OPEN ACCESS Freely available online

Journal of Information Technology and Software Engineering

Commentary

Malware Detection Using Machine Learning in Android Devices

Lorea Joseph*

Department of Computer Science, Harvard Universit, Massachusetts, USA

ABOUT THE STUDY

Malicious cyberattacks on Android mobile devices have proliferated as the use of smartphone devices has grown rapidly. Because the Android system has acquired a wide range of sensitive apps, such as banking applications, it has become a target for malware that exploits security system vulnerabilities. Several research presented models for detecting mobile malware. However, advancements are necessary to obtain peak efficiency and performance. As a result, we used machine learning and deep learning techniques to detect Android-directed harmful assaults. To detect malware in mobile applications, the Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Linear Discriminant Analysis (LDA), Long Short-Term Memory (LSTM), Convolution Neural Network-Long Short-Term Memory (CNN-LSTM), and autoencoder methods were used.

Two Android mobile benchmark datasets were used to test the cybersecurity system. The correlation was analysed to identify the aspects of these systems that are very significant in terms of attack protection. The malware was found on Android applications using machine learning and deep learning methods. Using the CICAndMal2017 dataset, the SVM algorithm attained the maximum accuracy (100%). Using the Drebin dataset, the LSTM model similarly achieved a high percentage accuracy (99.40%). Furthermore, in the validation phase, we discovered a good association between the predicted values and the target values by assessing the mean error, mean square error, root mean square error, and Pearson correlation.

The SVM approach achieved R^2=100% in the CICAndMal2017 dataset, whereas LSTM achieved R^2=97.39% in the Drebin dataset. Our results were compared with existing security systems, demonstrating that the SVM, LSTM, and CNN-LSTM algorithms are highly effective in detecting malware in the Android environment. The prominence of the Android operating system has drawn the attention of malware developers, whose activity has risen considerably in recent years. Many malware developers are interested in hacking mobile devices and converting them into bots. This allows hackers to get access to the infected device as well as other linked devices and create botnets. Botnets are used to carry out various harmful activities, such as Distributed Denial-of-Service (DDoS) assaults, spam distribution, data theft, and so on.

Malicious botnet assaults use complex strategies (eg., multi-staged payload or self-protection), making the malware difficult to identify. This, in turn, creates significant dangers that necessitate the development of efficient methods for detecting these attacks. Android botnets are used to launch attacks on targeted devices. DDoS attacks are executed out by flooding the target computer with unnecessary requests while blocking valid ones, resulting in the failing of the targeted system and interruption of services. As a result, machine learning algorithms have been shown to be useful in detecting and monitoring such risks in the internet of things.

According to Haystack, a third of software development businesses handle 70% of mobile applications and hold user personal data. According to the AV-TEST Security Institute malicious programming has surged, with Kaspersky detecting 5.7 million malware Android packages in 2020, three times more than in 2019 (2.1 million). The rise of malware installation packages for smartphones over the previous five years. As a result, signature-based harmful installation packages for extracting malware patterns based on their features can be a useful technique for securing mobile applications. Malicious assaults can be carried out in a variety of ways, including fuzzing, denial of service, DDoS, port scanning, and probing.

These attacks may endanger the transport, application, or protocol layers, including the internet control message protocol, file transfer protocol, user datagram protocol, simple mail transfer protocol, transmission control protocol, hypertext transfer protocol, and others. Network-based intrusion detection systems can identify and respond to such attempts by scanning the network. Smartphones are growing increasingly ubiquitous, making them a lucrative target for hackers due to their vulnerability to security breaches. Android is an open portal for attackers who use malicious applications to exploit the system's security weaknesses. Antivirus programmes against new malware, produced using AI, machine learning, and deep learning algorithms that forecast malware, are an emerging way for signature-based harmful attack detection.

Correspondence to: Lorea Joseph, Department of Computer Science, Harvard Universit, Massachusetts, USA, E-mail: josephL@hotmail.com

Received: 18-Nov-2022, Manuscript No. JITSE-22-20851; **Editor assigned:** 21-Nov-2022, Pre QC No. JITSE-22-20851 (PQ); **Reviewed:** 07-Dec-2022, QC No. JITSE-22-20851; **Revised:** 14-Dec-2022, Manuscript No. JITSE-22-20851 (R); **Published:** 21-Dec-2022, DOI: 10.35248/2165-7866.22.12.307.

Citation: Joseph L (2022) Malware Detection Using Machine Learning in Android Devices. J Inform Tech Softw Eng. 12.307.