International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

Anomaly Based Malware Detection System on Smartphone – A Systematic Review

Ezeh Kingsley Ikechukwu, Prof. Ejiofor Virginia Ebere, Frank Ekene Ozioko, Asogwa T.C, Nzeogu Neheta Chinyere, Nwankwo Ugochukwu Cornelius

Department of computer science, Enugu state university of science and technology.
Department of computer science,NnamdiAzikwe University.
Department of computer science, Enugu state university of science and technology.
Department of computer science, Enugu state university of science and technology.
Department of computer science, Enugu state university of science and technology.
Department of computer science, Caritas University, Enugu State.

Date of Submission: 05-10-2022 Date of Acceptance: 14-10-2022

ABSTRACT- Malware has been a significant issue on cell phones. General countermeasures to Smart phone malwares are at present restricted to signature-based enemy of infection scanners which proficiently identify known malwares, yet they have genuine inadequacies with new and obscure malwares making a lucky opening for assailants. The prevalence of mobile devices (smartphones) along with the availability of high-speed internet access worldwide resulted in a wide variety of mobile applications that carry a large amount of confidential information. Although popular mobile operating systems such as iOS and Android constantly increase their defenses methods, data shows that the number of intrusions and attacks using mobile applications is rising continuously. This paper presents an extensive review of anomaly based malware detection stem on smartphone. It explores the existing mobile malware detection, android malware detection system. Though many malicious applications have been in existence, the analysis presented in this paper gives new insights to the readers on the applications of malware detection system. The K-Nearest Neighbour (KNN), Naive Bayes, K-means, DecisionTrees, C4.5 (=J48), Bayesian classifier, machine learning techniques and neural network algorithms in the review aid in the detection of malicious applications. The malware techniques in this review helps in detection of malware irrespective of the form it appears.

Keyword: malware detection, smartphone, anomaly based, mobile malware.

OVERVIEW: This paper presents a systematic review of Anomaly based malware detection system on smartphone. As Android ruling most of the market, malware keeps on growing; Thousands of new malware appear rapidly. The theoretical introduction of malware detection system on smartphone is presented in Section I. Section II discussed the types of malware. Section III-A, reviews malware detection techniques, also intrusion detection method was discussed in section III-B, section III- C, deals with review of literature. Section III-D, table 1 comparison of algorithms used in the reviewed literature, section IV, malware detection approaches and counter measures was discussed. Android Malware Threats and their Evolution was reviewed in section V, section VI (A-C), deals with Tools for Malware Detection. Section VI-D, table 2 Comparison of mobile malware detection methods. Summary was covered in Section VII.

I. INTRODUCTION

The rapid growth of smartphone technologies and their widespread user acceptancecame simultaneously with an increase in the number and sophistication of malicious software targeting popular platforms. Malware (short for malicious software) developed forearly mobile devices such as Palm platforms and featured mobile phones**.** According to Global market share,during second quarter of 2018, there was 88% smartphones inthe market have been sold towards end users and that isAndroid systems [1].Besides, it is becoming more and more popular because of itsportability andconvenient to use. For

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

an example, thesmartphone contains various types of functions and serviceslike it can hold the personal information and access files that usually been stored in the cloud such as bank accountinformation, email details, password and it also allows theuser to interact with each other by sending a message or call.However, with the growth of the Android mobile popularityhas brought many security concerns and threats from theattacker that might spread the malware that makes the systemact differently than it is supposed to behave. The malwareusually sent such fraudulent message and charge the user fortheir fake services.According to the Security Threat Report released bySymantec in 2018 [2], the overall target activities thatattacked is up by 10 percent in 2017. In fact, by March 12,2018, there are 4, 964, 460 devices infected by RottenSysmalware [3]. This situation desperately needs to find apotential method to detect malware before it harmed moreAndroid smartphones. In this era globalization, peoplecommonly used smartphones in such many ways like using anetwork connection to interact with the world. For example,online shopping, online banking, and cloud storage. Naturally,there are also disadvantages by using this kind of networkconnections towards the user. Like example, the storing ofconfidential information in smartphones might attract theattacker to use dirty things in order to get user details likespreading malware towards some software or applications thatmight be installed in their smartphones either they realized ornot especially for Android users.[4] As Android ruling most of the market, malware keeps on growing; Thousands of new malware appear rapidly. The term malware emanates from coalescing two words malignant and software, and to be acclimated to betoken any unwanted software.it recognizes any code incorporated, transmuted, or preoccupied from software system so as to deliberately cause hurt or subvert theplanned functionality of the system. Malware is described by replication, self-execution, and corruption of PC framework. [5] The present malware can do a lot of things, for example, transmitting user contact list and other information, bolting the gadget totally, giving remote access to [6] lawbreakers, sending SMS and MMS messages and so forth.

II. MALWARE TYPES

For making malware, aggressors use diverse courses going from clear standard systems that embedding's an outstanding piece of codes into a program document, to complex ones that use refined calculation to make obfuscated and polymorphic malware. [7]

A. Ordinary Malware (Static)

This kind of malware can be distinguished effectively by separating some unique characteristics which famous of a signature.

B. Polymorphic Malware

There is variable malware in which sentence structures of mal-code change in each time of infection, however the semantic proceed as before with no critical change at all.

C. Obfuscated Malware (Dynamic)

Incorporate polymorphic and transformative malware, in which the first code changed into a shape that is practically the equivalent however is substantially harder to becomprehended.

D. Encryption Malware

Encryption procedures are the most generally perceived strategies used in polymorphic malware.

III. MALWARE DETECTION

A. Malware Detection Techniques

Techniques utilized for identifying malware can be classified comprehensively into two classifications:Anomaly-Based Detection and Signature-Based Detection. An inconsistency based identification strategy utilizes its information on what comprises ordinary conduct to choose the noxiousness of a program under examination, Figure 1. Indicates distinctive approaches, which go underthese techniques. A particular analysis or approach of both thetechniques is dictated by how specific techniques accumulatedata to recognize and detect malware.

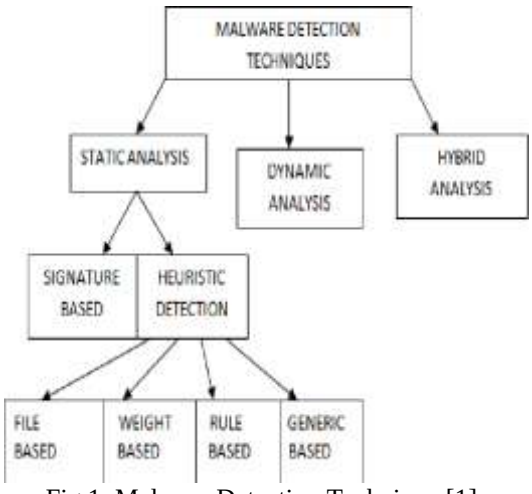

Fig 1: Malware Detection Technique [1].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

1) Signature-based techniques: The pernicious practicesof know malware are caught as their signatures. When one ofits signatures is perceived, the malware is recognized. [8]

2) Anomaly-based techniques (behavior-based): Thetypical system conduct is displayed first. At that point, themalware is identified at whatever point the system conduct goes amiss from the displayed ordinary conduct. [9]

3) Heuristic based techniques (specification-based):Artificial intelligence (AI), signature and anomaly-basedtechniques to upgrade their proficiency. [10]

B. Intrusion Detection Methods:

All malware scanners, essentially, utilize signature and anomaly -based techniques for perceiving personalities ofprograms.

1) Dynamic methods: Utilization run-time data of amalware, when it is executed in a memory.

2) Static methods: Those are finished by extricatingfeatures from static malware when it is in a disk.

3) Hybrid methods: Utilization mix of dynamic and staticmethods [11].

C. Malware Detection Types

1) Host-based intrusion detection system (HIDS): monitordynamic conduct and condition of particular PCframework to check whether there are any inner or outsideactivities swindle the framework approach [12].

2) Network-based intrusion detection system (NIDS):Used to sniff every one of the parcels on network nodes forexamination. In this create a lone sniffer module set in everyframework segment to screen traffic in that fragment.Interestingly dispersed system based interruption locationframework has different modules put in each hub to screen movement in those nodes or hubs. [13]

C.Review of Related Literature

This section, examine some of the previous methodologies used by researchers for malware detection on smartphone. Various approaches have been used to detect malware on smartphone and they can be generally classify into K-Nearest Neighbour (KNN), Naive Bayes, K-means,DecisionTrees, C4.5 (=J48), Bayesian classifier, machine learning techniques and neural network

According to [14], present a standard based framework so as to demonstrate pernicious capability of Android applications. Hence, they gathered the top311 applications from android market and checked them for events of certain authorization set in an arrangement document of each. This Check demonstrated that five of these applications executed perilous functionalities. Another five additionally indicated perilous authorizations however these could be contended through gave usefulness of those applications.

In [15], study introduced a cell phone double safeguard insurance system that permits official and elective Android Markets to identify malignant applications among those new applications that are submitted for open delivery. This structure comprises of workers running on mists where engineers who wish to deliver their new applications can transfer their product for check reason. The confirmation worker first uses framework call measurements to recognize expected noxious applications. After check, on the off chance that the product is perfect, the application will at that point be delivered to the significant business sectors. The test results utilizing 120 test applications (which comprise of 50 malware and 70 typical applications) demonstrate that we can accomplish 94.2% and 99.2% exactness with J.48 and Random woodland classifier separately utilizing this structure.

According to [16], proposed a lightweight IDS fordetecting malicious behavior for android devices which used avery powerful multi-layer perception (MLP) neural network.This system consists of three components: information source,analysis engine, response. There is a machine learningalgorithm for detecting unknown threads with accuracyreaches to 81, 39% and detection rate reaches to 85,02%. Themain goal of system is to achieve very high rates of maliciousbehavior detection with small rates of false alarms. Thedetection in this system achieved by monitoring the NetFlows, then IDS, which has a strong Python backendanalyzing the network traffic, and matched it with (MLP)neural network. If there is matching an alert is fired fordetecting an intrusion.

As indicated by [17], proposed another system to get and examine cell phone application movement. They found that observing framework calls is one of the most precise procedures for deciding the conduct of Android applications. The creator built up a lightweight customer called Crowdroid. This application utilizes publicly supporting way of thinking where a client sends non individual however conduct related information of every application they use to the worker. This is trailed by malware recognition dependent on the call vectors by the worker. The

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

exploratory outcomes did by the writer had 100% identification rate for self-composed malware.

In [18], express that implanted gadgets, as mobile phones, shrewd cards or installed network sensors are generally compact, convey remote and are battery controlled or if nothing else vitality restricted. The plan of security for implanted frameworks contrasts from customary security plan, as various attributes can be found for every sort. There are two principle gatherings of qualities that separate the security engineering from Embedded System from that of workstations and workers: asset impediments and physical openness. In their work, Hwang et al. guarantee that inserted security can't be comprehended at single security deliberation layer and subsequently present safety efforts for all reflection layers.

In [19], introduced TaintDroid, a productive, framework wide data stream following apparatus that can all the while track different wellsprings of delicate information. We additionally utilized our TaintDroid usage to consider the conduct of 30 famous outsider applications, picked indiscriminately from the Android Marketplace. Our investigation uncovered that 66% of the applications in our examination display dubious treatment of touchy information, and that 15 of the 30 applications revealed clients' areas to far off promoting workers.

According to [20], introduced an anomaly-based system,which consist of two stages: first constructs signatures for theAPI calls of target device then train a classifier using a support vector machines (SVMs) in order to distinguish between amalicious programs from benign program.

In [21], a basic, but then profoundly compelling procedure for identifying malevolent Android applications on an archive level was proposed. The procedure performs programmed classification dependent on global positioning framework calls while applications are executed in a sandbox domain. The method was actualized in an apparatus called MALINE, and performed broad experimental assessment on a set-up of around 12,000 applications.

According to [22], proposed a proactive plan to spot zero-day Android Malware without depending on malware tests and their marks to spot potential security hazards presented by untrusted applications. They created Risk Ranker, a robotized framework that scalably dissect applications whether they display perilous practices. They performed static investigation on the figured out Dalvik bytecode contained in each application by separating the information stream and control stream from the code way. They gathered 118,318 applications from different Android advertises and handled it inside four days. From their examination they revealed 3281 hazardous applications.

In [23], utilized both static and dynamic examination to distinguish malware in android applications. They consolidated the static investigation (consent) and dynamic examination (System call following) with AI. They performed static examination by separating authorizations from the Android's manifest.xml document and contemplated the distinction between the quantity of consents mentioned by kind and noxious applications. They understood that the quantity of consents mentioned by favorable and pernicious application is marginally the equivalent. This strategy was tried on different amiable and noxious applications.

In [24], Kirin security administration which performs lightweight affirmation of utilizations was proposed for Android to alleviate malware at introduce time. Kirin proclaims that a mix of consents could be risky. Kirin comprises of three parts, installer, security administration and information base of security rules. The installer separates security arrangement from the AndroidManifest.xml document. Their outcome shows that affirmation method fizzles for just 1.6% of uses in their dataset subsequently Kirin can be sensible for essentially moderate malware.

According to [25], proposed DREBIN, a lightweight strategy for recognition of Android malware that empowers recognizing noxious applications legitimately on the cell phone. DREBIN plays out a wide static examination, removes a lot of highlights from the application's AndroidManifest.xml (equipment segments, mentioned authorizations, App segments, and separated plans) and dismantled code (limited API calls, utilized consents, confined API calls, network addresses) to create a joint vector space. At the point when tried with 123,453 considerate applications and 5,560 malware tests, DREBIN effectively identified 94% of the malware with a bogus positive pace of 1%.

According to [26], extricates six sorts of data Permission, Intent channel, Intent channel, Process name, Intent channel, number of re-imagined consent from show records and uses them to identify Android malware. Results show that the strategy can identify obscure malware tests that are imperceptible by a straightforward mark based methodology. This methodology is modest to execute in light of the fact that solitary the show record is examined.

In [27], introduced a quick, versatile, and exact framework for Android malware location and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

family distinguishing proof dependent on lightweight static investigation. DroidSieve utilizes profound review of Android malware to assemble successful and strong highlights reasonable for computational learning. Their discoveries show that static examination for Android can succeed in any event, when gone up against with obscurity methods, for example, reflection, encryption and progressively stacked local code. While essential changes in attributes of malware stay a generally open issue, DroidSieve stays tough against cutting edge obscurity methods which can be utilized to rapidly determine new and grammatically extraordinary malware variations.

In [28], Droid Detective, an android malwaredetection system was proposed to enhance the Security ofmobile devices. It is offline tools, which depend onpermissions analysis combinations in order to detect anymobile malware. This tool developed by using K-mapsalgorithm. Droid Detective achieve false positive rate =12.47%, false negative rate= 16.43% and with positive rate =87.53%.

According to [29], proposed a scheme byextract several Permissions from .APK files: RequestedPermissions, Request Permission Pairs, Used Permissions, used Permission Pairs. This schema TPR IS 80.5%, FPR 0.5%and with accuracy 98,6%.

In [30], a Genome Project data classifier forandroid application by using Bayesian classifier based onstatic code analysis. A feature extracted from .apk files like:API calls, Linux system commands and permissions so as toresults announced preferable discovery rates over signature-based antivirus.

According to [31], presents an authorization based Android malware recognition framework, APK Auditor that utilizes static investigation to describe and order Android applications as benevolent or malevolent. APK Auditor comprises of three parts: A mark data set to store removed data about applications and examination results, an Android customer which is utilized by endusers to give application investigation demands, and a focal worker answerable for speaking with both mark information base and cell phone customer. 8762 applications were utilized to test framework execution. Result shows that APK Auditor can recognize most notable malwares and features the ones with a potential in roughly 88% exactness with a 0.925 specificity.

D. Comparison of the algorithms

Algorithm	Strength	Weakness
K-Nearest Neighbour (KNN),	High percentage of accuracy in detecting malicious application	Coast very big load to un determined data set.
Naive Bayes	Very fast and simple in malware detection	Require presumption of shared freedom of features
DecisionTrees	Ability to deal with undetermined data set or features whatever size of data	Difficulty to control the process
C4.5 (=J48)	Easy to understand produced rues of process	Low capacity

IV. MALWARE DETECTION APPROACHES AND COUN-TER MEASURES

Countermeasures, which help to secure a system, can be usually taken by installing certain hard- or software. Three main systems for computers can be identified: firewalls, antivirus software and intrusion detection systems. Firewalls are purported "white list" - based frameworks, which implies that there is an uncommon rundown of rules expressly permitting certain ports to speak with inward or outside peers. On the off chance that noxious programming can take on the appearance of believed programming utilizing a confided in port, an essential firewall will permit all correspondence exercises. Antivirus scanners

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

use "boycotts" so as to distinguish certain dangers remembered for the boycott. An infection scanner can impede infections, worms, and Trojan ponies with continuous checking or manual examining. Malware is recognized by filtering for and finding a specific string or example, additionally called signature. There-front, the malware must be known by the scanner. Infection scanners typically incorporate a particular cleansing schedules relating to the recognized marks [32]. Interruption Detection Systems (IDS) once were frameworks that observed organization traffic. Logged traffic was utilized by network directors so as to identify irregular conduct [33]. Countermeasures like shutting ports or bolting frameworks could be taken by the overseers. IDS advanced into interruption anticipation frameworks (IPS) which can recognize certain irregular practices and take preventive measures naturally. Base on anomalous practices, interruption discovery and avoidance frameworks (IDPS) are fundamentally ready to recognize malware movement while they do not have the expulsion schedules known from infection scanners. Infection scanners and Intrusion Detection Systems present the premise of our methodologies. While firewalls center on confining organization traffic, infection scanners and Intrusion Detection Systems attempt to identify vindictive programming and exercises utilizing static and dynamic examination.

V. ANDROID MALWARE THREATS AND THEIR EVOLUTION

Types of threats found on Android mobile applications, which are summarized below.

1. Malware

Attackers want to gain access to a device by installing malware on it. The purpose is to stealdata or damage the device. Malware is installed by tricking the user to install a legitimatelylooking application or in most cases to exploit vulnerability on the device, e.g., a securityflaw in the Web browser.

2. Spyware

One of the most common types of malicious applications for the Android platform is spy-ware. It is designed to get sensitive information from a victim's system and transfer thisinformation to the attacker. Spyware can be commercial and malicious. Commercial spyware are applications installed on the user's handset manually by another person specificallyto spy on the user, while malicious spyware covertly steal data and transmit it to a third party.An example of commercial spyware is CarrierIQ, used extensively by various mobile devicemanufacturers and vendors [34]. CarrierIQ had the capability to log everythingthat was done on a device, including Web search using the secure HTTPS protocol, andwas allegedly used to increase customer satisfaction by logging dropped calls and similarinformation.

3. Grayware

The main purpose of grayware is to spy on users who installed the software on their ownbecause they thought that it is legitimate software. This is partly correct because the authorsinclude real functionality as advertised. Nevertheless, they also collect information from thesystem such as the user's address book or his browsing history. The main goal is to collectinformation for marketing purposes, etc.

4. Fraudware

Corresponding applications are installed by tricking the user to install a legitimately lookingapplication, which will gain full functionality after sending several premium-rated SMSmessages. In contrast to malware, fraudware informs the user about the upcoming charges, but this information is often hidden and not minded by the user.

5. Trojan

Trojans are applications that pretend to be useful, but perform malicious actions in the back-ground such as downloading additional malware, modifying system settings, or infectingother files on the system. Android malware is mostly Trojans. The attack vectors used byviruses and worms are largely unavailable to malware developers because of the sandboxing model. The malicious code is usually included into legitimateapplications, which are then redistributed [35] as the original application. Applications misused for this purpose are often paid applications redistributed as free applicationson third party markets.

6. Root exploit

Root exploits are possible on Android in order to gain control of the device, but are considered a double-edged sword among the security community. Rooting can give the usercontrol over a device and also gives the same amount of control to any application, whichgains access to the root rights. Root privileges given to a malicious application can completely compromise the device, as the application can theoretically remove the root privileges from the user. This is a security flaw in this case. The malicious application pretendsto be normal until it is installed on the user's device, like most Trojans. It attempts,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

wheninstalled, to use one or more root exploits to gain root access to the device. An applicationwith root access can replace, modify and install applications as it wishes. The DroidKungFuTrojan is an example. It installs a backdoor on the phone once it has gainedroot access. It then disguises this backdoor from the user both by using a name, whichlooks innocent and hiding the application icon from the user. This backdoor can then beused for installing other malicious applications on the device or simply for stealing privateinformation.

VI. TOOLS FOR MALWARE DETECTION

While malware tries to conceal its presence and its actions, users try to find it and protect themselves. To help users in the task, free and paid tools are available to them. Three tools are commonly used for this purpose in discovery, assimilation and destruction stages: Firewalls, Intrusion Detection Systems (IDS) and antivirus software. Their common mission is to track down and to eliminate potential malicious applications.

A. Firewall

A firewall is a barrier that protects information from a device or network when establishing communication with other networks, e.g. the Internet. Its purpose is to protect the purity of the devices on which they are installed by blocking intrusions orchestrated from the Internet.

Several benefits are associated with their use. First, they are well known solutions. They are also extensively used on other platforms (PC and server). And finally, they are very effective because they take advantage of the maturity gained by firewalls on PCs. A disadvantage is, that they are ineffective against attacks on the browser, bluetooth, e-mail, SMS, and MMS. They are used as modules in antiviruses on Android.

B. Intrusion Detection Systems

An Intrusion Detection System (IDS) represents a set of software and hardware components whose main function is to detect abnormal or suspicious activities on the analysed target: A network or a host. This is a family of tools of many types: IDS, Host Intrusion Detection System (H-IDS), Network Intrusion Detection System (NIDS), IDS hybrid, Intrusion Prevention System (IPS), and Kernel IDS / IPS Kernel (K-IDS / IPS-K). IDS has two major advantages. First, it is able to detect new attacks, even those that seem isolated. Second, it can be easily adapted to any task. It generates unfortunately a high consumption of resources and a high false alarm rate. Andromaly [Shabtai et al. 2012] are examples of an IDS dedicated to detecting malware on the Android platform. Crowdroid is specifically designed to recognise Trojans.

C. Antiviruses

Antiviruses are security software mostly used on smartphones. The popularity gained by their counterparts on desktop has greatly contributed to increase the level of confidence acquired by mobile users. Avast, AVG and F-Secure are examples of renowned antiviruses. They are facing new constraints brought by the rapid evolution of malicious applications. Like desktop platforms, their efficiency is closely related to their detection methods. Form analysis, integrity checking, and dynamic behaviour analysis.

1. Form analysis is detecting the presence of a threat in an application by static characters. It can be based on research of signatures, heuristics or spectral analysis.

• Research of signatures: Searches for patterns or bits, which are characteristics of a known threat. Its main disadvantage is that it is not able to detect unknown threats and known threats, which are modified. It requires a permanent update of the signature database. It is simple to implement and the most used in antivirus companies [36].

• Spectral analysis: Scrutinizes statements commonly used by malware samples but rare in normal applications. It analyses the frequency of such statements statistically to detect unknown threats. This approach is subject to false positive, i.e. normal applications, which are incorrectly classified as malware.

• Heuristic analysis: Its approach is to establish and maintain rules, which are used as pattern to recognize malicious applications. It is also subject to false alerts, as the previous approach.

D. Comparison of mobile malware detection methods

# Ref	IDS type	Techniques	Algorithms	Pros & Cons
Radoglou et al. [16]	NIDS	Anomaly-based	neural network	Achieve a very high percentage of accuracy with low percentage of false alarms. There is

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 686-696 www.ijaem.net ISSN: 2395-5252

				no saving of resources, which cause fast battery lost.
Guo et al. [20]	HIDS	Signature-based	Naive Bayes algorithms	Semantic patterns and creates a unique signature, but this detection cause time consumption.
Shuang et al. [28]	HIDS	Permission-based	K-maps algorithm	It is offline tools which depend on permissions analysis combinations in order to detect any mobile malware, but doesn't detect some types of zero days malwares.
Xing Liu and Jiqiang Liu. [29]	HIDS	Permission-based	machine learning techniques	Detecting Android malicious applications by extracting several features from a large number of APK files: Requested Permissions, Request Permission Pairs, Used Permissions, Used Permission Pairs. But there is consumption of time.
Yerima et al. [30]	HIDS	Permission-based	Bayesian classifier	Based on static code analysis. achieve high rates of accuracy than signature-based antivirus. But there is dynamic support analysis for any zero days malwares.

E. Review Strategy

This systematic review of food recognition and classification to aid diabetes patient is based on the below guidelines as reflected in the Table below:

1. Inclusion and exclusion criteria

The exclusion criteria include:

• Articles concerned mainly with food recognition and classification for diabetes patient

• Studies that also review papers diabetes patient care

• Conference papers, which have also been published in a journal.

The inclusion criteria include the following:

• Articles food recognition system for diabetes patient

.• Articles that discussed classification of diabetes

• Journals ranked by the Scientific Journal Ranking (SJR)
• Conferences ranked by the Computing Research Education (CORE)

By applying the inclusion and exclusion criteria, 17 studies were selected, as summarized in table3.

Table 3. List of Data Source

Source type	Name of database
Online databases	IEEEXplore, Springer, ACM, ArXiv DOAJ.
Search engines	Google Scholar, CiteSeerx

VII. SUMMARY

This section presents the summary background of literature for malware detection system on smartphone. The related literature on malware detection system helps to detection any malicious application of smartphone. From the above review the system anomaly based malware detection on android helps to secure android phone from any attack of a malware. Malware has been a significant issue on cell phones. General countermeasures to Smart phone malwares are at present restricted to signature-based enemy of infection scanners which proficiently identify known malwares, yet they have genuine inadequacies with new and obscure malwares making a lucky opening for assailants. The prevalence of mobile devices (smartphones) along with the availability of high-speed internet access worldwide resulted in a wide variety of mobile applications that carry a large amount of confidential information. Although popularmobile operating systems such as iOS and Android constantly increase their defenses methods, data shows that the number of intrusions and attacks using mobile applications is risingcontinuously.The review shows that the system aids smartphone users in securing there phone from malware attacks.

REFRENCE

[1]. Statista, “Global market share held by the leadingsmartphone operating systems in sales to end users from1st quarter 2009 to 2nd quarter 2018,” Statista, 2019.
[2]. Symantec, “Internet Security Threat Report,” 2018.
[3]. Feixiang He, Bohdan Melnykov, and Elena Root,“RottenSys: Not a Secure Wi-Fi Service At All,” CheckPoint Research, 2018..https://research.checkpoint.com/2018/rottensys-not-secu re-wi-fi-service/
[4]. M. (Business I. Rosoff, “IDC smartphone OS market share - Business Insider,” 2015. [Online]. Available: http://www.businessinsider.com/idc-smartphone-os-market-share-2015-12?IR=T. [Accessed: 10-Aug-2017].
[5]. R. Price, “BlackBerry global smartphone market share is 0,” 2017. [Online]. Available: http://www.businessinsider.com/blackberry-smartphone-marketshare-zero-percent-gartner-q4-2016-2017-2?IR=T. [Accessed: 10-Aug-2017].
[6]. H. A. Alatwi, “Android Malware Detection Using Category-Based Machine Learning Classifiers,” Rochester Institute of Technology, 2016.
[7]. Saeed, I. A.; Selamat, A. &Abuagoub, A. M. A survey on malware andmalware detection systems, International Journal of Computer Applications,Foundation of Computer Science, 2013, 67
[8]. https://openi.nlm.nih.gov/detailedresult.php?img=PMC4138763_TSWJ2014-983901.005&req=4
[9]. Papamartzivanos, D.; Damopoulos, D. &Kambourakis, G.A cloud-based architecture to crowdsource mobile app privacy leaksProceedings of the 18th Panhellenic Conference on Informatics, 2014, 1-6
Ham, H.-S. & Choi, M.-J. Analysis of android malware detectionperformance using machine learning classifiers ICT Convergence (ICTC),2013 International Conference on, 2013, 490-495
[10]. Ahmadi, M.; Biggio, B.; Arzt, S.; Ariu, D. &Giacinto, G.Detecting misuse of google cloud messaging in android badwareProceedings of the 6th Workshop on Security and Privacy in Smartphones andMobile Devices, 2016, 103-112
[11]. Liu, X. & Liu, J. A two-layered permission-based Android malwaredetection scheme Mobile cloud computing, services, and engineering(mobilecloud), 2014 2nd ieee international conference on, 2014, 142-148.

[12]. He, D.; Chan, S. &Guizani, M. Mobile application security: malwarethreats and defenses IEEE Wireless Communications, IEEE, 2015, 22, 138-144.

[13]. Zheng, M.; Sun, M. &Lui, J. C. Droid analytics: A signature basedanalytic system to collect, extract, analyze and associate androidmalwareTrust, Security and Privacy in Computing and Communications(TrustCom), 2013 12th IEEE International Conference on, 2013, 163-171

[14]. William Enck, MachigarOngtang, and Patrick Drew McDaniel. Onlightweight mobile phone application certification. InACM Con-ference on Computer and Communications Security, pages 235–245,2009.

[15]. X. Su, M. Chuah, and G. Tan, "Smartphone Dual Defense Protection Framework : Detecting Malicious Applications in Android Markets," Mob. Ad-hoc Sens. Networks (MSN), 2012 Eighth Int. Conf., pp. 153–160, 2012.

[16]. Radoglou-Grammatikis, P. I. &Sarigiannidis, P. G.Flow anomaly-based intrusion detection system for Android mobile devicesModern Circuits and Systems Technologies (MOCAST), 2017 6thInternational Conference on, 2017, 1-

[17]. I. Burguera and U. Zurutuza, "Crowdroid : Behavior-Based Malware Detection System for Android," Proc. 1st ACM Work. Secur. Priv. Smartphones Mob. devices (SPSM '11). ACM, New York, NY, pp. 15–26, 2011.

[18]. David D. Hwang, Patrick Schaumont, Kris Tiri, and Ingrid Ver-bauwhede. Securing embedded systems.Security& Privacy Magazine,IEEE, 4(2):40–49, 2006.

[19]. W. Enck, L. P. Cox, P. Gilbert, and P. Mcdaniel, "TaintDroid : An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," ACM Trans. Comput. Syst., p. 32(2):5, 2014.

[20]. Mohata, V. B.; Dakhane, D. M. &Pardhi, R. L.Mobile Malware Detection Techniques
International Journal of Computer Science & Engineering Technology (IJCSET), 2013, 4, 2229-3345.

[21]. M. Dimjaˇ, S. Atzeni, I. Ugrina, Z. Rakamari, and M. Dimjaˇ, "Android Malware Detection Based on System Calls Android Malware Detection Based on System Calls," J. Comput. Secur., 2015.

[22]. M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "RiskRanker : Scalable and Accurate Zero-day Android Malware Detection Categories and Subject Descriptors," Int. Conf. Mob. Syst. Appl. Serv., 2012.

[23]. P. Kaushik and A. Jain, "Malware Detection Techniques in Android," Int. J. Comput. Appl., vol. 122, no. 17, pp. 22–26, 2015.

[24]. W. Enck, M. Ongtang, and P. Mcdaniel, "On Lightweight Mobile Phone Application Certification," ACM Conf. Comput. Commun. Secur., 2009.

[25]. D. Arp, M. Spreitzenbarth, H. Malte, H. Gascon, and K. Rieck, "Drebin : Effective and Explainable Detection of Android Malware in Your Pocket," Proc. 17th Netw. Distrib. Syst. Secur. Symp., pp. 23–26, 2014.

[26]. R. Sato, D. Chiba, and S. Goto, "Detecting Android Malware by Analyzing Manifest Files," Proc. Asia-Pacific Adv. Netw., vol. 36, pp. 23–31, 2013.

[27]. G. Suarez-tangil, S. K. Dash, M. Ahmadi, J. Kinder, G. Giacinto, and L. Cavallaro, "DroidSieve : Fast and Accurate Classification of Obfuscated Android Malware," ACM Conf. Comput. Commun. Secur., 2017.

[28]. Liang, S. & Du, X. Permission-combination-based scheme for androidmobile malware detection Communications (ICC), 2014 IEEE InternationalConference on, 2014, 2301-2306

[29]. Liu, X. & Liu, J. A two-layered permission-based Android malware detection scheme Mobile cloud computing, services, and engineering (mobilecloud), 2014 2nd ieee international conference on, 2014, 142-148

[30]. Pehlivan, U.; Baltaci, N.; Acartürk, C. & Baykal, N.The analysis of feature selection methods and classification algorithms inpermission-based Android malware detectionComputational Intelligence in Cyber Security (CICS), 2014 IEEE Symposiumon, 2014, 1-8

[31]. K. Abdullah, D. Ibrahim, and C. Aydin, "APK Auditor : Permission-based Android malware detection system," vol. 13, pp. 13–15, 2015.

[32]. Mohata, V. B.; Dakhane, D. M. &Pardhi, R. L.Mobile Malware Detection

Techniques
International Journal of Computer Science & Engineering Technology(IJCSET), 2013, 4, 2229-3345

[33]. X. Su, M. Chuah, and G. Tan, "Smartphone Dual Defense Protection Framework : Detecting Malicious Applications in Android Markets," Mob. Ad-hoc Sens. Networks (MSN), 2012 Eighth Int. Conf., pp. 153–160, 2012.

[34]. Fang, Z., H. Weili, and L. Yingjiu: Permission based Android security: Issues and countermeasures. Computers & Security 43 (2014), pp. 205–218.

[35]. Liang, S. and X. Du: Permission-combination-based scheme for Androidmobile malware detection. In: Proceedings of IEEE International Conference on Communications (ICC). Sydney 2014, pp. 2301-2306.

[36]. Shabtai, A., U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss: Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems 38 (2012) No. 1, pp. 161-190.