triumphant programs in communication identification, figure categorization, and natural language concoct. An introductory chore in DL as it administer to Android malware recognition was bestowed as explained in [18]. However, there are very restricted concentration has been reimbursed to

Revised Manuscript Received on June 05, 2019

Abdulrazak Yahya Saleh, FSKPM Faculty, University Malaysia Sarawak (UNIMAS), Kota Samarahan, 94300 Sarawak, Malaysia.

Corrine Francis, FSKPM Faculty, University Malaysia Sarawak (UNIMAS), Kota Samarahan, 94300 Sarawak, Malaysia.