Asian Journal of Research in Computer Science

10(4): 30-46, 2021; Article no.AJRCOS.71739
ISSN: 2581-8260

A Comprehensive Study of Malware Detection in Android Operating Systems

Suhaib Jasim Hamdi[1*], Ibrahim Mahmood Ibrahim[1], Naaman Omar[1], Omar M. Ahmed[1], Zryan Najat Rashid[2], Awder Mohammed Ahmed[2], Rowaida Khalil Ibrahim[3], Shakir Fattah Kak[1], Hajar Maseeh Yasin[1] and Azar Abid Salih[1]

[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.
[2]Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq.
[3]University of Zakho, Duhok, Kurdistan Region, Iraq.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v10i430248
Editor(s):
(1) Dr. G. Sudheer, GVP College of Engineering for Women, India.
Reviewers:
(1) Anthony (Tony) Spiteri Staines, University of Malta. Malta.
(2) Robiah binti Yusof, Universiti Teknikal Malaysia Melaka, Malaysia.
Complete Peer review History: https://www.sdiarticle4.com/review-history/71739

Review Article

Received 15 May 2021
Accepted 20 July 2021
Published 20 July 2021

ABSTRACT

Android is now the world's (or one of the world's) most popular operating system. More and more malware assaults are taking place in Android applications. Many security detection techniques based on Android Apps are now available. The open environmental feature of the Android environment has given Android an extensive appeal in recent years. The growing number of mobile devices are incorporated in many aspects of our everyday lives. This paper gives a detailed comparison that summarizes and analyses various detection techniques. This work examines the current status of Android malware detection methods, with an emphasis on Machine Learning-based classifiers for detecting malicious software on Android devices. Android has a huge number of apps that may be downloaded and used for free. Consequently, Android phones are more susceptible to malware. As a result, additional research has been done in order to develop effective malware detection methods. To begin, several of the currently available Android malware detection approaches are carefully examined and classified based on their detection methodologies. This study examines a wide range of machine-learning-based methods to detecting Android malware covering both types dynamic and static.

**Corresponding author: E-mail: Suhaibbaroshky@gmail.com;*

Keywords: Malware; detection; operating system; android; viruses.

1. INTRODUCTION

Android is the most popular smartphone platform in today's market, and its popularity is growing by the day, Malware includes viruses from computers, worms, backdoors, spyware, Trojans and other harmful systems [1]. There are many malware strategies that target the Android platform without the victim's awareness. This is done by transferring confidential information [2,3].The Android operating system is usually regarded as the most popular and the most regularly affected [4]. The quick growth of the mobile Internet has made Android the smartest terminal operating system in the world, Mobile malware has become a serious cyber security problem [5,6].The phrases 'virus' and 'malware' are often used yet vary technically. Malware is a comprehensive phrase including all kind of malware, by accessing the infected folder or application, the victim is woken up to the infection [7]. The virus might erase or encrypt the data while it is running the infection. In addition, the software may be changed or system features may be disabled, the software detection system focuses on the qualities both of the execution and of the source code of the program, the software detection system focuses on the qualities both of the execution and of the source code of the program Android malware detection techniques and machine learning [8]. Malware analyses are a procedure that detects software programs to determine their behaviour, functioning and whether or not they are malware. Methods of Android malware detection may be classified or also dynamic analysis [9,10]. This indicates that every 10 seconds a new Android malware application is being identified, Malware detection technique may be classified as static detection, dynamic detection and hybrid detection in three categories [11,12]. Since android is the most common operating system used for Internet access. Android includes an operating system, an app framework and key apps. Each Android app is segregated from other applications [13,14]. Machine Learning algorithms and methods have reached a high accuracy in malware detection among the several methods in the detection of malware [15,16]. Many mobiles with several operating systems are available. Android is a mobile open source operating system that can be accessed on numerous devices. Android devices are activated every day according to Google 1.3 million, the risk of malware will rise by extending mobile phone capabilities [17].

Mobile malware is malicious software targeting mobile phones or PDAs causing system crashing and private information loss or leak [18]. Personal digital assistants (PDA) As wireless telephones and PDA networks are increasingly popular and sophisticated, ensuring security and protection against electronic attacks in the form of viruses or other malware is increasingly difficult [19].

Mobile malware is malicious software aimed at mobile phones or wireless Personal Digital Assistants (PDA), due to system breakdown and private information loss or leaking [20].

The detection of malware is the scanning procedure for computers and malicious files [21]. It detects malware effectively, because there are several techniques and procedures involved [22]. It's not a single way, it's very complicated. It simply takes less than 50 seconds to malware identification and eradication [23].

Checking for Android malware: Go to the Google Play Store app on your Android smartphone. Tap on the button of the menu [24]. Google Play Protect will then tap. To compel the device to check for malware, tap the scan button [25]. You'll notice an opportunity to uninstall any dangerous applications on your smartphone [26].

How to remove malware and viruses from your Android smartphone: Power off your phone and safely boot back [27]. Press the power button to access Power Off, deactivate the suspicious program, and find other applications that you believe may be infected by the mobile security application [28].

You will frequently not instantly detect an infection as the spyware might run sleeping while you're using your phone [29]. Some performance problems are a normal wear-on-phone symptom. These symptoms may, however, also be an indication of malware at work [30].

When you download or install an infected software, malware spreads across the computer. You also write an email or a link in your PC [31]. After malware comes into your computer, it connects to several files and overwrites the data. When malware is sent across the network, the machine is infected [32].

In most situations, antivirus is not necessary for Android smartphones and tablets [33]. However, it's also true that there are Android infections and the antivirus with helpful functions may offer an additional safety layer [34]. You can download the finest Android antivirus app. Mobile Security Bitdefender [35].

The reputation of Android for safeguarding its fragmented environment is not good - the broad opinion is that iPhone are more secure [36]. But you can get an Android and simply lock it down. With an iPhone, not like that. It is more difficult to attack Apple's gadgets, but also to safeguard [37].

Signature-based detection employs malware identification viral codes [38]. Malware has a unique code to identify it [39]. The malware scanner captures the code and transmits it to a cloud based database when a file enters the machine [40]. The virus prevents the file from being removed from the computer [41]. In brief, a computer and its network can be havoced by malware. It is used by hackers to steal passwords, destroy information and inoperative machines [42]. A malware infestation can cause various difficulties that impair your business' day-to-day functioning and long-term security [43].

The type of machine learning seen in a large number of antimalware software seeks to learn the harmful files that are benign based on malicious and benign code databases [44]. Malware evolves quickly, therefore the algorithms also need to adapt fast [45]. Detection of abnormalities (or external detection) is a discovery of uncommon objects, occurrences or observations that trigger suspicions that are substantially different from most data [46]. Many significant issues have been demonstrated to be undecidable in malware analyses. These difficulties include virus detection, unpackaging detection, malware samples being matched to a number of templates and trigger-based behavior detection [47].

There are two approaches to malware analysis – static analyzes or dynamic analyses. The malware sample is checked without detonating it, but the virus is really run in a controlled, remote setting with dynamic analysis [48]. The purpose of malware analysis is to learn how a certain component of malware works to help secure the networks of a company. In general, static malware analyzes are difficult yet worthwhile [49]. The following I would recommend: Know what to ask questions Without a purpose, you don't begin an analysis [50].

I've usually referred to two primary parts of the process when discussing malware analytics: computational analysis and code analysis [51]. Most Virus is written in a language of middle level, and after the code is done the malware is compiled to make it readable across the operating system and/or hardware [52]. The code is not readable or readable by people at this level [53]. Malware analyst is uncommon and demanding. A expert in one competency is excellent but it is also useful to be a generalist with several talents [54]. Therefore, be open-minded and decide what you love [55]. For a few of months, I have been able to accomplish this work [56]. Malware is a collective word for a number, including viruses, ranching software and spyware, of malware types [57]. In the short term, malware usually includes code written by cyber attackers which causes severe data or systems damage or illegal network access [58].

This research addresses the issues related to the risks and malware problems faced the Android operating systems. The style of the depended methodology is structured as explaining the general related theory to be a ware of the addressed subject, then followed by a detailed survey of what have been depended and proposed by previous works.

2. MALWARE TECHNIQUES DETECTION

Malware methods are used to identify malicious software and prevent computer system infection, therefore preventing it from losing potential information [59]. Abandonment of the system. Three methods to detect and categorize malware have been identified:

- Detection on permission basis.
- Detection on the basis of signature
- Methods based on pacification [2].

2.1 Malware Based on Machine Learning Android Malware Schemes

Application of machine learning, which has been defined by different academics, is an artificial intelligence research branch [60]. Machine learning, according to, comprises of a series of approaches for automating predictions on the basis of historical data [61]. Machine learning can be separated into five paradigms with various theoretical notions based on a comparison between the master's learning

algorithms and activities carried out by the human brain: symbolists, connectivity, evolutionist, Bayesian and analogizer [62]. Each machine learning category has its own fields of study and algorithms [63].

2.2 Android Malware's Risks

Once a malware-infected Android OS is installed, users are exposed to and are exposed to several risks. Some of the possible problems that can occur are:

- Database loss
- Theft of personal data that may lead to Dieft of identity
- Users' spying
- Telephone remote operation
- Ransomware causing financial loss [5].

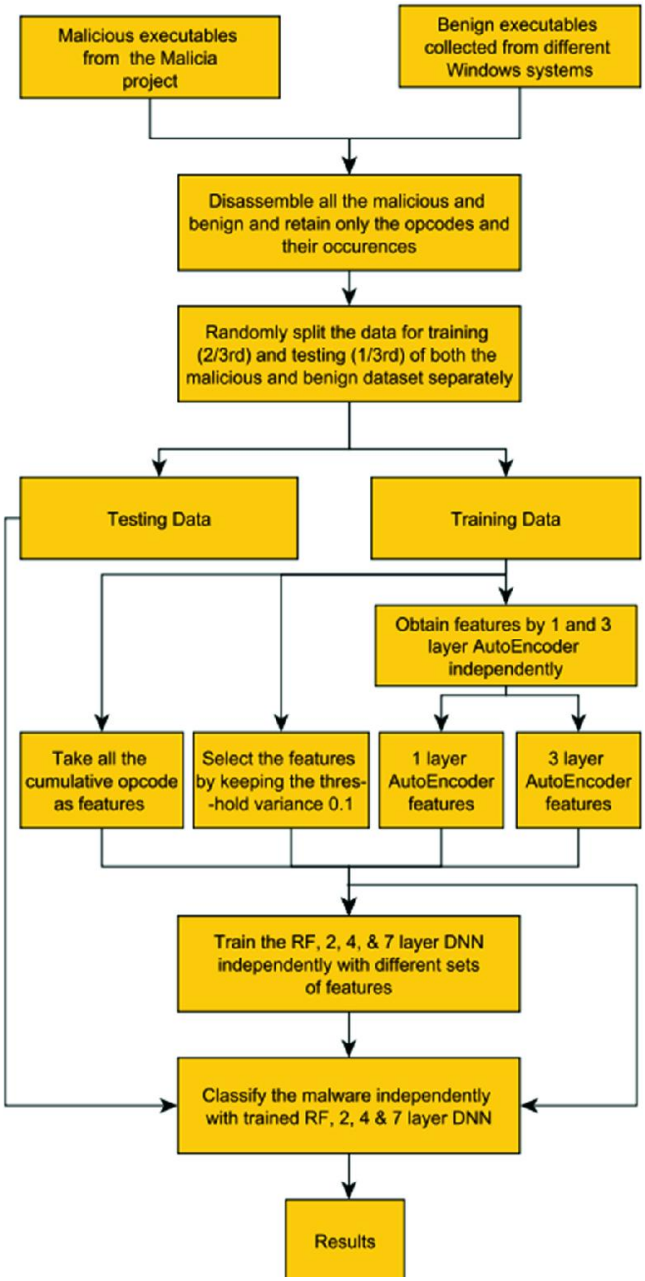

Fig. 1. Malware Detection flowchart [64]

2.3 Random Forest Algorithm

The random forest provides random selection attributes based on decision-making trees. The classic decision tree selects an excellent attribute in the current node attribute set [47]. The random forest picks a subset of the k characteristics in the set of node characteristics randomly. And then chooses an ideal attribute for the partition from the subset [65].

2.4 Android Malware Based

2.4.1 Classification

Machine learning involves statistics and theory of probability. The learning model of the machine is primarily designed to provide algorithms that allow the computer to learn [66].

2.4.2 Static analysis

Static analysis is used to decompile the application to retrieve the code file and extract the features without executing the application software via reverse engineering. These characteristics are static [67].

2.4.3 Dynamic analysis

The dynamic analysis approach is to replicate the behaviour of the user by executing the program and to identify if malicious software is based on the program's real functioning [68,69].

2.5 Algorithms for Machine Learning

There is an enormous range of classifiers that can be utilized for machine learning. Once the current techniques to machine learning have been intensively studied, the downsides and advantages of succeeding algorithms have been highlighted such that I consider that I am particularly willing to be able to identify malware:

1) K-Nearest Neighbor (knn): Although it is claimed to be an extremely simple algorithmic program (silent algorithms) and performs quickly, it is improper or not very rewarding as soon as the training set is blare or outliers undergoing.

2) Subject Vector Machine Support (SVM): method comprises a robust and intricate theoretical and abstract basis, since it typically performs more than alternative algorithms for classification outcomes.

3) Decision Tree (J48): might be a classification tree which hopes to categorize the instances properly with functional values. There are nodes and distribution leaves in a decision tree.

4) Neural networks (NN): is another extremely productive, human-brain-based machine learning method. Neural networks methodology is nevertheless longer than alternative clinicians, and is considered to be troubling or rigorous, in which real time might be limiting in any malware detection system.

5) Naive Bayes (NB): presume that the structures are casual sovereigns and calculate its potential for the decision to be appealed [70].

3. RELATED WORK

The effective and precise detection of malware. This study provides an effective and accurate solution to this problem, called SAMADroid, a new 3-degree hybrid malware detection model for Android operating systems, Some of the latest malware identification and protection methods were studied in detail. SAMADroid is a new malware identification model that combines the advantages of static analysis, dynamic analysis, and intelligence learning. Based on the advantages and disadvantages of current anti-malware technologies [4]. Many attacks targeting Android phones may be carried out, mostly by the development of applications. Some classification algorithms have been evaluated in their research to assess best performance. Algorithm when it comes to malware identification android. An Android device data collection was collected from fig share and used for information in the Waikato environment, Training and research analysis (WEKA), calculated by accuracy, false-positive rate, accuracy, retrieval, f-method, receiver operating curve (ROC) and root-mean square, Mistake (RMSE). Multi-layer perceptron's were found to work best with 99.4 percent accuracy, their project was designed to test Android malware classification algorithms [5]. A security detection approach based on the Metropolis algorithm is proposed in their article on Android introduce a concept method named PPMDroid to conserve bandwidth and speed up the process with many optimizations [71]. Today, in all countries, the usage of cell phones is increasing and sadly, cyber criminals are constantly targeting mobile phones. The key cause of this kind of assault is the malicious software that a consumer downloads from reputable media like Play store, the App Store and everything. Their framework is

a smartphone android technology focused on deep learning. In order to detect the malicious actions of an algorithm the application can conduct static and dynamic analysis. When security makers used signature detection to detect a ransomware, attackers began to create a new signature to circumvent those solutions. This reduced the reliability of those solutions apps [72]. This approach evaluates the 24 risky allowances of Android using the Metropolis algorithm; Removes permissions for uncertainty, extracts characteristics of permission. [65].

An Android learning machinery and systems been built. It identifies Android malware from two static and dynamic analytical perspectives. Using machine learning, it is feasible to successfully identify malware with Android malware. The combination of static analysis and dynamic analysis may simultaneously increase detection accuracy and efficiency [68]. A portable malware position was peoposed to display the speed up the efficiency of operation classifier with 9 movement highlights. The model also uses grouping techniques like stream, package and time-based highlights to describe families of malware. Mobile malware is thus pernicious and therefore it is essential for users to provide a fast and accurate detection method, Minimize malware investigation costs by picking representative samples only 8.5 % to 22 percent (12). They suggested a malware identification scheme to safeguard the protection of Android that protects the privacy (or assets) of telephone vendors, consumers and security service providers. It identifies malicious applications in app stores of telephone providers and on phones of consumers without exchanging data, First, the privacy problems of current static and dynamic malware detection methods are highlighted; runtime actions of apps and malware signatures with others. Fig. 1, illustrates the architecture of Droid Deep as (Dynalog-Dynamic Analysis and Deep Leerning Classifiers). The mechanism of the system starts with Benigm/Malware, then Real Phones, after that Logs Files, finally Features Extraction/Selections.

They suggested DL-Droid, a deep learning framework used in state-of-the-art input generation to detect malicious apps from Android. Experiments on actual devices per developed with more than 30,000 applications (benign and malware). They introduced DL-Droid, an advanced dynamic analysis system for the identification of Android malware, Droid uses profound learning with a standard input generation technique, although it has the potential to use the popular Monkey platform in state-of-the-art practice (stateless method). This is the first study to examine profound learning with complex functions derived from smartphones utilizing actual mobile. Their findings also emphasize the importance of enhanced input generation for complex analytical systems built to identify Android malware through machine learning [73]. Today, several smartphone operating systems are used, including various formats and market shares. Mobile networks, like other information systems, are sensitive to virus assault. Detection of malware is very critical and is a must-deliver method for protecting and minimizing private data in any system. The objective of theie workr was to create a user profiling method for the mobile identification of malware. The vulnerability of any malware identification strategy has already been noted and debated [74]. With the spread of.

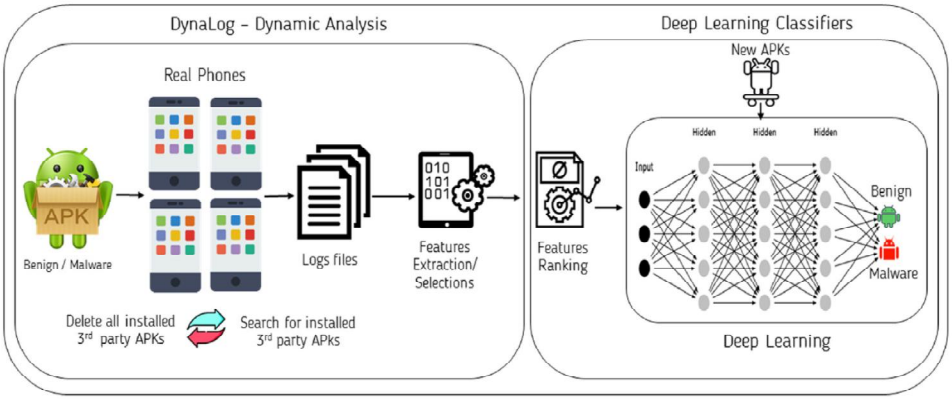

Fig. 2 Architecture of Droid Deep [73]

Android-based smart Internet of Things (IoT), malicious Android apps for IoT devices have attracted the publicity because of their privacy and property loss concerns. Their paper introduced Eve Droid, a malware identification framework designed to allow detection of Android and IoT malware, which allows the IoT world safer by decreasing malicious software running on Android-equipped smartphones. Due to API changes, they were able to capture previously unseen activities. The results also demon strate that EveDroid is more accurate and robust to malware evolvement compared to existing detection systems [75]. Classification utilizing machine learning was an important class of malware security solutions. They proposed a new classification method based on the findings of a longitudinal analysis on Android applications focusing on their complex behaviour. The key lesson learned is that learning software development offers a promising way to identify malware over the long term, they have examined a new approach centered on an evolutionary characterization of smartphone behaviours. These results showed the potential of long-term malware identification approaches focused on evolution [76]. A comparison was done to accessible Android malware datasets with 15 key requirements and identifying key weaknesses. In this portion, they proposed the second part of CICAndMal2017 which incorporates new feature sets such as static permissions and attempts and the appended API calls. In the portion of dynamics [77]. In recent years, many mobile malware detection systems have been suggested to deal with this issue. Their paper is about the survey of current smartphone detection systems for malware. Their paper includes a systematic investigation of some accurate structures built on a method of static analysis. It explains and evaluates each scheme. In addition, both programs are similar to a tutorial on techniques. Malware detection is considered a key precondition for Android Operating System to defend mobile users from personal theft of privacy [78]. Two kinds of characteristics, permission requests and system calls are examined as a technique to identify malware, in their study. The model used permissions to get an accuracy of approximately 80% and system calls to reach a classic cation accuracy of about 60%. Their article analysed two major characteristics for Android malware detection, permission and system calls, and applied machinery education to both. The results suggested that permission data is better for malware detection than system call data [79]. Their paper is based on Android and learning machines. It identifies malware from two static analytical and dynamic analytical aspects. With machine learning for Android malware detection, it is feasible to identify malware successfully. Static analysis and dynamic analysis may simultaneously increase detection accuracy and efficiency, to discover malicious software, a security technique must be developed. The exponential growth in the amount of Android malware presents great challenges for malware programs because the number of malware samples is overwhelming. They worked to build a new framework that automatically classifies Android malware samples with high precision and accelerates malware detection efficiently by proposing representative malware screening samples. Android is more efficient and reliable than advanced methods. Malware inspection and malware raising to avoid analysis. It offers significant knowledge for the identification and inspection of malware and increases malware levels to avoid review [80]. Due of Android's open nature, an investigating a number of various malware methods of detection such as: MalDozer, Droid Detector, Droid Deep Learner and Deep Flow. It employs a static analysis approach as well as an API technique. MalDozer is used to detect malware in the Convolution Neural Network, Whether or if an android application is contaminated with malware without a facility, Our goal is to create a profound learning model which can recognize automatically [81]. In order to train the pre-processed sequences, next utilize two deep learning methods: DexCNN and DexCRNN. Two meth- abilities have been examined on a data set of 80 0 benign APKs and 80 0 malignant APKs, Your study presents two detection approaches for end-to-end malware without human engineering. First, utilizing the sample retrieval technique to pre-process the classes.dex APK file. DexCNN can achieve accuracy of 93.4 percent, while the DexCRNN can reach accuracy of 95.8 per cent. Other comparable malware detection tasks may readily be expanded to the approaches given [82]. This mode of detection increases to some level the detection accuracy. The random forest method has been upgraded to yield flourishing sets. Then the approach is used Rules for sensitive authorization, to analyse this detection mechanism and validate the efficacy of the system, a number of assessment approaches have been applied. Utilized to assess the method of detection and to validate the system's efficacy [83]. DAMBA, a novel prototype system based on C/S architecture, is presented in their article.

DAMBA extracts the application's dynamic and static characteristics. TANMAD-method was provided, a two-step methodology for detecting malware from Android, which minimizes the spectrum of probable families of malware. Numerous optimization ideas were provided for hybrid analysis to achieve improved efficiency and precision in their papers. The complicated computation work of the PC customer was finished to maintain the limited resources of the mobile customer [84].Cloak & Dagger, a specific kind of assaulting action, is detailed in length. Detection algorithm for harmful software packages, The Cloak and Dagger attack algorithm is presented for the detection of malicious software packages. It is suggested that you conduct a Cloak and Dagger assault [85]. The detection will be measured using three Distinct classifications: K-nearest (KNN), Random Forest (RF) and Decision Tree (DT). In the identification and classification of computer.

Malware, a visualization methodology was used, although not many trials concentrated on Android operating system. By utilizing the Random forest machine learning method on picture characteristics created from APK samples, the suggested study could reach 84.14 percent detecting accuracy [86]. The technology has been used to build a framework named the ONAMD Online Android Malware Detection Approach, The ONAMD initially collects the details (e.g., requested permissions, and basic data info, etc.). Next, the SVM and Random Forest algorithm improves the capacity of malware simulation to identify the program as benign or harmful. The method has been extended to 600 applications. The experimental results indicate that the solution takes half-time and higher reminder rates than Androguard [87]. By utilizing the Random forest machine learning method on picture characteristics created from APK samples, the suggested study could reach 84.14 percent detecting accuracy. Android malware has been detected daily such that malware analysts find it tough to identify it. For autonomous learning, the detection is done and compared using three distinct classifiers: KNN, Random Forest and Decision Tree (DT).Less costly memory representation and hence speed up the learning process [88].

4. DISCUSSION AND COMPARISON

After browsing the most related previous works and explaining the depended algorithms in the field of malware detection faced Android operating systems, it is very important to provide a summary of them. This has been done by making a comparison among all addressed related works in previous section, the comparison is done depending on terms of (Model, Methods, Algorithms, Achieved Objectives, and Significant Results)

Table 1. Analysis and Results of the Existing Systems for Malware Detection

Ref.	Model	Methods/ Algorithm	Achieved Objectives	Significant Results
[4]	model that combines the advantages of static analysis, dynamic analysis	Intelligence Machine Learning	This study provides an effective and accurate solution to this problem	achieves high accuracy of malware detection via efficiency
[5]	Each malware detection technique's flaws were highlighted.		The objective of the paper is to create a user profiling method for the mobile identification of malware.	Based on mobile user profile, it may be utilized effectively.

Ref.	Model	Methods/ Algorithm	Achieved Objectives	Significant Results
[11]	Some classification algorithms have been evaluated in their research to assess best performance	f-method, receiver operating curve (ROC)	Their project was designed to test Android malware classification algorithms.	It was discovered that multi-layer perceptron Performs best with an accuracy of 99.4%.
[13]	Proposed a new classification method based on the findings of a longitudinal analysis	machine learning	The key lesson learned is that learning software development offers a promising way to identify malware over the long term	These results showed the potential of long-term malware identification approaches focused on evolution.
[17]	ONAMD Online Android Malware Detection Approach	the SVM and Random Forest algorithm		The experimental results indicate that our solution takes half-time and higher reminder rates than Androguard
[65]	Removes Uncertainty permissions, and extracts certain permission features.	Metropolis algorithm	To learn and classify, use these essential permissions	Our solution decreases detecting, achieve 93.5 percent for the accuracy of harmful program detection.
[68]	Built FalDroid, a new framework that automatically classifies Android malware		Malware inspection and malware raising to avoid analysis.	Minimize malware investigation costs by picking representative samples only 8.5 % to 22 percent
[70]	The model also uses grouping techniques like stream	machine learning	It is essential for users to provide a fast and accurate	This study condenses the progression

Ref.	Model	Methods/ Algorithm	Achieved Objectives	Significant Results
			detection method.	of malware detection techniques supported
[71]	First, the privacy problems of current static and dynamic malware detection methods are highlighted	PPMDroid method	To conserve bandwidth and speed up the process with many optimizations.	Large evaluation findings with real malware samples show the reliability and efficacy of the method
[72]	The method will combine both static and evolving effects of study	deep learning	The usage of cell phones is increasing and sadly, cyber criminals are constantly targeting mobile phones.	This reduced the reliability of those solutions
[73]	DL-Droid,	deep learning	To detect malicious apps from Android.	Our findings also emphasize the importance of enhanced input generation for complex analytical systems built
[76]	designed to allow detection of Android and IoT malware	EveDroid	Due to API changes, they are able to capture previously unseen activities.	The results also demon strate that EveDroid is more accurate and robust to malware evolvement compared to existing detection systems
[77]	Proposed the second part of CICAndMal2017	CICAndMal2017	the main targets for attackers to unleash destructive	At the first layer, they were successful 95.3 % with Static-Based

Ref.	Model	Methods/ Algorithm	Achieved Objectives	Significant Results
			intentions	Malware Binary, 83.3 % with Dynamic-Based, and 59.7% with Dynamic-Based at the second layer.
[79]	The model used permissions to get an accuracy of approximately 80% and system calls to reach a classification accuracy of about 60%.	machine learning		The results suggested that permission data is better for malware detection than system call data.
[80]	It identifies Android malware from two static and dynamic analytical perspectives	machine learning classification	It is possible to effectively detect malware.	Improve precision and efficiency of detection.
[82]	study presents two detection approaches for end-to-end malware without human engineering	deep learning DexCNN and DexCRNN	In order to train the pre-processed sequences	DexCNN can achieve accuracy of 93.4 percent, while the DexCRNN can reach accuracy of 95.8 per cent.
[83]	Utilized to assess the method of detection and to validate the system's efficacy.	random forest algorithm	This method increases to a certain degree the detection accuracy	The sensitive allowance rules approach is used
[84]	DAMBA collects application's static and dynamic characteristics.	TANMAD Algorithm	to preserve the mobile client's limited resources	In order to improve efficiency and precision,
[85]	It is suggested that you conduct a Cloak and Dagger assault.	Cloak and Dagger attack algorithm	The market for mobile operating systems is	Enables the detection of all potentially harmful

Ref.	Model	Methods/ Algorithm	Achieved Objectives	Significant Results
			expanding.	programs on a mobile device's operating system.
[86]	The detection will be measured using three distinct classifications (KNN), (RF) and (DT).	GIST descriptor	to create a malware application for Android devices	Achieve 84.14% accuracy detection
[88]	Our solution use the matrix representing the system calls gathered and the CNN model input	a neural network	For autonomous learning, employed a neural network, and to be more specific	Less costly memory representation and hence speed up the learning process

Table below compares several suggested methods for detecting Android malware, one of which is based on machine learning algorithms. It is the most effective method among all, and it is utilized more often than the others. Various machine learning techniques have been considered in the development of malware detection systems, Machine learning-based classification was an important class of malware protection methods. Next, treated on DexCNN and DexCRNN, the two deep learning techniques. Moreover, the research provides two detection methods for end-to-end malware without human engineering, which were tested on a data set of 80 0 benign APKs and 80 0 malicious APKs. The system comparison is beneficial in gaining insight into the systems utilizing a static analysis method for Android Malware detection. The metrics shown in the table are used to evaluate the system's performance and functionality. As well as this section contains a short description of the parameters. We considered different types of Android malware detection technologies using various deep learning techniques. Because of Android's open nature, we're looking at a variety of malware detection techniques, including: Deep Flow, MalDozer, Droid Detector, and Droid Deep Learner also We advised a neural network for automatic learning, and morepreciselythe Convolutional Neural Network (CNN).

5. CONCLUSION

This paper introduces a good basic understanding of Android malware detection technologies. Malware detection is one of the importan approaches depended for the Android Operating System's security. The comparison in this work is based on the various techniques presented. The detection techniques using hybrid analysis and deep learning are both accurate and scalable. This is also the case for machine-based learning detection. Previously undiscovered malware kinds can be detected, and this could improve the efficiency of detection performance. The strategy that reports all the constraints of static and dynamic analysis methodologies must be introduced to identify hybrid malware. Research is still ongoing in this area to enhance the accuracy and reliability of systems.

DISCLAIMER

The products used for this research are commonly and predominantly use products in our area of research and country. There is absolutely no conflict of interest between the authors and producers of the products because we do not intend to use these products as an avenue for any litigation but for the advancement of knowledge. Also, the research was not funded by

the producing company rather it was funded by personal efforts of the authors.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Abdullah DM, Ameen SY, Omar N, Salih AA, Ahmed DM, Kak SF, et al. Secure data transfer over internet using image steganography. Asian Journal of Research in Computer Science. 2021;33-52.
2. Uma K, Blessie ES. "Survey on android malware detection and protection using data mining algorithms," in 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on. 2018;209-212.
3. Kareem FQ, Ameen SY, Salih AA, Ahmed DM, Kak SF, Yasin HM, et al. SQL injection attacks prevention system technology. Asian Journal of Research in Computer Science. 2021;13-32.
4. Arshad S, Shah MA, Wahid A, Mehmood A, Song H, Yu H. Samadroid: a novel 3-level hybrid malware detection model for android operating system. IEEE Access. 2018;6:4321-4339.
5. Amro B. Malware detection techniques for mobile devices. International Journal of Mobile Network Communications & Telematics (IJMNCT). 2017;7.
6. Ismael HR, Ameen SY, Kak SF, Yasin HM, Ibrahim IM, Ahmed AM, et al. Reliable communications for vehicular networks. Asian Journal of Research in Computer Science. 2021;33-49.
7. Abdullah RM, Ameen SY, Ahmed DM, Kak SF, Yasin HM, Ibrahim IM, et al. Paralinguistic Speech Processing: An Overview. Asian Journal of Research in Computer Science. 2021;34-46.
8. Ibrahim IM, Ameen SY, Yasin HM, Omar N, Kak SF, Rashid ZN, et al. Web Server Performance improvement using dynamic load balancing techniques: A review. Asian Journal of Research in Computer Science. 2021;47-62.
9. Bayazit EC, Sahingoz OK, Dogan B. "Malware detection in android systems with traditional machine learning models: A survey," in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 2020;1-8.
10. Ahmed DM, Ameen SY, Omar N, Kak SF, Rashid ZN, Yasin HM, et al. A state of art for survey of combined iris and fingerprint recognition systems. Asian Journal of Research in Computer Science. 2021;18-33.
11. Olorunshola OE, Oluyomi AO. "Android applications malware detection: A comparative analysis of some classification algorithms," in 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). 2019;1-6.
12. Maulud DH, Ameen SY, Omar N, Kak SF, Rashid ZN, Yasin HM, et al. Review on natural language processing based on different techniques. Asian Journal of Research in Computer Science. 2021;1-17.
13. Fu X, Cai H. "On the deterioration of learning-based malware detectors for Android," in 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), 2019;272-273.
14. Salih AA, Ameen SY, Zeebaree SR, Sadeeq MA, Kak SF, Omar N, et al. Deep learning approaches for intrusion detection. Asian Journal of Research in Computer Science. 2021;50-64.
15. Alqahtani EJ, Zagrouba R, Almuhaideb A. "A Survey on android malware detection techniques using machine learning algorithms," in 2019 Sixth International Conference on Software Defined Systems (SDS), 2019;110-117.
16. Hassan RJ, Zeebaree SR, Ameen SY, Kak SF, Sadeeq MA, Ageed ZS, et al. State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. Asian Journal of Research in Computer Science. 2021;32-48.
17. Riasat R, Sakeena M, Sadiq AH, Wang YJ. "Onamd: An online android malware detection approach," in 2018 International Conference on Machine Learning and Cybernetics (ICMLC). 2018;190-196.
18. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, Adel AZ, et al. Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling. Asian Journal of Research in Computer Science. 2021;1-16.

19. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Yahia HS, Mahmood MR, et al. Comprehensive survey of big data mining approaches in cloud systems. Qubahan Academic Journal. 2021;1:29-38.
20. Abdulrahman LM, Zeebaree SR, Kak SF, Sadeeq MA, Adel AZ, Salim BW, et al. A state of art for smart gateways issues and modification. Asian Journal of Research in Computer Science. 2021;1-13.
21. Yazdeen AA, Zeebaree SR, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. Qubahan Academic Journal. 2021;1:8-16.
22. Haji SH, Zeebaree SR, Saeed RH, Ameen SY, Shukur HM, Omar N, et al. Comparison of software defined networking with traditional networking. Asian Journal of Research in Computer Science. 2021;1-18.
23. Malallah H, Zeebaree SR, Zebari RR, Sadeeq MA, Ageed ZS, Ibrahim IM, et al. A comprehensive study of kernel (issues and concepts) in different operating systems. Asian Journal of Research in Computer Science. 2021;16-31.
24. Yasin HM, Zeebaree SR, Sadeeq MA, Ameen SY, Ibrahim IM, Zebari RR, et al. IoT and ICT based smart water management, monitoring and controlling system: A review. Asian Journal of Research in Computer Science. 2021;42-56.
25. Ibrahim IM. Task scheduling algorithms in cloud computing: A review. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12:1041-1053.
26. Zebari IM, Zeebaree SR, Yasin HM. "Real time video streaming from multi-source using client-server for video distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
27. Yasin HM, Zeebaree SR, Zebari IM. "Arduino based automatic irrigation system: Monitoring and SMS controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
28. Zeebaree S, Yasin HM. Arduino based remote controlling for home: power saving, security and protection. International Journal of Scientific & Engineering Research. 2014;5:266-272.
29. Zeebaree S, Zebari I. Multilevel client/server peer-to-peer video broadcasting system. International Journal of Scientific & Engineering Research. 2014;5:260-265.
30. Taher KI, Saeed RH, Ibrahim RK, Rashid ZN, Haji L.M, Omar N, et al. Efficiency of semantic web implementation on cloud computing: A review. Qubahan Academic Journal. 2021;1:1-9.
31. Zebari S, Yaseen NO. Effects of parallel processing implementation on balanced load-division depending on distributed memory systems. J. Univ. Anbar Pure Sci. 2011;5:50-56.
32. Sadeeq MM, Abdulkareem NM, Zeebaree SR, Ahmed DM, Sami AS, Zebari RR. IoT and cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal. 2021;1:1-7.
33. Hasan DA, Hussan BK, Zeebaree SR, Ahmed DM, Kareem OS, Sadeeq MA. The impact of test case generation methods on the software performance: A review. International Journal of Science and Business. 2021;5:33-44.
34. Jijo BT, Zeebaree SR, Zebari RR, Sadeeq MA, Sallow AB, Mohsin S, et al. A comprehensive survey of 5G mm-wave technology design challenges. Asian Journal of Research in Computer Science. 2021;1-20.
35. Kareem FQ, Zeebaree SR, Dino HI, Sadeeq MA, Rashid ZN, Hasan DA, et al. A survey of optical fiber communications: Challenges and processing time influences. Asian Journal of Research in Computer Science. 2021;48-58.
36. Abdullah SMSA, Ameen SYA, Sadeeq MA, Zeebaree S. Multimodal emotion recognition using deep learning. Journal of Applied Science and Technology Trends. 2021;2:52-58.
37. Sadeeq MA, Zeebaree S. Energy management for internet of things via distributed systems. Journal of Applied Science and Technology Trends. 2021 ;2:59-71.
38. Omer MA, Zeebaree SR, Sadeeq MA, Salim BW, Mohsin SX, Rashid ZN, et al. Efficiency of malware detection in android system: A survey. Asian Journal of Research in Computer Science. 2021;59-69.
39. Maulud DH, Zeebaree SR, Jacksi K, Sadeeq MAM, Sharif KH. State of art for semantic analysis of natural language processing. Qubahan Academic Journal. 2021;1:21-28.

40. Shukur H, Zeebaree SR, Ahmed AJ, Zebari RR, Ahmed O, Tahir BSA, et al. A state of art survey for concurrent computation and clustering of parallel computing for distributed systems. Journal of Applied Science and Technology Trends. 2020;1:148-154.
41. Jacksi K, Ibrahim RK, Zeebaree SR, Zebari RR, Sadeeq MA. "Clustering documents based on semantic similarity using HAC and K-mean algorithms," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;205-210.
42. Sadeeq MA, Abdulazeez AM. "Neural networks architectures design, and applications: A review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020 ;199-204.
43. Ageed ZS, Ibrahim RK, Sadeeq M. Unified ontology implementation of cloud computing for distributed systems. Current Journal of Applied Science and Technology. 2020;82-97.
44. Zeebaree S, Ameen S, Sadeeq M. Social media networks security threats, risks and recommendation: A case study in the kurdistan region. International Journal of Innovation, Creativity and Change. 2020;13:349-365.
45. Salim BW, Zeebaree SR. "Design and analyses of a novel real time kurdish sign language for kurdish text and sound translation system," in 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). 2020;348-352.
46. Sulaiman MA, Sadeeq M, Abdulraheem AS, Abdulla AI. Analyzation study for gamification examination fields. Technol. Rep. Kansai Univ. 2020;62:2319-2328.
47. Abdulla AI, Abdulraheem AS, Salih AA, Sadeeq M, Ahmed AJ, Ferzor BM, et al. Internet of things and smart home security. Technol. Rep. Kansai Univ. 2020;62:2465-2476.
48. Sadeeq M, Abdulla AI, Abdulraheem AS, Ageed ZS. Impact of electronic commerce on enterprise business. Technol. Rep. Kansai Univ. 2020;62:2365-2378.
49. Alzakholi O, Shukur H, Zebari R, Abas S, Sadeeq M. Comparison among cloud technologies and cloud performance. Journal of Applied Science and Technology Trends. 2020;1:40-47.
50. Ageed Z, Mahmood MR, Sadeeq M, Abdulrazzaq MB, Dino H. Cloud computing resources impacts on heavy-load parallel processing approaches. IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:30-41.
51. Sallow A, Zeebaree S, Zebari R, Mahmood M, Abdulrazzaq M, Sadeeq M. "Vaccine tracker," SMS reminder system: Design and implementation; 2020.
52. Sharif KH, Zeebaree SR, Haji LM, Zebari RR. "Performance measurement of processes and threads controlling, tracking and monitoring based on shared-memory parallel processing approach," in 2020 3rd International Conference on Engineering Technology and its Applications (IICETA). 2020;62-67.
53. Sadeeq MA, Zeebaree SR, Qashi R, Ahmed SH, Jacksi K. "Internet of things security: A survey," in 2018 International Conference on Advanced Science and Engineering (ICOASE). 2018;162-166.
54. Abdulazeez AM, Zeebaree SR, Sadeeq MA. Design and implementation of electronic student affairs system. Academic Journal of Nawroz University. 2018;7:66-73.
55. Sallow AB, Sadeeq M, Zebari RR, Abdulrazzaq MB, Mahmood MR, Shukur HM, et al. An investigation for mobile malware behavioral and detection techniques based on android platform. IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:14-20.
56. Mohammed SM, Jacksi K, Zeebaree SR. "Glove word embedding and DBSCAN algorithms for semantic document clustering," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;1-6.
57. Dino HI, Zeebaree SR, Hasan DA, Abdulrazzaq MB, Haji LM, Shukur HM. "COVID-19 diagnosis systems based on deep convolutional neural networks techniques: A review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;184-189.
58. Zebari RR, Zeebaree SR, Sallow AB, Shukur HM, Ahmad OM, Jacksi K. "Distributed denial of service attack mitigation using high availability proxy and network load balancing," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;174-179.

59. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Rashid ZN, Salih AA, et al. A survey of data mining implementation in smart city applications. Qubahan Academic Journal. 2021;1:91-99.
60. Ageed ZS, Zeebaree SR, Sadeeq MA, Abdulrazzaq MB, Salim BW, Salih AA, et al. A state of art survey for intelligent energy monitoring systems. Asian Journal of Research in Computer Science. 2021;46-61.
61. Abdulqadir HR, Zeebaree SR, Shukur HM, Sadeeq MM, Salim BW, Salih AA, et al. A study of moving from cloud computing to fog computing. Qubahan Academic Journal. 2021;1:60-70.
62. Shukur H, Zeebaree S, Zebari R, Zeebaree D, Ahmed O, Salih A. Cloud computing virtualization of resources allocation for distributed systems. Journal of Applied Science and Technology Trends. 2020;1:98-105.
63. Liu K, Xu S, Xu G, Zhang M, Sun D, Liu H. A review of android malware detection approaches based on machine learning. IEEE Access. 2020;8:124579-124607.
64. Rathore H, Agarwal S, Sahay SK, Sewak M. "Malware detection using machine learning and deep learning," in International Conference on Big Data Analytics. 2018;402-411.
65. Yuan H, Sun W. "Android application security detection method based on metropolis algorithm," in 2019 IEEE 19th International Conference on Communication Technology (ICCT). 2019 ;1280-1284.
66. Abdulraheem AS, Salih AA, Abdulla AI, Sadeeq M, Salim N, Abdullah H, et al. Home automation system based on IoT; 2020.
67. Salih AA, Zeebaree S, Abdulraheem AS, Zebari RR, Sadeeq M, Ahmed OM. Evolution of mobile wireless communication to 5G revolution. Technology Reports of Kansai University. 2020;62:2139-2151.
68. Fan M, Liu J, Luo X, Chen K, Tian Z, Zheng Q, et al. Android malware familial classification and representative sample selection via frequent subgraph analysis. IEEE Transactions on Information Forensics and Security. 2018;13:1890-1905.
69. Dino HI, Zeebaree S, Salih AA, Zebari RR, Ageed ZS, Shukur HM, et al. Impact of Process Execution and Physical Memory-Spaces on OS Performance. Technology Reports of Kansai University. 2020 ;62:2391-2401.
70. Murtaz M, Azwar H, Ali SB, Rehman S. "A framework for Android Malware detection and classification," in 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS). 2018;1-5.
71. Cui H, Zhou Y, Wang C, Li Q, Ren K. "Towards privacy-preserving malware detection systems for android," in 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). 2018;545-552.
72. Shibija K, Joseph RV. "A machine learning approach to the detection and analysis of android malicious apps," in 2018 International Conference on Computer Communication and Informatics (ICCCI). 2018;1-4.
73. Alzaylaee MK, Yerima SY, Sezer S. DL-Droid: Deep learning based android malware detection using real devices. Computers & Security. 2020;89:101663.
74. Wu Q, Zhu X, Liu B. A survey of android malware static detection technology based on machine learning. Mobile Information Systems; 2021.
75. Samra AAA, Qunoo HN, Al-Rubaie F, El-Talli H. "A survey of static android malware detection techniques," in 2019 IEEE 7Th palestinian international conference on electrical and computer engineering (PICECE). 2019;1-6.
76. Lei T, Qin Z, Wang Z, Li Q, Ye D. EveDroid: Event-aware android malware detection against model degrading for IoT devices. IEEE Internet of Things Journal. 2019;6:6668-6680.
77. Taheri L, Kadir AFA, Lashkari AH. "Extensible android malware detection and family classification using network-flows and API-calls," in 2019 International Carnahan Conference on Security Technology (ICCST). 2019;1-8.
78. Patel ZD. "Malware detection in android operating system," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). 2018;366-370.
79. Leeds M, Keffeler M, Atkison T. A comparison of features for android malware detection," in Proceedings of the South East Conference. 2017;63-68.
80. Qing-Fei W, Xiang F. "Android malware detection based on machine learning," in

2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC). 2018;434-436.
81. Sabhadiya S, Barad J, Gheewala J. "Android malware detection using deep learning," in 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). 2019;1254-1260.
82. Ren Z, Wu H, Ning Q, Hussain I, Chen B. End-to-end malware detection for android IoT devices using deep learning. Ad Hoc Networks. 2020;101:102098.
83. Lu T, Hou S. "A two-layered malware detection model based on permission for android," in 2018 IEEE International Conference on Computer and Communication Engineering Technology (CCET). 2018;239-243.
84. Zhang W, Wang H, He H, Liu P. DAMBA: detecting android malware by ORGB analysis. IEEE Transactions on Reliability. 2020;69:55-69.
85. Omelchenko T, Nikishova A, Umnitsyn M, Sadovnikova N, Parygin D, Kostyukov A. "Protection software for mobile operating systems," in 2018 International Conference on System Modeling & Advancement in Research Trends (SMART). 2018;54-59.
86. Darus FM, Salleh NAA, Ariffin AFM. "Android malware detection using machine learning on image patterns," in 2018 Cyber Resilience Conference (CRC). 2018;1-2.
87. Agrawal P, Trivedi B. "A survey on android malware and their detection techniques," in 2019 IEEE International conference on electrical, computer and communication technologies (ICECCT). 2019;1-6.
88. Abderrahmane A, Adnane G, Yacine C, Khireddine G. "Android malware detection based on system calls analysis and CNN classification," in 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW). 2019;1-6.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle4.com/review-history/71739